Ohio Attorney General's Office
Bureau of Criminal Investigation
Investigative Report

2020-3388
Officer Involved Critical Incident - 1062 Oberlin Drive, Columbus, Ohio

Investigative Activity:	Cell Phone Analysis and Review, Digital Evidence Analysis
Involves:	Officer Adam Coy (S), Andre Hill (S)
Date of Activity:	12/22/2020
Author:	SAS Justin L. Root, #149

Synopsis:

On December 22, 2020 at approximately 0126 hours, officers from the Columbus Division of Police responded to the area of 1054 Oberlin Drive on a report of an occupied suspicious vehicle. Upon arrival, officers encountered a subject and a shooting occurred, resulting in the death of one individual. Adam C. Coy was identified as the Columbus Police Officer who fired the shots resulting in the death. The Ohio Bureau of Criminal Investigation was contacted to investigate the shooting. The BCI Cyber Crimes Unit was requested to assist with electronic evidence.

Investigative Narrative:

On December 22, 2020 at approximately 9:00 AM, I (Root #149) arrived at the area of 1054 Oberlin Drive and met with other investigators. SA Aja Chung provided me with a packaged cellular telephone, later designated as BCI CCU Evidence Item 001, that had been collected from the driveway near the decedent. The device had been identified prior to packaging as a black LG cellular telephone. I took possession of the device at approximately 0905 hours and began drafting a search warrant application through the Franklin County Municipal Court. The search warrant application was approved by Judge Jessica G. D'Varga at 10:38 AM on December 22, 2020.

I next met with SA Perry Roeser, who provided me with a consent to search form signed by Dystanie Lydelle, who had provided her Apple iPhone cellular telephone for data extraction and analysis. This item is identified as BCI CCU Evidence Item 002 (reference only). I began by manually reviewing the device to see which applications were running at that time. Open applications included Messenger, Voice Memos, Messages, Calculator, Safari, RealCamera, App Store, Photos, Google Photos, News, Maps, TextNow, Clock, Pinterest, Gmail, and Numbers. The device was connected to a forensic computer running the Cellebrite 4PC forensic extraction tool and a data acquisition was performed. (See below for details.)

I next traveled to the Ohio Bureau of Criminal Investigation's Cyber Crime Unit in London, Ohio

with BCI CCU Evidence Item 001. I reviewed the lock screen of the device, which was found to be displaying a message alert for the gmail account '[redacted]'. The phone was taken off the cellular network connected to a forensic tool capable of extracting data from Android devices. BCI CCU Item 001, however, was not supported for data acquisition and no extraction could be obtained.

On December 30, 2020, I met with Columbus Police Sergeant Terry McConnell at the Columbus Police headquarters, 120 Marconi Blvd., Columbus, Oh. Sgt. McConnell had arranged for CPD cruisers 9030 and 9031 to be brought in. Each of these cruisers was equipped with a Panasonic WJ-VR30 cruiser camera system designed to activate either manually or when emergency lights and/or sirens are activated. Although the cameras were not recording actively on the night of the incident, the decision was made to attempt to review the storage media with a forensic tool to see if any residual data might have been present. One Panasonic SSD cartridge (Model WJ-VR3002) was removed from each of the cruisers and collected as BCI CCU Item 003 and 004. Items 003 and 004 were transported to the Ohio Bureau of Criminal Investigation's Cyber Crime Unit in London, Ohio for later analysis.

On January 12, 2021 at approximately 1450 hours, I obtained search warrants from Judge Jenifer French of the Franklin County Court of Common Pleas for Charter Communications records relating to telephone number [redacted] and T-Mobile records relating to telephone number [redacted]. I also obtained a search warrant for the physical cellular telephone used by Adam Coy near the time of the incident, which was believed to have been assigned telephone number [redacted]. On that same date at 1519 hours, and pursuant to an agreement between counsel for Adam Coy and the Ohio Attorney General's Special Prosecutions section, I took possession of Mr. Coy's cellular telephone from employee Athena Denney of attorney Mark Collins' law office. This device was subsequently designated BCI CCU Evidence Item 005. I left with Ms. Denney a copy of a search warrant issued for the device by Judge Jenifer French of the Franklin County Common Pleas Court. The device was placed into airplane mode to remove it from all networks and transported to the Ohio Bureau of Criminal Investigation's Cyber Crime Unit in London, Ohio for data acquisition and analysis.

Due to concerns that had arisen that the telephone number listed on the search warrant for the device might not be accurate, a new search warrant was presented to Judge French identifying the device by its International Mobile Equipment Identity (IMEI), which had been recorded at the time the device was provided by Ms. Denney. The new search warrant was forwarded to Mr. Coy's attorney's office electronically. The original search warrant was returned unexecuted. Data was extracted from the device as described below. Due to the potential for privileged material to exist on this device, arrangements were made with Prosecutor Justin Lovett of the Jackson Ohio Prosecutor's Office for that office to conduct a privilege review on a full data extraction set to remove privileged material prior to the content being reviewed by investigators. A copy of the extracted data in a human-readable format was provided to Prosecutor Lovett on July 12, 2021.

On February 25, 2021, a search warrant was issued by Judge Julie Lynch of the Franklin County Common Pleas Court for telephone records from Verizon pertaining to telephone number [redacted], and for records from Facebook, Inc. pertaining to the Facebook account andre.m.hill (100000945067113).

Records received pursuant to these search warrants were forwarded to case investigators for review and analysis.

