TYLER POLICE DEPARTMENT
GENERAL ORDER

DIGITAL FORENSICS **17.700**

REVISED **EFFECTIVE 11/1/10**

17.701 PURPOSE

A. The purpose of this order is to establish responsibility and procedures for the seizing, processing and examination of digital and high technology evidence by the Tyler Police Department.

B. The processing of digital evidence shall be conducted in accordance with General Order 17.100 CRIME SCENE PROCESSING unless otherwise noted in this policy.

17.702 DEFINITIONS

A **Forensic Computer Examiner (FCE)** – one who has received specialized training in the processing and recovery of digital evidence

B **Technology Sergeant** – Sergeant assigned by the Chief of Police to oversee the technology functions of the department including the Digital Forensics function.

17.703 ETHICS

Forensic Computer Examiners will operate under strict ethical guidelines, including:

1. Maintain the highest level of objectivity in all forensic examinations and accurately present the facts involved.
2. Thoroughly examine and analyze the evidence in a case.
3. Conduct examinations based upon established, validated principles.
4. Render opinions having a basis that is demonstratively reasonable.
5. Not withhold any findings, whether inculpatory or exculpatory, that would cause the facts of a case to be misrepresented or distorted.
6. Never misrepresent credentials, education, training, experience, or professional organization membership status.

17.704 ASSIGNMENTS AND DUTIES

A. The Digital Forensics function will be performed by Crime Scene Investigators, Forensic Computer Examiner(s), and the Technology Sergeant.

B. The responsibilities of the Technology Sergeant will consist of:

1. Ensure Forensic Computer Examiners receive the training necessary to maintain their professional knowledge in the field.
2. Prepare the annual budget for the function.
3. Order equipment and supplies required for the function. Oversee the maintenance and proper storage of specialized equipment.
4. Ensure support is maintained for the hardware and software utilized by the function.
5. Routinely review activities relating to digital evidence examinations performed by the Forensic Computer Examiner(s).
6. Make examination assignments to the Forensic Computer Examiner(s).
7. Coordinate and conduct training for personnel on the proper procedures to employ when seizing and preserving electronic evidence.

8. Determine the cause of failed validation tests on examination tools. Remove any tools from use in investigations that are determined to not be functioning properly through the validation process. Take necessary steps to correct the issue with the problematic tool.

C. The responsibilities of the Forensic Computer Examiner(s) will consist of:

1. Perform investigative analysis of all computers and electronic storage devices excluding cell phones in any case where evidence or information pertinent to an investigation may be stored on the computer or electronic media.
2. Provide technical assistance and guidance for members of the Department in the proper safeguarding and collection of evidence stored in electronic form.
3. Develop and deliver training for the department in the continually evolving and emerging area of high technology crime.
4. Provide assistance to investigators in the preparation of search warrants and search warrant affidavits.
5. Validate and document validation of the software and hardware tools used in digital forensic investigations. Should any tool fail to pass a validation test, document the results and provide the documentation to the Technology Sergeant.
6. Keep current on changes in technology, software, hardware used for examinations and methods used to conceal, encrypt, or destroy computer data.
7. Seize computers or other digital evidence when the location of a search and seizure is a place of business.
8. Assist on the seizure of computers or other digital evidence as needed when the location of a search and seizure is not a place of business.

D. The responsibilities of the Crime Scene Investigator will consist of:

1. Process crime scenes where evidence is believed to exist in a digital format on computers or other electronic storage media. Digital evidence will be preserved in accordance with this policy. No evidence will be moved or altered should the investigator reasonably believe the actions will alter or hamper the evidentiary value. A FCE shall be consulted in all of these cases to ensure case integrity.
2. Notify the Technology Sergeant when the computer or digital evidence to be seized is at a place of business or is critical to the operations of a business.

E. The responsibilities of field personnel will consist of:

1. When a Patrol Officer believes that a crime scene investigation is needed and digital evidence is included in the items to be seized, the officer shall contact a supervisor who may request the dispatching of a Crime Scene Investigator or an Intermediate Crime Investigator.
2. When securing the scene involving computers, officers shall:

    a. Immediately isolate any suspects from the computers.
    b. **DO NOT** allow anyone (especially the suspect) to touch the computer or keyboard.
    c. If the officer sees a destructive script or program running on a computer the officer should disconnect the power cord from the back of the computer.
    d. Never turn a computer on.
    e. Never open files or folders or run programs on the computer. Doing so could destroy evidence critical to an investigation.

