OVERVIEW

The use of computers and digital data to commit crimes is growing at tremendous rates. The Scottsdale Police Department understands the importance of investigating crimes involving such technology.

SEARCH and SEIZURE of COMPUTERS and DIGITAL DATA STORAGE DEVICES

1. While sworn and un-sworn personnel are involved with discovering and impounding potential digital evidence, only qualified CCU staff complete the forensic search of the device.

2. CCU staff are available to assist with the most recent verbiage necessary for obtaining a search warrant for digital data and during the execution of a search warrant.

INVESTIGATIONS

Computer Crimes and Financial Crimes detectives investigate identity theft to include, but not limited to, the following when appropriate:

1. Reviewing the DR and conducting follow-up inquiries for clarification/expansion of information.

2. Checking PACE, Triple I, criminal records, and MVD for activity.

3. Contacting the FTC Consumer Sentinel Law Enforcement Network at sentinel@ftc.gov and searching the database for investigative leads.

4. Contacting other involved or potentially involved law enforcement agencies to collaborate and avoid duplication. Agencies include, but are not limited to:
   a. Federal law enforcement, such as the U.S. Secret Service, the Federal Bureau of Investigation, and the U.S. Postal Inspection Service whether or not the victim has filed a report with them.
   b. Any state and/or local enforcement agency where the victim has filed a crime report or where there is an indication that identity theft took place.

5. Scottsdale Detectives
   a. Investigate cases if the victim resides within
Scottsdale and the victim's identity is being used within Maricopa County. If the victim's identity is being used outside Maricopa County, forward a copy of the DR t to the appropriate law enforcement agency for follow-up investigation.

b. Conduct follow-up investigations for other law enforcement agencies located outside Maricopa County, when the victim's identity is being used within Scottsdale.

c. Conduct follow-up investigations of in-progress and just occurred identity theft cases committed within Scottsdale.

PROCEDURE

ASSIGNED EXAMINER

1. Obtains and secures evidence prior to and during the examination process.

2. Maintains the chain-of-custody of evidence during the examination process.

3. Attempts to protect and maintain the integrity of stored data by using procedures and techniques in compliance with current forensic standards and practices. Organizations of relevance include: IACIS, LEVA, and SWIGIT (Scientific Working Group on Imaging Technology)

4. Document the initial state of examined evidence and any subsequent changes resulting from the examination process.

5. Document hardware, software, procedures, and methodology used during the examination process.

6. Prepare an official report detailing the examination process and resultant findings. Impound a copy of the examination report and provide a copy to the assigned case detective/officer.

7. Evidence files, forensic images, and report documentation files generated as the result of an examination conducted by detectives currently working with the DPS Computer Crime Laboratory, are archived and maintained by the Computer Crimes Unit.