311 CYBER CRIMES INVESTIGATIONS

I. DISCUSSION: The internet has become a ubiquitous part of the daily lives of most people, and with it has come digital evidence that extends well beyond traditional "computer crimes." Frequent interaction with digital devices creates a trail of evidence in a wide variety of crimes, but such evidence may not always be easy to recognize or secure. Ever increasing access to the internet and social media by children exposes them to online predators who are adept at exploiting children. The Tampa Police Department recognizes the need to maintain investigators with the specialized training and equipment necessary to identify and collect digital evidence, as well as conduct the type of investigation necessary to properly respond to and prevent the online exploitation of children. Those functions will be the responsibility of the Tampa Police Cyber Crimes Squad.

II. DEFINITIONS:

A. Digital Forensics: The practice of identifying, preserving, recovering, analyzing and presenting facts about digital evidence found on computers, mobile devices, or other digital media devices.

B. ICAC Task Force: The Internet Crimes Against Children (ICAC) Task Force is a national network of coordinated task forces representing over 4,500 federal, state, and local law enforcement and prosecutorial agencies. These agencies are continually engaged in proactive and reactive investigations and prosecutions of persons involved in child abuse and exploitation involving the internet. Tampa Police investigators assigned to the Central Florida ICAC Task Force will be part of the Cyber Crimes Squad.

C. Criminal Tracking: The component of the Cyber Crimes Squad responsible for investigations involving Sexual Predators as defined by F.S. § 775.21(4) and Career Criminals as defined by state and federal law.

D. NCMEC: the National Center for Missing and Exploited Children (NCMEC) serves as the national clearinghouse and comprehensive reporting center for all issues related to child victimization. Reports taken by the NCMEC are forwarded via the ICAC Data System to the appropriate regional task force / affiliate agency for investigation. The Cyber Crimes Squad serves as the department's liaison with NCMEC and has primary responsibility for investigating NCMEC reports within the City of Tampa.

III. PROCEDURES

A. Duties and Responsibilities of ICAC Investigators Assigned to the ICAC Task Force:

1. ICAC Task Force investigators assigned to the Cyber Crimes Squad will be under the supervision of the Cyber Crimes Sergeant and are responsible for investigating the online exploitation of children. This will include conducting reactive investigations of cyber tips assigned by NCMEC and proactive investigations to target online predators.

2. As part of their assigned duties, ICAC investigators will:

    a. Conduct latent investigation of cases involving the online exploitation of children reported to the Department by the NCMEC and assigned by a Cyber Crimes supervisor.

    b. As determined by the Cyber Crimes Sergeant, conduct latent investigation of incidents in which the primary offense is one of the following:

        i. Possession of Child Pornography, FS § 827.071(5);

        ii. Transmission of Child Pornography by Electronic Device, FS § 847.0137;

        iii. Transmission of Harmful Material to Minors, FS § 847.0138;

        iv. Traveling to Meet a Minor, or other offenses involving a minor under FS § 847.0135; or

        v. Any incident which in the opinion of the Criminal Investigations Division Commander, involves elements requiring specialized training or equipment to the extent that it cannot be handled by another latent investigative squad.

    c. Conduct proactive investigations to target offenders that are attempting to exploit minors online.

    d. Conduct surveillance as necessary for assigned cases.

    e. Conduct investigations related to juvenile sex trafficking.

    f. Comply with current ICAC Operational and Investigative Standards as defined by the United States Department of Justice.

    g. Receive training in ICAC investigations.

h. Assist other units throughout the department when cases involve digital evidence that require specialized training or experience.

B. Duties and Responsibilities of Digital Forensics Detectives

1. Detectives assigned to Digital Forensics will be under the supervision of the Cyber Crimes Sergeant and will be primarily responsible for conducting forensic examinations of digital devices (e.g. computers, cell phones, etc.) Digital Forensics detectives will possess the necessary skills and training to assist other units in the department with investigations involving digital evidence.

2. As part of their assigned duties, Digital Forensics detectives will:

a. Conduct forensics examinations of digital devices (computers, cell phones, memory cards, etc.).

b. Accurately document the results of examinations via forensic reports and supplements.

c. Provide examination results to requesting investigators and assist with the interpretation of those results when necessary.

d. Maintain certifications in digital forensics.

e. Review forensic examination requests in Versadex to ensure legal authority exists and comply with scope of search.

f. Assist with search warrants where significant digital evidence may be present, if requested.

g. Maintain a log of all digital examinations.

h. Assist other units throughout the department with cases that involve digital evidence requiring specialized training and experience.

C. Duties and Responsibilities of Criminal Tracking Detectives

Detectives assigned to Criminal Tracking will be under the supervision of the Cyber Crimes Sergeant and will be primarily responsible for latent investigations regarding violations of sexual predator, sexual offender, and career criminal registration.

Criminal Tracking detectives will conduct investigations and adhere to the guidelines outlined in SOP 309 Sexual Predators and Offenders, and SOP 307.7 Career Criminals.

D. Patrol Responsibilities

Officers may encounter digital evidence in the field in a wide variety of offenses. They should be aware that digital evidence is inherently volatile, and should take steps to ensure its preservation by adhering to the requirements of SOP 338, Seizure of Computer Equipment.

If large or complex computer systems are encountered, officers should first consult with a Digital Forensics Detective prior to attempting to collect evidence.

E. Forensic Examination Requests

1. All requests for digital forensics examinations will be made through Versadex.

2. The investigator making the request will first attach documentation of their authority to search the device to the report (i.e. signed search warrant, electronic consent form, or valid legal exception) or provide it to Cyber Crimes by other means.

3. The investigator making the request will complete the Versadex attachment titled "Digital Forensic Examination Request." The investigator should fill out as much information as possible, including passcode if known, TPD property tag number, make and model of device, evidence sought, etc.

4. The case will then be routed as a notify to the Cyber Crimes handle (HCYBER) for assignment to a Digital Forensics examiner.

5. Property removed from evidence by a Digital Forensics examiner will be returned to evidence by the examiner. Cyber Crimes will store extraction results in accordance with current procedures. A copy of the examination results will be made available to the requesting investigator.

6. Cyber Crimes will not examine devices that do not have a TPD property number and a fully completed Versadex Digital Forensics Examination Request documenting the property number. Exceptions may be made in exigent circumstances upon approval of the Cyber Crimes supervisor.

a. In circumstances where a device was directly provided to an examiner (e.g. exigent consensual searches), the device may be returned directly to the requesting investigator or designee, as approved by the Cyber Crimes supervisor.

b. Each unique device should be packaged and tagged separately. Cyber Crimes will not accept multiple devices in one package.

Supersedes SOP 311, dated 6/20.