Louisville Metro Police Department

Standard Operating Procedures	SOP Number: 8.59
	Effective Date: 09/07/23
	Accreditation Standards:
Chapter: Field Operations	
Subject: Digital Forensic Unit	

8.59 DIGITAL FORENSIC UNIT

8.59.1 POLICY

The Digital Forensic Unit (DFU) is responsible for the examination and analysis of handheld cellular devices and laptops, the submission and analysis of historical call detail records, electronic surveillance, and social media/networking digital platforms, vehicle infotainment systems requests, and the analysis of digital evidence for investigations. The DFU also maintains and updates the digital search warrant database on the Louisville Metro Police Department (LMPD) Intranet and acts as a liaison for LMPD personnel with local and federal law enforcement partners.

8.59.2 RESPONSIBILITIES

The DFU is a specially-trained digital evidence unit that assists investigators, prosecutors, and partner agencies with the collection, analysis, and training in the field of digital evidence. DFU personnel provide members with forensic support and advice for the preparation of search warrants, the seizure of digital evidence, and the recovery and examination of relevant evidence.

DFU personnel are responsible for duties, including, but not limited to, the following:

- Basic and intermediate data extraction techniques from cellular devices to achieve manual, logical, file system, and physical (invasive and non-invasive) extractions.
- Mobile device chip-offs.
- Performing post-extraction analysis and advanced search techniques using Physical Analyzer, in a forensically sound manner.
- Submitting electronic surveillance requests to social media companies, such as Facebook, Instagram, Google, etc., and assisting with investigations from the Pen Register Trap and Trace (PRTT) evidence.
- Submitting, analyzing, and examining Call Detail Records (CDRs) and cell site dumps.
- Submitting electronic surveillance, mapping, and analysis for LMPD units.
- Submitting and handling tech-related search warrants, while assisting personnel with an analysis of information (e.g., Apple, Google, T-Mobile, AT&T, Verizon, etc.).
- Identifying, acquiring, and analyzing data obtained from vehicle infotainment systems.
- Assisting investigators with the analysis and planning of digital evidence seizure and processing for investigations.
- Utilizing software for computer analysis and extraction.
- Maintaining and updating the digital search warrant database on the LMPD Intranet.

When situations occur where exigent circumstances exist and DFU personnel are needed immediately, a member's supervisor may contact the DFU Commander for assistance from DFU personnel. Exigent circumstances where DFU personnel may be requested to assist include, but are not limited to, the following:

- Submitting requests to cellular providers
- Submitting requests to social media companies (e.g., Facebook, Instagram, etc.)
- Forensic examination of handheld cellular devices
- Vehicular infotainment systems

8.59.3 SEARCH WARRANTS AND OTHER LEGAL AUTHORITY FOR DIGITIAL EVIDENCE

Officers are not authorized to conduct a warrantless search of a cellular device, or any other form of digital media, incident to arrest (*Riley v California*). Warrants to search a cellular device, or any other form of digital media, must state, with a particularity, the evidence of information upon the device for which there is probable cause to search and seize such data.

Officers are not authorized to obtain CDRs without a search warrant (*Carpenter v United States*) Search warrants sent to cellular providers (e.g., T-Mobile, AT&T, and Verizon) will be submitted to the DFU, which is responsible for submitting the search warrant and the evidence will be returned and analyzed.

Officers are not authorized to use the real time cell site location information of a citizen's telephone number without a search warrant, absent probable cause and an articulable exigent circumstance (*Commonwealth v Reed*). Search warrants related to pen registers and live location information will be submitted to the DFU. If exigent circumstances exist, officers must be able to articulate the facts supporting the exigency, and a search warrant will be written within a reasonable amount of time.

Digital evidence search warrants should be written in accordance with current LMPD policy. The investigator must be able to articulate a link between the electronic data to be searched and seized and evidence of, or related to, criminal activity.

If an investigator, who is otherwise lawfully on the premise, develops probable cause to believe that an electronic device may be seized, and that device is located in an area in which an individual has a reasonable expectation of privacy, a search warrant (or warrant exception) will be required to enter that location and seize evidence. A forensic examination of the device or storage media generally requires a separate search warrant than the warrant to search a particular location where the device may be found.

A warrant exception, such as consent or exigent circumstance, must exist for an investigator to search digital evidence without a warrant. "Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury" (*Riley, supra*).

Templates or "go-bys" for digital evidence search warrants can be found on the LMPD Intranet by clicking on the "Investigative Apps" button.

