

# THE RALEIGH POLICE DEPARTMENT

**1110-05**

## SEARCHES OF COMPUTERS AND ELECTRONIC DEVICES

### PURPOSE

Investigations involving the use of computers or other electronic devices are specialized, and require technical processes to successfully resolve. The initial reporting, subsequent investigation, and collection or processing of evidence in these cases may be technical and complex. This procedure will provide guidelines to first responding officers and detectives to expedite the proper resolution of computer-related crime cases.

### VALUES REFLECTED

This directive reflects our values of *Service and Integrity*. By following the guidelines contained here we will demonstrate our commitment to combat crimes in which computers and other electronic devices are involved. We will also demonstrate our use of the best available practices and maximize the use of available equipment and technology.

### UNITS AFFECTED

All Units/All Personnel

### REFERENCES/FORMS

DOI 1110-08 "Searches and Seizures: Investigative Stops and Frisks"  
"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,"  
Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice

Attachment A: Consent to Search Computer and Media, Consent by Owner

Attachment B: Consent to Search Computer and Media, Consent by Third Party with Access to Computer

Attachment C: Consent to Search Computer and Media, Consent by Additional Parties

Attachment D: Request for Computer Examination

Attachment E: Request for Video Forensic Exam

May be Released to the Public

---

Effective Date: 10-06-14  
Prepared By: C.L. Deck-Brown  
Chief of Police

---

Supersedes: 07-09-07  
Approved By: Ruffin Hall  
City Manager

## **GENERAL POLICIES**

The investigation of many crimes may ultimately involve computer-related evidence. First responding officers or detectives may continue to investigate most aspects of these crimes. However, analyzing computer systems for criminal evidence is a highly technical process requiring expert skills and a properly controlled environment. Because of this, a member of the Department's Technical Assistance Response Unit (TARU) who has completed a prescribed training process in Computer Forensics will complete the actual search of physical devices.

In the interest of regional problem-solving and inter-agency cooperation, personnel from the Department's TARU may also provide assistance to other local Law Enforcement agencies in computer-related investigations. However, such assistance must be approved by a Raleigh Police Department supervisor, and will always be secondary to RPD matters.

## **DEFINITIONS**

Investigations involving computers or other electronic devices inescapably involve the use of technical jargon. The following common terms may be encountered during the initial or follow-up investigation of computer-related crimes. A basic definition is provided to assist officers and detectives in communicating with victims, suspects, or witnesses:

- Network – Two or more computers that are somehow connected to share resources. Networks may be large, such as the Internet, or very small, such as a home network.
- Server – A server is a computer that provides some service for other computers connected to it via a network. Any computer, including a laptop, can be configured as a server. A server provides shared resources such as e-mail, file storage, Web page services, and print services for a network.
- IP Address – Internet Protocol address. A numeric address assigned to a networked computer, which uniquely identifies that individual computer. Currently, the IP address is in a format consisting of four segments, with each segment containing one to three digits, for example 198.168.10.1
- ISP – Internet Service Provider. A company that provides a connection to the Internet for an individual computer user. Examples are America Online (AOL), AT&T, Time Warner, etc.
- Instant Messaging or IM – A service that allows live "chat" sessions between computer users. Examples of programs that provide this service are AOL Instant Messenger, Yahoo! Messaging, IRC, or MSN Messenger. IM sessions are not usually recorded, and therefore are not usually available for court order requests.
- Email – Electronic mail sent via the internet. These are not "live" communications, and the term should not be used in place of Instant Messaging. Emails are sometimes stored on some computers, and can be retrieved with a court order or search warrant.
- Email Header – The first section of an email message that documents the path the message made through the network. The header is, by default, not shown by most email programs. However, the program can be made to show the header. The header may show the IP

address of the originating computer and is instrumental in determining the sender of a message.

