GRAYSHIFT

ACCESS TO THE TRUTH

eBook | Vol. 2

GrayKey Stories from the Field

GRAYKEY STORIES FROM THE FIELD

In the field of digital forensics, mobile devices often contain critical information. This information once accessed by GrayKey (a mobile digital forensics tool, by Grayshift), can be beneficial and become evidence. Evidence that can lead to the truth. These are the GrayKey stories from the field.

GRAYSHIFT

Table of
CONTENTS

GRAYSHIFT

THE DATA IS IN THE DETAILS

TYPE OF AGENCY

Large Police Department

TYPE OF CASE

Active Shooter Homicide

CHALLENGE

An active shooter targeted a recreation venue, killing one individual and severely injuring another. After the incident took place, the shooter fled the scene and officers had no way to identify the suspect. Prior to the incident, the suspect gave their mobile devices to a friend so if they did get caught, authorities would not be able to seize the device and therefore find supporting evidence. However, when the shooting took place, the trusted friend panicked, discarded the devices which were located by a witness and turned over to the law.

When a device is in a BFU state, it means the device hasn't been unlocked since its last reboot. BFU extractions can contain limited user data but can still provide useful data for an investigation.

HOW GRAYKEY HELPED

Even though the devices were powered-off, the investigator was able to successfully conduct a Before First Unlock (BFU) extraction. This resulted in user-generated photos that led authorities to successfully identify the shooter. The photos geolocation metadata also helped authorities identify potential hide out locations. The results from the BFU extraction helped authorities successfully located and arrested the shooter.

Geolocation data is found in metadata from multimedia files. It can help identify places or locations where the suspect has been which can be useful in identifying additional places of interest.

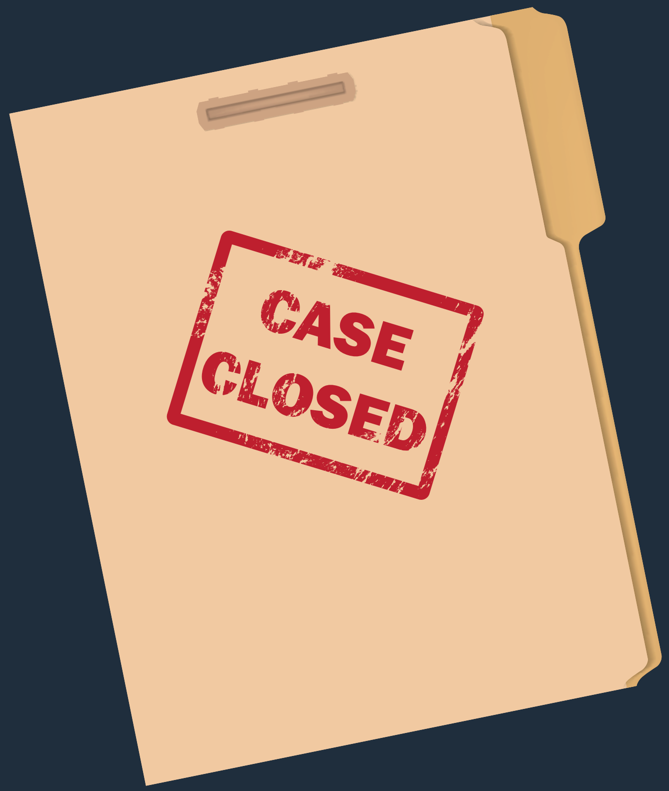
ALWAYS TRY AGAIN

TYPE OF AGENCY

Large Police Department and District Attorney Office

TYPE OF CASE

Homicide



CHALLENGE

A homicide took place, and the main suspect was held in prison while awaiting trial. At the time of the initial investigation, digital forensic investigators did not have GrayKey and were unable to successfully access the suspect's device. Since the device had sat in evidence for over a year, the suspect's attorney requested a motion hearing to request that the suspect's mobile device be released.

HOW GRAYKEY HELPED

The state's prosecutor grew concerned when they heard about the motion hearing. Why, after all this time, did the suspect want their device back? The District Attorney filed for an additional search warrant to examine the device one more time before they released it to the owner. However, this time, investigators had GrayKey. Within minutes of connecting the device to GrayKey, investigators preformed a Full File System (FFS) extraction that helped the District Attorney access the evidence they needed to stop the motions hearing and add incriminating evidence to the original homicide case.

Many GrayKey customers have been able to use GrayKey on cold case investigations where they previously were unable to access the device.

A Full File System extraction is a full physical extraction of the phone's file system.

YOU CAN'T DELETE THE PAST

TYPE OF AGENCY

Mid-sized Sheriff's Department

TYPE OF CASE

Crimes Against Children

CHALLENGE

An online cloud storage provider noticed a user was uploading Child Sexual Abuse Material (CSAM) to their platform. They immediately notified local law enforcement and provided them with user data, including the user's location. Authorities used the information to locate the suspect's residence where they seized a mobile device and other electronics. However, CSAM was not discovered since the cloud storage user account had been deleted.

