

County of Santa Clara
Office of the District Attorney Annual Use Report
Data Extraction/Examination
Forensic Tools and Software

July 1, 2022 – June 30, 2023

1. Description

Data extraction/examination forensic tools and software were used only in compliance with the Board-approved Surveillance Use Policy (SUP) during fiscal year 2022-2023. Specifically, investigators in the District Attorney's Office, REACT Task Force, and authorized investigators employed by outside law enforcement agencies used the tools and software to extract, process, enhance, and analyze data from various types of digital devices, including computers, cellular phones, tablets, thumb drives, audio equipment, and video equipment. All of the examinations occurred in the context of criminal investigations. All data extractions or examinations were performed with judicial authorization through a search warrant or written consent from the owner of the device. The data retrieved using the tools and software included computer files, e-mails, contacts, digital images, audio and video files, and other multimedia files. When the tools and software were used consistent with those Board-approved uses, they did capture sound, pictures, video, and information regarding certain members of the public who were not suspected of engaging in unlawful conduct.

Authorized data extraction/examination forensic tools and software employ different processes to track usage and limit access to only authorized persons. These include, but are not limited to, individualized usernames and passwords, mandatory pre-use training, supervisor approval and monitoring, system activity logs, judicial authorization, mandatory chain of custody documentation, and secured locations requiring supervisor presence for access.

The data retrieved from extractions is stored on a password protected forensic computer with sufficient storage capacity and processing capabilities to handle terabytes of data. The data can also be examined by the investigating officer(s) on this computer, which is kept in a secure location requiring supervisor presence for access. Investigators can examine smaller portions of the extractions on their county-issued computers, but are limited by the storage and processing capabilities of the county's standard-issued computer systems. When the data retrieved from extractions needs to be shared with authorized personnel (see Data Sharing below), a forensic copy of the data is transferred to a hard drive device with sufficient storage capacity to hold the data. The data stored on the forensic computer is deleted once forensic copies have been saved to a hard drive for investigatory, prosecutorial or evidence retention purposes.

2. Data Sharing

The data retrieved with data extraction/examination forensic tools and software was regularly shared with authorized personnel in the District Attorney's Office, including investigators, attorneys, paralegals, and justice systems clerks. The data was also regularly shared with authorized personnel at local, State, and Federal law enforcement agencies when authorized and relevant to ongoing criminal investigations and prosecutions. The data was also regularly shared with defense counsel as authorized and required by criminal discovery obligations.

Data was shared with outside law enforcement organizations when authorized and relevant to ongoing criminal investigations and prosecutions involving various crimes, including homicides, cybercrimes, refund fraud, network intrusion, SIM swapping, and grand theft. All data sharing was done in conformity with the Board-approved SUP.

Investigators and the Forensic Examiner assigned to the REACT Task Force performed at least 125 forensic examinations between July 1, 2022 and June 30, 2023. They utilized 14 different tools to extract and examine data from a variety of sources, including cellphones and computers. The data was shared with the following law enforcement agencies:

Local Agencies

Milpitas Police Department
Gilroy Police Department
Los Gatos Police Department
Mt. View Police Department

Out-of-State Agencies

Middlesex District Attorney's Office, Massachusetts

Federal Agencies

U.S. Attorney's Office, Eastern District of California
Federal Bureau of Investigation
DHS – Homeland Security Investigations

International Agencies

National Crime Agency, United Kingdom

3. Community Complaints or Concerns

The District Attorney's Office did not receive any complaints regarding the use of data extraction/examination forensic tools and software during the period covered by this Annual Report.

4. Audits/Policy Violations

Data extraction/examination forensic tools and software were used only in compliance with the Board-approved SUP. Investigators in the District Attorney's Office, REACT Task Force, and authorized investigators employed by outside law enforcement agencies received judicial authorization and/or consent, and obtained supervisor approval before utilizing the data extraction/examination forensic tools and software. All new hires and newly assigned staff are trained on the County's Surveillance Use Ordinance and required SUP. All current District Attorney's Office investigators and REACT Task Force members received training on the County's Surveillance Use Ordinance and District Attorney's Office investigators electronically read and acknowledged the ordinance and SUP as required by our Policy & Procedure Manual. Data retrieved by the data extraction/examination forensic tools and software was retained in conformity with the Board-approved SUP.

The data extraction/examination forensic tools and software do not have embedded audit features, unlike criminal history databases. Supervisors use a variety of methods to ensure that authorized users access and use forensic tools only as authorized by judicial authorization or consent. These safeguards include, but are not limited to, individualized usernames and passwords, mandatory pre-use training, supervisor approval and monitoring, system activity logs, mandatory chain of custody documentation, and secured locations requiring supervisor presence for access. Additionally, investigators complete monthly "stat" sheets that require them to document the number of forensic examinations conducted, which should coincide with their requested access to the forensic room.

Supervisors perform monthly audits of access to the forensic room by reviewing the Forensic Room Log. Depending on the age of the phone, the type of operating system, and the password complexity, it can take days, weeks, or even years to unlock a device. Personnel must abide by the forensic room procedures and complete the log when a device will take longer than the workday to unlock/image. Auditing of the room includes ensuring that any phone connected to the system has the proper documentation.

In addition to supervisors performing monthly audits of the Forensic Room Log, supervisors also conducted four random case file audits to verify the information contained on the log was accurate. There were no detected violations of the Board-approved SUP.

5. Effectiveness

Data extraction/examination forensic tools and software were utilized in numerous criminal investigations and prosecutions during the relevant reporting period. The REACT Task Force relied extensively on these forensic tools and software to properly investigate high technology crimes.

Authorized forensic examinations were performed in large-scale, multi-state, and on-going criminal investigations including, but not limited to, identify theft, organized crime fraud rings, multi-million-dollar fraud schemes, homicides, high technology crimes, gang investigations, network intrusions, and possession of illegal weapons. As a result of data collected by these forensic tools, District Attorney's Office and REACT investigators obtained critical evidence that protected Santa Clara County residents and visitors and resulted in successful prosecutions, additional arrests, and indictments. Additionally, forensic tools were used to locate and recover stolen property and to recover monies stolen from crime victims to be used for victim restitution.

6. Public Records Act Requests

The District Attorney's Office received no Public Records Act requests for information related to the Office's use of data extraction/examination forensic tools technologies.

7. Costs Incurred

The State of California completely funded all of the costs for the data extraction/examination forensic tools and software purchased by the District Attorney's Office REACT Task Force during the reporting period covered by this Annual Report. The State transmitted funds to the County's Trust Fund, and the County transferred those funds to the REACT Trust Fund so they could be used to compensate vendors for products and services. The County is not expected to incur any expenses in the next reporting period.