- Hard Drive – A physical device that stores information for a computer. Stored information is in a semi-permanent state. Most hard drives are within the computer's case (internal), but some may be external. Some computers may have more than one hard drive. Computer forensics is performed on the hard drive of a computer, making it the focus of a physical seizure.

## **SEARCH AND SEIZURE**

Computers or other electronic devices may contain evidence of a crime. As such, they may be seized as physical evidence. The general requirements for the seizure of computers or other electronic devices are the same for other types of physical evidence. See RPD DOI 1110-8 "Searches and Seizures" for guidance in the legal aspect of computer seizures. Other specific considerations for computer-related investigations follow:

### **Search Warrants**

The TARU can provide templates for computer-related search warrants or court orders to assist detectives. Generally, a court order is all that is required for subscriber information on ISP or email accounts. However, a search warrant is usually required for email content.

If a search warrant is required for the seizure of a computer, the following guidelines should be observed:

- In order for a Computer System's peripherals and storage media to be seized and searched, one or more of the following must be supported by the probable cause statement in the search warrant:
  - The computer itself is contraband, evidence or an instrumentality or fruit of a crime, or
  - The computer is a storage device for evidence of a crime
- If prior knowledge exists that a computer falls into one of the above described categories, then the computer, along with facts justifying seizure and forensic analysis, should be included in the original search warrant intended to gain entry into the house or building in which the computer is maintained. The computer can then be seized and later searched. In this case, a separate search warrant is not needed for the computer.
- If no search warrant exists, and officers are otherwise lawfully inside a structure and subsequently develop probable cause that a computer might be evidence, they should isolate the computer and obtain a search warrant for the computer. Once a search warrant is obtained, the computer may be seized and searched.
- Upon a return of service for a search warrant on a computer, the officer can simply record the computer's physical identification (model, serial number, etc.) and "digital evidence" (for anything that is subsequently retrieved from the analysis of the hard drive) on the

inventory. A listing of files that the examiner subsequently recovers from the hard drive is not necessary on the search warrant's inventory.

- Special care should be used when applying for a search warrant on a computer that may be used in legitimate publishing (authors, columnists, etc.). These are usually protected items that cannot be seized. Officers should check with the Police Attorney's Office if they have any questions.
- If during the actual forensic examination of a computer system, the examiner encounters evidence of a new crime not covered by the original search warrant, it is essential that analysis stop immediately and a supplemental search warrant be obtained to expand the scope of the search to include the newly discovered crimes.

### Consent Searches

If a suspect or victim provides consent to search a computer, the following guidelines shall be followed:

- Written consent is preferred over oral consent.
- Consent search forms that are specifically designed for computer consent searches are available on Polshare (attachments A, B, C). A regular consent search form should not be used for this purpose.
- All computer searches shall be made in the RPD computer forensics lab. On-scene examinations are technically complicated, and create undesirable variables. On-scene examinations are not done except in special situations and then only by properly trained Forensic Examiners. Therefore, the person granting consent should understand that their computer must be retained by RPD for a period of time in order to properly examine it.

### Collection of Evidence

The search scene should be secured for the officer's physical safety. Computers or other electronic devices are to be considered as evidence and treated the same as any other crime scene items such as fingerprints, blood or weapons. The following guidelines shall be followed:

- Suspect(s) must not be allowed to remain near any computers. A single keystroke could launch a program that would permanently destroy digital evidence. In addition, some computers can be controlled through remote devices, such as a wireless mouse. Therefore, suspects should not be allowed to retain any electronic devices during the search.
- Under no circumstances should officers turn on, boot up or attempt to conduct their own search of the contents of a suspect computer. Turning a computer "on" can alter hundreds of digital files, and possibly destroy digital evidence.
- In addition to written documentation, photographs should be made of the computer's original state, especially the cabling in the rear of the computer. If the computer is "on," a photograph should be taken of the monitor's screen before it is powered down.