8.59.4 REQUESTS FOR DATA EXTRACTION FROM A CELLULAR DEVICE

Members who are requesting data extraction from a cellular device will login to the Cellebrite Guardian Investigator Portal at https://prelog-louisville-ky.guardian.cellebrite.cloud/login.php to submit a new lab request. Members who require access to the Cellebrite Guardian Investigator Portal will have their supervisor contact the DFU Commander to request a user login.

Investigators will complete the lab submission and attach a copy of legal authority, such as a search warrant, court order, written consent, etc. Once the submission has been completed, the investigator will print the label provided by Cellebrite Guardian associated with their cellular device and submit it to the DFU.

Once the lab request has been submitted for forensic examination of a cellular device, the member will then bring the evidence label and cellular devices to:

8.59.4 REQUESTS FOR DATA EXTRACTION FROM A CELLULAR DEVICE (CONTINUED)

- The DFU, located at 834 E. Broadway, 5th floor.
- If a search warrant has been granted after-hours (e.g., 1600-0700 hours) and there are no exigent circumstances for DFU personnel to be called in, the cellular device will be secured at the LMPD CSU office, located at 701 E. Ormsby Ave.
- Once inside the main entrance to the CSU office, the member will place the cellular device and evidence label inside of a cellular device locker.
- The locker will be secured and the key placed inside of the lockbox located on the wall next to the cellular device locker. The investigator will send an email to DigitalForensic@louisvilleky.gov, indicating the locker where the evidence has been secured.

Members will be able to monitor the status of their lab submission through the Cellebrite Guardian Investigator Portal. Once the submission has been completed by a member of the DFU, an email will be sent to the member, indicating the lab request has been completed. The notification will include the original unit case number(s), the DFU case number, and the name of the DFU personnel. DFU personnel will also provide the member with the following:

- The DFU's Forensic Investigation Report.
- A copy of the requested evidence or electronic image from one (1) of the DFU's applications.
- An analysis of the evidence that was obtained.

Once DFU personnel have completed the request, the member will take custody of the cellular device, located at the DFU, and will refer to SOP 11.2 for the purposes of storing evidence in the LMPD Evidence and Property Unit (EPU).

8.59.5 ELECTRONIC SURVEILLANCE AND CALL DETAIL RECORDS

Electronic surveillance (cell phone pings and pen registers) is an important investigative tool to track the location of cellular devices. Electronic surveillance results in financial costs to the department from cellular/social media providers. As a result, electronic surveillance should only be used for felony investigations. Electronic surveillance is primarily utilized by the Major Crimes Division and the Criminal Interdiction Division (CID). All electronic surveillance requests require an official search warrant affidavit, search warrant, and if applicable, an order to seal.

All non-exigent cellular device electronic surveillance requests will be submitted through the DFU by sending an email to DigitalForensic@louisvilleky.gov. All exigent cellular device electronic surveillance requests will be approved by a commanding officer and coordinated through the on-duty MetroSafe supervisor. DFU personnel may be called for assistance. For the purposes of this policy, acting sergeants will not be considered commanding officers. Exigent electronic surveillance requests will only be conducted in situations involving an imminent risk of death or serious physical injury.

Cellular device electronic surveillance orders will not extend beyond 30 days unless approval has been obtained from the DFU Commander. Any electronic surveillance request order exceeding 30 days, without prior approval, will be denied.

All CDR requests will be submitted through the DFU to the respective cellular providers and require an official search warrant affidavit, search warrant, and order to seal (if applicable). Requested data will be returned to the

8.59.5 ELECTRONIC SURVEILLANCE AND CALL DETAIL RECORDS (CONTINUED)

DFU. Geolocation and CDR analysis/examination will be completed only by trained DFU personnel at the request of the lead detective.

Unless otherwise approved by the DFU Commander, social media PRTT search warrants will only be utilized for the following offenses:

- Any Criminal Homicide or Death Investigation
- Assault in the First, Second, or Third Degree
- Wanton Endangerment in the First Degree
- Strangulation
- Unlawful Imprisonment in the First Degree
- Kidnapping
- Rape in the First Degree
- Sodomy in the First Degree
- Sexual Abuse in the First Degree
- Arson in the First Degree
- Robbery in the First Degree
- Escape in the First Degree

Search warrants for other online based companies may be submitted through the DFU. Digital evidence returned from social media and other technology companies can be processed and analyzed for court proceedings though forensic tools from DFU personnel.

