8

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 3 June 5, 2013

TO: Concerned Personnel

FROM: Commanding Officer, Major Crimes Division

SUBJECT: DIGITAL FORENSIC ANALYSIS REQUEST PROCEDURES

Background: This Order establishes a standardized approval process for digital forensic analysis requests. Additionally, the Order defines the method for referring digital forensic cases to the Orange County Regional Computer Forensic Laboratory (OCRCFL). Prior to referring digital forensic cases to the OCRCFL, Major Crimes Division (MCD) personnel shall obtain approval from the Commanding Officer, MCD.

Definition of Terms:

Digital Evidence: Any computer, hard drive, cell phone, tablet, optical disk, flash storage device, or any other device capable of storing evidence in digital format.

Mobile Device: Any personal communication or computing device including, but not limited to, cellular phones, tablet computers, smart phones, GPS navigation devices, digital book readers, and digital music players.

Digital Forensic Analysis: A branch of forensic science encompassing the examination and recovery of material stored on digital devices relative to criminal and terrorist activity. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover the examination of all devices capable of storing digital data.

Orange County Regional Computer Forensics Laboratory: A Regional Computer Forensics Laboratory (RCFL) is a one stop, full service forensics laboratory and training center that is devoted entirely to the examination of digital evidence in support of criminal investigations, such as, but not limited to

- Homicide
- Child pornography/crimes against children
- Crimes of violence
- Terrorism
- The theft or destruction of intellectual property
- Financial, property, or Internet crimes
- Fraud
- Trade secret theft.

Major Crimes Division Participation

An RCFL is a partnership between the Federal Bureau of Investigation (FBI) and other law enforcement agencies operating within a geographic region. Organizations that enter into a Memorandum of Understanding with the FBI become participating agencies in the RCFL.

In this capacity, they assign personnel to staff the laboratory, and in return, they and their respective agencies receive access to digital forensics examination and advisory services. Each member of a participating agency will receive sophisticated technical training that is provided to FBI's certified computer forensics examiners. Major Crimes Division is a participating agency for the Orange County branch of Regional Computer Forensic Laboratories. As a participating agency, MCD assigns one person from the Division to the OCRCFL. In return, the Los Angeles Police Department is afforded the following on-going benefits:

- Unlimited access to the mobile device data extraction kiosk located in the front lobby area of the OCRCFL
- Four (4) full-service digital forensic case referrals per month to the OCRCFL to be assigned to a forensic examiner for analysis

Mobile Device Data Extraction Kiosk

The OCRCFL maintains a mobile device data extraction kiosk that is open to any law enforcement officer that is a member of a participating agency. This is a self-service area that contains specialized data extraction tools for mobile devices. The tools are guided and do not require the user to have an expertise or specialized training in mobile device forensics. No appointments are necessary to utilize the capabilities of the kiosk nor is there a limitation to the frequency of use or total usage by participating agency personnel.

Note: For special handling beyond what the kiosk tools can provide (i.e. passcode lock, deleted file recovery, etc.), the mobile device will require submittal to the OCRCFL for full-service examination and will count toward the (4) monthly full-service allotments.

Employee's Responsibility. The procedure for submitting digital evidence for forensic analysis to the OCRCFL is as follows:

1. The investigating officer shall complete an LAPD Letter of Request detailing the nature of the request. This letter shall be on Department letterhead and be addressed to Supervisory Special Agent, OCRCFL Lab Director, from the Commanding Officer, Major Crimes Division. Ensure that the specific device(s) is listed along with the type of information sought. Additionally, include a brief synopsis of the case and what time sensitivity issues exist – if any – in the event case prioritization is necessary. The OCRCFL will not accept direct requests from investigating officers. The Letter of Request shall then be submitted to the Officer-in-Charge of the Anti-Terrorism Intelligence Section Cyber Unit for review before it is sent to the Commanding Officer for approval. Once approved, the signed letter will be returned to the investigating officer who will be responsible for submitting it to the OCRCFL via email at ocsr@rcfl.gov.

2. In addition to the Letter of Request, the OCRCFL Request for Service form must be completed by the investigating officer and emailed to ocsr@rcfl.gov. A copy of the form can be downloaded from http://www.ocrcfl.org/Downloads/Documents/OCRCFL_Request_for_Service.pdf. This form will also be available on the Major Crimes Division "P" drive. The LAPD Letter of Request and the OCRCFL Request for Service form can be emailed together. An OCRCFL representative will contact the investigating officer when the request has been reviewed and processed.

3. Submit documentation in support of the search to the OCRCFL. Whether the authority is a search warrant or consent to search, without legal justification, forensic services will not be rendered. This documentation can be sent electronically via email along with the other documents or submitted at the time the hardware is delivered to the OCRCFL for analysis.

4. The case agent must transport the evidence to the OCRCFL at 3800 W Chapman Ave, 8th floor, in the city of Orange. Hours of operation are 0800-1600 hours, Monday-Friday. To allow an appropriate amount of time to intake the evidence, arrive no later than 1500 hours. A hard copy of the above-listed documentation can accompany the evidence if a digital copy was not emailed prior.

Supervisor's Responsibility. The Cyber Unit Supervisor, or assigned designee, shall ensure that the Letter of Request is thoroughly and properly completed. The supervisor, or assigned designee, shall then evaluate the information contained within the letter and determine if submittal to the OCRCFL is justified and appropriate based on the information contained in the letter. If approved, the supervisor, or assigned designee, shall ensure that a buck slip is completed and the referral is appropriately entered into the tracking log. The letter shall then be forwarded to the Commanding Officer for final approval and signature. If the matter is urgent, telephonic approval can be granted by the Cyber Unit supervisor or assigned designee.

Commanding Officer's Responsibility. The Commanding Officer, Major Crimes Division, shall review the information contained within the form and make final determination that all conditions justifying referral to the OCRCFL were met at the Employee and Supervisor levels. The approved and signed Letter of Request shall be returned to the investigating officer for submittal to the OCRCFL.

Computer Crimes Unit

The Computer Crimes Unit (CCU) of Commercial Crimes Division is the Department's designated digital forensic service provider. In the event a referral to the OCRCFL is denied, the investigating officer shall submit the case to CCU for handling. Providing the requisite criterion is met (i.e. a crime has occurred and legal authority to search exists), CCU will accept the case and will conduct the digital forensic examination based on priority and the order in which the request was received.

STEVEN S. SAMBAR, Captain
Commanding Officer
Major Crimes Division