- If the computer is “on,” the officer’s supervisor should contact the TARU supervisor for direction on proper collection.
- If a Computer Forensic Examiner is not available to assist in the seizure of the computer, the hardware should be photographed both front and back and the power plug should be pulled from the back of the computer, not the wall outlet. This abrupt power down method prevents any possible terminal programs that may destroy evidence from initiating. It also prevents certain temporary files from being deleted.
- If a computer remains “on” after pulling the power cord (usually due to an internal power source), the officer should push the computer’s power button and hold it in for about six to eight seconds. This should power off the computer, regardless of internal power sources.
- When seizing a computer system, all attached and wirelessly accessible components, including the monitor, keyboard, mouse and power cables, as well as any other attached peripherals should be seized. Software installation media and any paper documentation for hardware or software should be seized as well.
- Some computers may have unique devices used to read or store data. Examples are tape drives, ZIP drives and external hard drives. If these devices exist, they should be seized (including any cables or connectors) in addition to the computer case.
- Computers may contain physical evidence in addition to digital evidence. If fingerprints, DNA, etc. are a concern in an investigation, then the appropriate accessories should also be collected for physical processing.
- When collecting the computer, officers should be sure to look closely in the immediate area for additional information or evidence. Frequently, user names, passwords, and hardware security devices can be found hidden under keyboards, or otherwise stored near the computer.
- The internal components of computers are fragile. Computers and evidence within them can be damaged by physical trauma, static electricity, magnets, and moisture. Care should be taken to avoid exposing the computer evidence to these hazards during collection, transportation, and storage.
- Occasionally, other electronic storage devices may be seized for evidence. These devices may be mobile telephones, “palm” computers, pagers, etc. When these devices are seized, any associated power cords or docking accessories should be seized. If a laptop computer is seized, its power cord should always be collected.
- When seizing a laptop computer, remove the battery first then disconnect the power supply. This ensures complete disconnection of all power sources to the laptop. It is important that the power cord always be collected. Power supplies are often proprietary to the manufacturer and may be required to access the laptop for further analysis.

## **INVESTIGATION**

### **Physical Data Examination**

After collecting computer evidence, a detective will usually require a forensic exam on the recovered digital media. This can be accomplished by a Computer Forensic Examiner, who is attached to TARU. A "Request for Computer Examination" form should be completed and submitted to the Computer Forensic Examiner (see attachment D).

Generally, the examination technique used by the Computer Forensic Examiner is a two-step process. This process involves imaging the Original Digital Evidence, then reviewing the Duplicate Digital Evidence.

During the imaging process, an exact bit-for-bit copy is made of the subject's digital media. Detectives should understand that this imaging process may be a matter of hours, or days, depending on the size of the media involved and the type of imaging performed. The forensic examination is then completed on the imaged copy of the subject's media.

Different techniques are used to obtain pertinent evidence from the image of the suspect's media. However, the Computer Forensic Examiner is not the assigned case detective. For this reason, the examiner will only have the case details that are provided on the "Request for Computer Examination" form. Therefore, it is important that the case detective provide relevant case information on this form. After imaging, Original Digital Evidence will be returned to RPD evidence as soon as practical. Duplicate Digital Evidence created in the RPD forensic lab will be stored in the Computer Forensic lab's Duplicate Digital Evidence Storage Room.

### **Interviews**

During suspect or victim interviews, it is important for officers to obtain and document certain technical information to aid in the successful resolution of a computer crime-related case. Some examples follow:

- Instant messaging usernames
- Email accounts
- Internet Service Providers
- Encryption software type and file passwords, if applicable
- Physical description of computer (Desktop, laptop, etc.)
- Operating system (Windows, Linux, etc.)

Officers should determine whether anyone else had access to the computer (children, spouses, etc.).

If a victim has an email message that needs to be collected for a police report, the victim should be instructed to not delete the email. If the victim is local and has the technical knowledge to do so, the original extended header information should be included with the printed email. If the victim

does not have the technical knowledge, or is reporting the crime over the telephone, he or she should be asked to await instructions from a member of TARU.