References:

001 - Mobile Phone - Black LG
002 - Mobile Phone - Black/Silver Apple iPhone SE A2275
003 - Hard Disk Drive - Gray Panasonic ARB-256SSD WJ-VR3002
004 - Hard Disk Drive - Gray Panasonic ARB-256SSD WJ-VR3002
005 - Mobile Phone - Black Samsung Galaxy note 8

Forensic Review:

Item 001: Item 001 is a black LG cellular telephone recovered from the scene of the shooting and believed to belong to Andre Hill. The device was locked with an unknown password at the time of its transfer from SA Chung to me (SA Root) and could not be placed into airplane mode. The device's SIM card was removed to disconnect it from the cellular network in order to preserve evidence on the device from the potential of a remote event. At that time, the device was found to not contain a microSD card.

Pursuant to a search warrant, Item 001 was transported to the Ohio Bureau of Criminal Investigation's Cyber Crime Unit for data acquisition and analysis. When removed from its case, the device was found to display a sticker on the back identifying the model as LM-K500UM. A separate sticker identified the device's International Mobile Equipment Identifier (IMEI) as 354591111821468.

The device was connected to a forensic tool often capable of bypassing security restrictions on cellular telephones but was found to be unsupported. No data could be extracted from the device. The device was inspected manually at its lockscreen. The displayed time and date were correct. The lockscreen displayed a notification of 25 new messages relating to the email address <biggdre73@gmail.com>. No other information could be obtained from the device.

Item 002: Item 002 is an Apple iPhone SE model D79AP, firmware 12,8, running iOS 13.6.1. The device's International Mobile Equipment Identifier (IMEI) was found to be 356463107422594. Its International Mobile Subscriber Identity (IMSI) was found to be 310240132529947. Its serial number was found to be FFWD86BGPLJN. The MSISDN (*i.e.*, the dialing number) for this device is [redacted]. The ICCID was found to be 89012 40132 72529 9475. Pursuant to consent of the owner, data from the device was extracted on site for subsequent analysis.

The device was powered on when received. It was placed into airplane mode and connected to a forensic computer running the Cellebrite UFED 4PC forensic extraction application for data acquisition. An advanced logical data extraction was obtained from the device.

The data extraction file was loaded into the Cellebrite Physical Analyzer data analysis utility. A timeline review of the device was then conducted. Relevant messages and audio files were extracted from the device and forwarded to the case investigator. These files include a spreadsheet demonstrating a timeline review of the device and an audio file created near the time of the shooting. A video filmed after the shooting was also extracted and forwarded to the

case investigator.

On September 2, 2021, at the request of the special prosecutor, a full Cellebrite forensic report was generated for this device. That report is saved in HTML format and will be provided to the special prosecutor and the defense. A copy will be retained in the Cyber Crime Unit.

Item 003: Item 003 is a 256GB Panasonic solid state drive, model ARB-256SSD, model number WJ-VR3002, serial number [redacted]. This device was removed from Cruiser 9031 on December 30, 2020 to determine whether any data could be recovered from it using forensic tools that was not available to the Columbus Police Department using the standard video review and recovery functionality of the cruiser camera system.

The device was connected to a hardware write-blocker and connected to a forensic computer running a forensic utility capable of extracting video footage from video recording systems. The drive was found to be encrypted by the system manufacturer. No additional data could be extracted.

Item 004: Item 004 is a 256GB Panasonic solid state drive, model ARB-256SSD, model number WJ-VR3002, serial number [redacted]. This device was removed from Cruiser 9030 on December 30, 2020 to determine whether any data could be recovered from it using forensic tools that was not available to Columbus Police Department using the standard video review and recovery functionality of the cruiser camera system.

The device was connected to a hardware write-blocker and connected to a forensic computer running a forensic utility capable of extracting video footage from video recording systems. The drive was found to be encrypted by the system manufacturer. No additional data could be extracted.

Item 005: Item 005 is a Samsung SM-N95OU Galaxy Note 8. It bears the International Mobile Equipment Identifier (IMEI) of 353639090218072. This device was searched pursuant to a search warrant. The SIM card was removed and was found to be marked with Verizon markings and bearing the ICCID number 89148 00000 56727 60949. A 32GB microSD card was removed from the device, placed in a write blocker, and imaged. The image was verified by its cryptographic hash value. The image file was loaded into the X-Ways forensic utility. Allocated data was exported to conduct a privilege review. Common file types (*e.g.*, .jpg) were carved and added to the exported data to conduct a privilege review.

The device's time was checked and found to be accurate. The device was ensured to be in airplane mode and the passcode provided, [redacted], was used to unlock it. The settings were accessed and the device was found to already be displaying the "developer options" option. The developer options tab was accessed and "USB debugging" and "stay awake" were enabled. The lock screen option was changed from "PIN" to "none" to facilitate data acquisition. The device was then connected to a forensic computer running the Cellebrite data extraction tool and a physical acquisition was obtained. The physical data extraction was then loaded into the Cellebrite Physical Analyzer data parsing utility and a "Cellebrite Reader" report was generated.

The Cellebrite Reader report and data extracted from the microSD card were provided to Jackson County Prosecutor Justin Lovett for privilege review. Prosecutor Lovett was instructed

on how to navigate the utility and how to tag items as privileged. Upon conclusion of his review, a subsequent redacted report will be generated, omitting the privileged materials, and provided to the case investigator.

Conclusion:

Items 001 through 005 were analyzed in connection with this investigation. No data could be obtained from Item 001, Item 003, or Item 004. Data extracted from Items 002 and Item 005 were parsed into human-readable formats for review. The human-readable format for Item 005 has not yet been reviewed and has instead been provided to Jackson County Prosecutor Justin Lovett to conduct a privilege review. Once that review is completed, a subsequent report of only unprivileged information will be provided to the case investigator.