17.705 SUPPLIES

A. The Technology Unit shall provide the Crime Scene Investigators and Forensic Computer Examiners with the necessary equipment and assistance for the performance of their duties related to the recovery and examination of digital evidence.

B. The Technology Sergeant shall conduct a periodic inventory examination to ensure that an adequate amount of supplies are available for the processing and examination of digital evidence.

C. Requests for these supplies will be made to the Technology Sergeant.

17.706 SUPERVISION

A. The Forensic Computer Examiner shall be under the supervision of the Technology Sergeant. When collecting, processing, examining, or reporting on forensic computer evidence

B. When a Forensic Computer Examiner is assigned to a crime scene, the FCE will be in charge of how digital evidence is gathered and processed unless countermanded by the Case Investigator or supervisor in charge of the investigation.

C. If the FCE determines that the processing of any particular item might cause damage to the item or cause harm to digital information stored on a computer or other electronic storage device, the investigator or supervisor in charge of the investigation shall be notified.

D. If the requesting officer or supervisor still desires that the item(s) be processed or seized, then the requesting officer or supervisor shall assume full responsibility for any damage that may occur.

17.707 FORENSIC COMPUTER EXAMINER AVAILABILITY

A. The Computer Forensics Examiner or the Technology Sergeant shall normally be available for consultation or response on a 24-hour basis.

B. An on-call schedule will be developed by the Technology Sergeant and placed in the on-call folder so that supervisory personnel are informed of who is on the call out list.

17.708 COLLECTION AND PRESERVATION OF DIGITAL EVIDENCE

The following procedures apply whenever data residing on a computer system or digital media is sought as evidence in an investigation. Computers or digital media seized as fruits of a crime shall be handled in accordance with General Order 17.100 CRIME SCENE PROCESSING.

A. When it is determined that a computer is to be seized and processed, the investigator or supervisor in charge of the investigation should contact an on-duty Crime Scene Investigator or Intermediate Crime Scene Investigator. If none are on duty, the on-call Crime Scene Investigator should be contacted.

B. Unless exigent circumstances exist, no department member, except a Crime Scene Investigator, Intermediate Crime Scene Investigator, Forensic Computer Examiner, or Technology Sergeant shall power off, disconnect, power on, or access a computer system or electronic media system that is to be seized. Computer systems can and have been found to contain destructive programs that can alter and destroy evidence. Accessing files and programs can also alter file access dates that may be critical items of evidence.

C. The responding Crime Scene Investigator or Intermediate Crime Scene Investigator will process the scene. Processing will include:

1. Collect all relevant evidence

2. Photograph the computer or other electronic devices or storage media prior to disconnecting any wires or other connections.
3. If the computer is on, photograph what is on the screen as a means of capturing what the suspect may have been doing prior to the seizure.
4. If the computer appears to be in "sleep mode", slightly move the mouse or hit the "Shift" key on the keyboard to "wake" it.
5. Properly mark all computer evidence:

    a. Affix identifiable mark labels with the department case number included to hardware (monitor, computer tower, laptops, printers, external hard drives, other peripherals) in such a manner as to minimize the potential for damage of the property.
    b. Count and package similar storage media (floppy discs, CD's, DVD's, etc.) and itemize by type on the Property report for the evidence.
    c. Storage media removed from the computer or attached drives at the time of seizure should be listed separately on the Property report and clearly labeled as recovered from the computer or attached drive.
    d. Do not use ballpoint pens when marking floppy disks as damage to data can occur. Felt markers or a label maker should be used.
    e. Avoid the use of plastic bags as plastic can build up a static charge which can destroy data in magnetic based storage devices. Paper or anti-static bags for the packaging of magnetic media will be made available to Crime Scene Investigators for use in their Crime Scene toolkits.

6. If a computer or electronic device is seized, attempt to locate and include in the seizure any power supplies or batteries for the devices. Paperwork associated with the device, passwords, ledgers, etc.
7. If the computer is a laptop, remove both the power cord and battery.
8. Cell phones and PDA procedures:

    a. If the device is on, leave it on.
    b. If the device is off, leave it off.
    c. Seize the power supply and charger if available.
    d. Recharge the device as soon as possible after seizure to prevent data loss from a dead battery.