**Consent to Search Computer and Media**

**Consent by Owner**

**RALEIGH POLICE DEPARTMENT  
CONSENT TO SEARCH**

I, \_\_\_\_\_, hereby give my consent to the removal of the below indicated equipment and the complete forensic analysis of:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(include general description of all items being submitted for analysis, including internal storage media and removable storage media)

This equipment was voluntarily provided by me to Raleigh Police Department personnel.

I am aware that the requesting officer does not have a search warrant. I am allowing this forensic analysis of my own free will. I understand that I am allowing access to all data present on this computer and related media. The above computer, computer equipment, and storage media is used:

☐ exclusively by me

☐ jointly by myself and \_\_\_\_\_

I am the owner of this equipment and, as such, have complete access and use of it.

Signed:		Date/Time:	
---------	--	------------	--

Witness: \_\_\_\_\_ Date/Time: \_\_\_\_\_



**Consent to Search Computer and Media**

**Consent by Third Party With Access to Computer**

**RALEIGH POLICE DEPARTMENT  
CONSENT TO SEARCH**

I, \_\_\_\_\_, hereby give my consent to the removal of the below indicated equipment and the complete forensic analysis of:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(include general description of all items being submitted for analysis, including internal storage media and removable storage media)

This equipment was voluntarily provided by me to Raleigh Police Department personnel.

I am aware that the requesting officer does not have a search warrant. I am allowing this transfer of possession and forensic analysis of my own free will. I understand that I am allowing access to all data present on this computer and related media.

The above computer, computer equipment, and storage media is used:

☐ exclusively by me

☐ jointly by myself and \_\_\_\_\_

While I am not the owner of this equipment, I have complete access and use of it and its components.

Signed:		Date/Time:	
---------	--	------------	--

Witness:		Date/Time:	
----------	--	------------	--

**Consent to Search Computer and Media**

**Consent By Additional Parties**

**RALEIGH POLICE DEPARTMENT  
CONSENT TO SEARCH**

I, \_\_\_\_\_, hereby waive any privacy interests that I might have to any data that might be on:


(owners personal computer, enter identifying information, including internal storage media & removable storage media).

I am aware that this equipment was voluntarily provided by

--	--

(owner)

to Raleigh Police Department personnel for the purpose of conducting a forensic examination of the equipment. I am aware that the requesting officer does not have a search warrant. I am executing this waiver of my own free will. I understand that it is possible that any data on this equipment may be accessed through the forensic examination.

The above computer, computer equipment, and storage media belongs to:

\_\_\_\_\_  
(owner)

and is used jointly by myself and:

\_\_\_\_\_  
(other relevant parties)

Signed:		Date/Time:	
---------	--	------------	--

Witness:		Date/Time:	
----------	--	------------	--

Attachment D  
DOI 1110-05

<b>Raleigh Police Department Computer Forensics Lab</b> <b>Request for Computer Examination</b>		Date Received in Lab	By (initials)
Today's Date	Agency Case #(s)	Computer Forensics Lab Case #	

Examination Requested by	Agency	Rank / Position	PSN	Contact / Phone #'s
<small>Name - PLEASE PRINT:</small>				

<b>SEARCH AUTHORITY : ATTACH COPIES OF DOCUMENTS AUTHORIZING SEARCH</b>			
Consent <input type="checkbox"/>	Court Order <input type="checkbox"/>	Search Warrant <input type="checkbox"/>	Abandoned Property <input type="checkbox"/>

Suspect(s) – Last, First, MI	DOB	Victim(s) Last, First, MI	DOB
<small>PLEASE PRINT:</small>		<small>PLEASE PRINT:</small>	

Offense	Date of Seizure

Please identify the types of evidence / information to be searched/ recovered:				
	X		X	
Financial Records		Word Processing/Text Documents		[Other – Please be specific]
* Internet History & log files		Child Porn		
* Email Files		Check-writing programs, credit card info		

Item #	Evidence ID / Bar Code #	Item Description	Serial Number	Special Instructions

Upon completion of forensic examination, RPD evidence items will be returned to the RPD Evidence Room for secure storage. A detailed report of findings will be returned to submitting officer/detective.