HOW GRAYKEY HELPED

The investigator connected the device to GrayKey and successfully accessed Keychain data that showed the device had been used to log into the reported cloud storage account. The data showed the exact account user ID, associated email address, and username. In addition, the investigator was able to find login data that showed the exact date and times of when the CSAM had been uploaded to the cloud storage site.

78% of surveyed law enforcement agencies said they are using GrayKey to assist in child Sexual Abuse Material (CSAM) cases.

TechValidate: DFB-767-EAB

CORROBORATING A SUSPECT'S STORY

TYPE OF AGENCY

Mid-sized Sheriff's Department

TYPE OF CASE

Vehicular Homicide Exoneration

CHALLENGE

Law Enforcement officers responded to the scene of a vehicle striking a pedestrian. A mobile device was lawfully seized from the driver of the vehicle who denied actively being on their cell phone at the time of the incident. The driver stated they only had the phone turned on so they could listen to a music streaming service.

HOW GRAYKEY HELPED

When investigators received the device, they connected it to GrayKey, and successfully extracted activity logs from a database within the device. From this information, investigators proved that the music streaming service was the only active application at the time of the accident. They also confirmed the device screen had not been turned on and the device had not been unlocked by the user at the time of the accident. They corroborated this evidence with the GPS locations of the device which showed where the vehicle was in motion near the accident site.

SECURING CONVICTING EVIDENCE ON ANDROID DEVICES

TYPE OF AGENCY

Large Police Department

TYPE OF CASE

Crimes Against Children

CHALLENGE

A police department identified a perpetrator for crimes against children. They obtained and issued a search warrant for the suspect's residence and acquired multiple devices. At the time, investigators did not have the proper license for their GrayKey unit to access the main suspect's device. Because of this, it was suggested that the charges be dropped for the main suspect.

HOW GRAYKEY HELPED

Since time was critical, the agency reached out to Grayshift so they could update their license in order to access the device. The Grayshift team acted quickly, provided the customer with the appropriate license, and the investigator was able to perform an extraction on the suspect's device and discovered CSAM that secured convicting evidence. GrayKey and Grayshift's customer-first culture enabled the investigator to quickly access the device, by providing the customer with what they needed quickly to discover incriminated evidence.

90% of GrayKey customers rated customer support as better than other vendors they have used or evaluated.

TechValidate: 57E-31E-20E

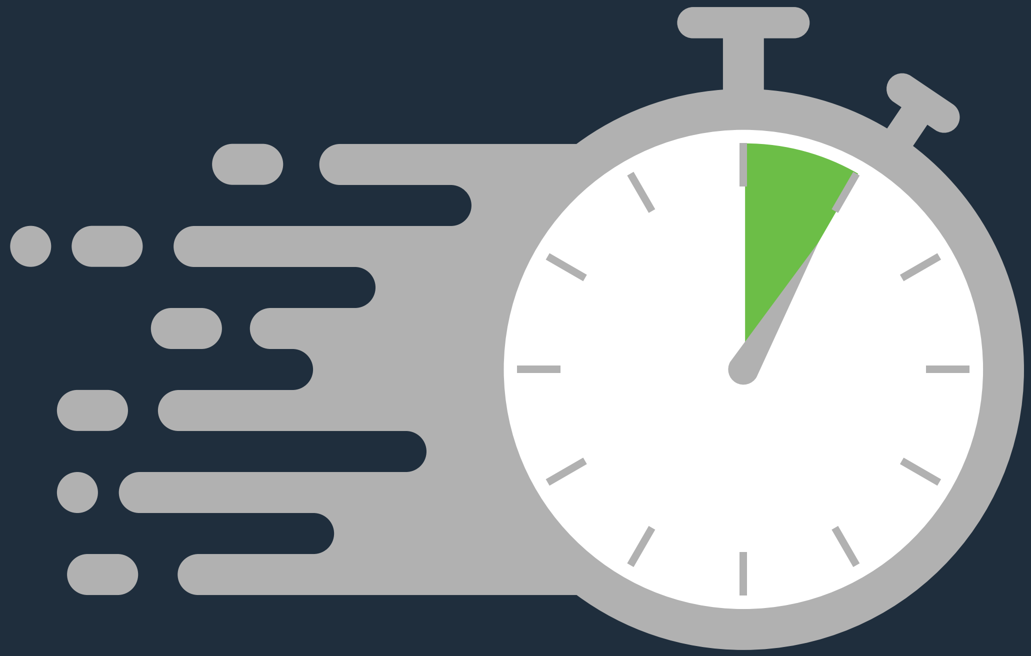
JUST IN TIME

TYPE OF AGENCY

Large Agency

TYPE OF CASE

Kidnapping



CHALLENGE

Authorities were informed of a missing person, and they believed the victim was kidnapped and facing a life-threatening situation. The agency did not have any evidence or location data for the victim. Time was of the essence to locate the victim as their life was in danger. During the investigation, investigators identified a suspect and seized their device.

