Surveillance Use Policy

Grayshift GrayKey
San Diego Police Department

PURPOSE

Grayshift GrayKey is a hardware and software tool used by the Forensic Technology Unit to extract cell phone data without altering the data or adding data to the phone.

USE

When proper authority, such as a search warrant or consent form, is obtained, cell phones are connected to the Grayshift GrayKey tool, and the data is extracted from the phone. Grayshift GrayKey is designed to complete the extraction without altering any of the data or adding data to the phone.

Due to the large variety of cell phone models and manufacturers, not all cell phones can be extracted in this way. Only phones that the vendor supports can have data extracted.

- Additional information can be found in the Forensic Technology Unit Manual Version 05.22.2022

DATA COLLECTION

Grayshift GrayKey is capable of extracting call logs, text messages, emails, photos, videos, contacts, browsing history, app data, and location data. GrayKey can also extract data from some social media apps on the phone.

Grayshift GrayKey software can also analyze deleted data and hidden files on a device and can recover data that has been deleted.

The extracted data is then stored on the department's Network Attached Storage (NAS) in Data Systems. Only investigators with a search warrant can access the data controlled by Data Systems.

DATA ACCESS

Only authorized users (criminalists) in the Forensic Technology Unit (FTU) that have completed training and have been authorized by the Quality Manager to perform extractions may use the Grayshift GrayKey tool.

DATA PROTECTION

Grayshift GrayKey software and equipment are stored and maintained in the FTU, a secured office within Police Headquarters. Only authorized users have access to the technology. Each user is required to use a unique login and password to access the software and conduct data extractions.

The Grayshift GrayKey software is not located on department network computers and can only be accessed by logging into a computer with the software installed inside the building. The computer has no internet access and is not accessible by the vendor. Additionally, the software can only be installed through a specific process, it cannot be moved, and the user must be an authorized user with a valid software license. The Grayshift GrayKey software cannot be accessed outside of the Department.

Surveillance Use Policy

Grayshift GrayKey
San Diego Police Department

DATA RETENTION

Other than homicides and violent sexual assaults, where extracted data is kept indefinitely, extracted data is retained based on the statute of limitations for the associated crime or if the case has been adjudicated. Data is purged from the NAS when it is at the end of its retention period.

PUBLIC ACCESS

The data extracted using Grayshift GrayKey technology is only used in criminal investigations and is not available to the public. Copies of the data can only be obtained with a court order or the discovery process.

THIRD PARTY DATA SHARING

Data that has been extracted using Grayshift GrayKey technology is not shared without a court order or other legal proceedings such as discovery. The extracted data is considered confidential, and there is no third-party access or sharing. Grayshift GrayKey does not have access to the extracted data.

TRAINING

Criminalists in FTU who use the Grayshift GrayKey software must complete and pass an extensive training program outlined in the FTU manual prior to using the software.

AUDITING AND OVERSIGHT

FTU maintains a log of all authorized Grayshift GrayKey users that tracks how many times the software was accessed by the user. FTU is also responsible for all Grayshift GrayKey software and granting access to the system.

Data is only extracted via legal authority, such as an active warrant. Department policies, State of California laws, and laboratory policies outline how extracted data is maintained. Misuse of the system would be reported to and investigated by the Department's Internal Affairs unit. Violations of laws, Departments Policies or user agreement terms would subject the department member to discipline and / or criminal proceedings or civil processes.

MAINTENANCE

The Grayshift GrayKey software is controlled and maintained by the vendor and FTU, following laboratory quality policies and department policies. FTU criminalists are responsible for monitoring and updating software when new versions are released. A log documenting all software updates is maintained by the FTU.