Effective:

Evidence from outside agencies will be returned directly to submitting officer with detailed report of findings.

**Brief Synopsis of case:**

---

---

---

---

---

---

---

**Requested keywords, numbers, or other data related to case (to aid in search process)**

\* Note: For Internet- and email-related investigations, please identify any known screen names, ISPs (Internet service providers) and other pertinent information for suspects and victims.

---

---

---

---

---

---

---

### **General Instructions – Completion of Request for Laboratory Examination Form**

- All seized evidence must be appropriately processed through your agency's evidence division prior to submission to RPD Computer Forensics Lab.
- Please do not place evidence tape directly on Computers or any other seized media such as floppy disks, backup tapes, CD's, etc. These items should be bagged and labeled in accordance with crime scene / evidence handling guidelines.
- It is important to identify what you expect/hope to find as evidence on the computer; please be as detailed as possible when completing this form. Please attach additional sheets if necessary.
- **Please attach a copy of your search warrant, or consent search form and, if from any agency other than RPD, please attach a copy of your case report.**

RPD Supervisor: _____	
Date Approved/Assigned: _____	PRIORITY NUMBER _____ Due Date: _____
Assigned Examiner: _____	

Attachment E  
DOI 1110-05

<b>Raleigh Police Department Computer Forensics Lab</b>  <b>Request for Video Forensic Exam</b>		Date Received in Lab	By (initials)
AGENCY		Computer Forensics Lab Case #	
<b>Case Number:</b>			

All tapes must be in RPD evidence prior to making this request - Submit all requests to Cyber Crimes Unit

Officer /  
Detective  
Making  
Request:

Crime / Class: \_\_\_\_\_

Date / Time that  
tape/CD was placed  
in evidence:

Date / Time of this  
request: \_\_\_\_\_

Physical description of tape /  
CD: \_\_\_\_\_

Tape/CD received from NAME: \_\_\_\_\_ BUSINESS: \_\_\_\_\_

Is tape damaged? ☐ Yes ☐ No

Is tape cued to event? ☐ Yes ☐ No

Type of Device recording Event \_\_\_\_\_

DATE / TIME of Recording Device \_\_\_\_\_ / \_\_\_\_\_

Actual DATE/TIME Comparison \_\_\_\_\_

(Compare the date/time indicated on the recording device with the date/time on a cell phone or other reliable source, do they match or is the recording device using an incorrect date/time stamp?)

Describe significant event on tape (be specific, include date/ time of event):	

What service are you requesting (still pictures,  
video shorts, etc.)? \_\_\_\_\_

**Effective:**

Contact #s for assigned Detective:	(W):		District:	
	(C):			
Detective's Supervisor:				
Evidence Returned To:			Date / Time Returned:	

**This section to be completed by TARU personnel**

Digitize: ☐ 1:1

☐ 2:1

Products Produced:

☐ \_\_\_\_\_ Single Photos (tiff)

☐ \_\_\_\_\_ Sequenced Photos (tiff)

☐ \_\_\_\_\_ AVI Files

☐ \_\_\_\_\_ Power Point

☐ \_\_\_\_\_ VHS Tape (analog)


Date Completed: \_\_\_\_\_

Total time spent on assignment: \_\_\_\_\_ Hours \_\_\_\_\_ Minutes

RPD Supervisor: \_\_\_\_\_

Date Approved/Assigned: \_\_\_\_\_

Due Date: \_\_\_\_\_

Assigned Examiner:

--	--