9. The Crime Scene Investigator should have the on-call Forensic Computer Examiner respond to the scene in the following situations:
10. The Crime Scene Investigator is unfamiliar with the type of digital evidence and the appropriate way to seize it.
11. The Investigator or Supervisor in charge of the investigation believes the case is of a nature that the seizure should be made by a Forensic Computer Examiner.
12. Special tools or knowledge is required for the seizure.
13. The scene is so large, additional assistance is needed.
14. Seizure of the computer, electronic equipment, or digital media would substantially impact a place of business.

D. The Forensic Computer Examiner will contact the Technology Sergeant in cases where the Department lacks the equipment or expertise necessary to complete the seizure. The Technology Sergeant will obtain necessary assistance from outside resources to complete the seizure and/or investigation.

E. Computers, storage devices, or other hardware seized will be submitted to the Property unit.

F. A Forensic Computer Examiner will check out items from Property as needed for examination.

G. Items checked out for examination but not currently being examined will be kept in the Technology Office in the locked property cabinet. The door to the Technology Office will be kept closed and locked when the room is unoccupied.

H. The temporary storage locker in the Technology Office is not to be used for long term storage of computers, storage media, or hardware. When an examination is finished, the item being examined will be returned to the Property Unit.

17.709 EXAMINATION

A. Prior to the examination, the Forensic Computer Examiner shall do the following:

1. Review the authority for the search and scope of the search (Consent to search form, search warrant / search warrant affidavit, etc.)
2. Review the incident report(s) available for the incident.
3. Obtain any necessary clarifications from the case investigator concerning scope of the search, authority for the search, and evidence to be searched for.

B. The Forensic Computer Examiner should minimize the use of original digital evidence stored on hard drives or other digital media. To accomplish this limited use, forensic images of the original evidence should be created and verified before the examination process. Write-blocking technology should be utilized on original evidence to ensure that the original evidence is not altered in the imaging process. In special circumstances where original media must be examined due to hardware configurations or operating system limitations, the Forensic Computer Examiner will document the steps of the examination performed on the original evidence.

C. The Forensic Computer Examiner shall make all efforts to accomplish the following during the examination of a seized computer or storage media:

1. Ensure the original media and data are maintained in their original, unaltered state.
2 Ensure no unauthorized writes are made to the media by viruses, booby-trap defense schemes, the operating system, write-back applications or by other inadvertent means.
3. Recover, unlock, and access relevant deleted files, hidden data, password-protected files and encrypted files as allowed by examination authority (search warrant language, subpoena language, user consent, etc.)
4. Examine unallocated and slack space for relevant data.
5. Provide report(s) of findings to the requesting investigator. Reports detailing the FCE's investigation in narrative form should be completed in the Department's record's package. Additional reports containing files or printouts should be given to the case investigator and a back up maintained in the Technology Office. When an alternative report format is used, a Department Record's system narrative must be submitted as well so anyone reviewing the case will know of the alternative report's existence.

17.710 CASES INVOLVING CHILD PORNOGRAPHY

In cases where images are discovered that depict possible child pornography, employees shall comply with the following steps to ensure that there is no unnecessary distribution or reproduction of the images:

A. Original evidence found to contain child pornography will only be released from the Property unit after approval by the Chief of Police or designee.

B. When printed images of child pornography are needed for court or grand jury, the images will be delivered in an envelope sealed with evidence tape and clearly marked as child pornography. Any images must be signed for by investigators. Digital Media containing Child Pornography will be conspicuously marked with the warning, "Contains Child Pornography".

C. Images of child pornography may be electronically duplicated by a Forensic Computer Examiner at the direction of the Technology Sergeant for the purpose of sending them to the National Center for Missing and Exploited Children.

D. Any investigator, district attorney, or other law enforcement representative that is provided a copy of child pornography is responsible for the destruction of such images at the conclusion of the case. Proper destruction shall include shredding printed images and optical media (CD's, DVD's, BluRay's, etc.)

E. Upon request from the prosecuting attorney or court order, a Forensic Computer Examiner will make evidence containing suspect child pornography available to be reviewed by the defense attorney or defense expert at the Technology Office. The FCE will remain with defense personnel during this review. Suspects will not be allowed into the Technology Office.

Approved: 11/1/10