8.59.6 REQUESTS FOR DATA EXTRACTION FROM A VEHICLE INFOTAINMENT SYSTEM

Members who are requesting the forensic examination of motor vehicle infotainment systems will send an email to DigitalForensic@Louisvilleky.gov.

Members must first determine if a motor vehicle infotainment system is supported by the software used by the LMPD. This can be accomplished by contacting DFU personnel. Once it is determined the motor vehicle infotainment system is supported, the member can proceed in obtaining legal authority, or consent, for the infotainment to be processed.

The member should attempt to obtain a key for the vehicle to be processed. Some vehicles are unable to be processed without a key. If a key is not obtained for the vehicle, members will contact the examiner to see if the vehicle can be processed without it or for other options to obtain a key for the vehicle.

DFU personnel who are receiving a request for analysis must receive a copy of legal authority, such as a search warrant, court order, written consent, etc., from the requestor.

The member will then contact DFU personnel to arrange the removal and processing of the infotainment.

Once DFU personnel have completed the request, the member will take custody of the infotainment system (if not placed back in the vehicle) and will refer to SOP 11.2 for the purposes of storing evidence in the LMPD EPU.

8.59.7 KENTUCKY REGIONAL COMPUTER FORENSIC LABORATORY (KRCFL)

The KRCFL provides high quality digital forensic services and assistance to any law enforcement agency with jurisdiction in the state of Kentucky, including the seizure and examination of computers, computer systems, computer media, and cellular devices. The KRCFL is an American National Standards Institute (ANSI) National Accreditation Board (ANAB)-accredited laboratory, guaranteeing examiner qualifications and quality control procedures. Forensic examiners offer court testimony explaining how they conducted their examinations and what they discovered as a result.

The KRCFL will maintain a chain of custody for evidence (e.g., computer equipment, media, software, and related peripherals) submitted to the laboratory for examination (KACP 27.1).

To request assistance from the KRCFL, the member will call (502) 423-6740 to schedule an appointment. The office is located at 440 North Whittington Parkway, Burhans Hall, Room 255, Louisville, KY 40222. The hours of operation are from 0800 to 1600 hours, Monday through Friday.

8.59.8 DIGITAL MEDIA EVIDENCE

Digital Media Evidence can be defined as evidence contained within any form of magnetic or electronic media. Digital evidence is found in, but is not limited to, computers/laptops, cellular devices/smartphones, digital cameras, hard drives, solid state drives (SSDs), universal serial bus (USB) drives, recordable discs, compact discs (CDs), digital versatile/video discs (DVDs), Blu-ray discs (BDs), flash memory cards, magnetic tape, secure digital (SD) cards, subscriber identity module (SIM) cards, Internet of Things (IoT) devices and other digital data provided by cellular carriers, online companies, and electronic devices.

- Any investigator who encounters digital evidence that they believe may contain evidence of a crime should determine if there is probable cause or request consent for the seizure of the system or device.
- If probable cause is established, a search warrant will be obtained and/or an Electronic Device Consent Search form (LMPD #21-0007) will be completed for the seizure of the data to be examined. If there is an imminent articulable basis to believe the electronic evidence may be destroyed, altered, or overwritten (i.e., exigent circumstances), the evidence should be safeguarded and secured pending a search warrant or warrant exception (e.g., consent)
- Unless exigent circumstances require it, digital and electronic evidence media should not be accessed without first consulting with DFU personnel.
- If circumstances require access to evidence prior to an acquisition or examination, the investigator will document the date, time, and description of evidence viewed or accessed, and will provide that written detail to DFU personnel.
- To accommodate helpful citizens, electronic devices that are voluntarily provided by bystanders and uninvolved parties are only to be searched as reasonably necessary and at the discretion of the lead investigator.

When handling all digital evidence, investigators must be mindful of what they access. Alterations of the mobile device's settings as described in the following are a necessary procedure that allows for proper acquisition of the mobile device's data for the case investigation. Manually searching the mobile device will cause changes in the evidence (e.g., browsing through text messages can change "unread" message flags to "read"). When collecting a mobile device, extreme care must be taken to isolate the device from any network (i.e., cellular, Wi-Fi, and/or Bluetooth) connections. If additional questions arise, contact the DFU for assistance.

8.59.8 DIGITAL MEDIA EVIDENCE (CONTINUED)

When legally permissible, the investigator should make a concerted effort to get the password, personal identification number (PIN), or other security measures for the mobile device.

8.59.9 EVIDENCE RETENTION

The DFU will maintain custody of evidence (e.g., cellular device, laptop, media, software, and related peripherals) submitted for forensic examination.