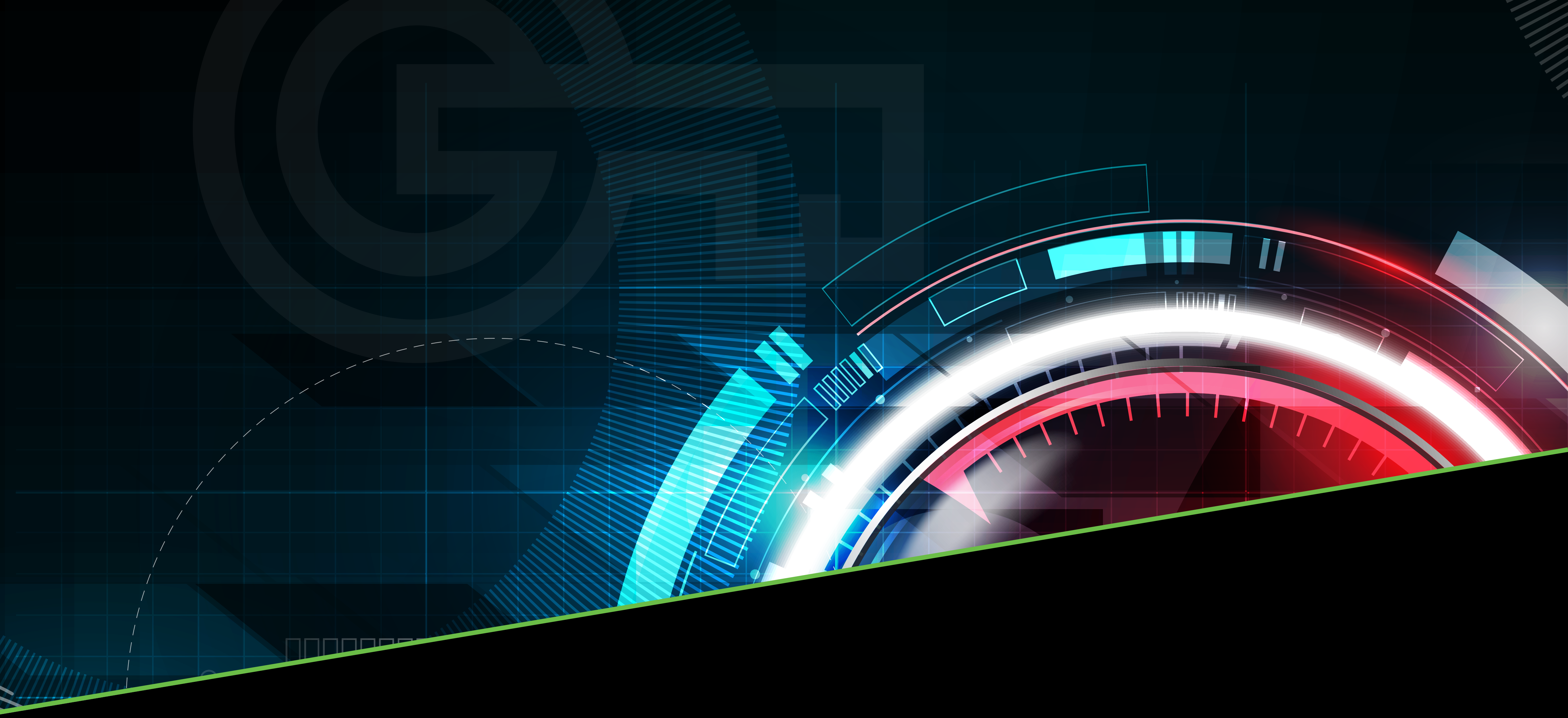
If the device passcode is unknown or the device is powered off, you can use GrayKey Brute Force Actions to discover the passcode.

HOW GRAYKEY HELPED

With GrayKey, the investigators were able to brute force the passcode on the suspect's device and recovered third party application multimedia that helped authorities positively identify the kidnapped victim's location. This multimedia also contained additional information that helped authorities identify contraband. Within an hour of using GrayKey, authorities were able to rescue the victim and return them to safety just in time.

90% of surveyed customers stated they selected GrayKey because of its ability to access and extract data from iOS devices within hours.

TechValidate: CC8-92A-8D4



WANT TO LEARN MORE?

Visit **www.grayshift.com/get-started**

GRAYSHIFT