

Directive	Electronic Evidence	700-4	1 of 9
Effective Date	January 1, 2010		



Wilkesboro Police Department

Electronic Written Directives Document

I. PURPOSE

The purpose of this directive is to provide guidelines for the collection of electronic evidence.

II. POLICY

It shall be the policy of the Wilkesboro Police Department to provide all members with guidelines and procedures for the proper collection and preservation of computer evidence.

When a computer is unexpectedly discovered as part of a crime scene or a search, call a supervisor for further instructions. Unless otherwise directed, do nothing to the computer equipment. If the computer is to be seized refer to seizure instruction in this policy.

III. DEFINITIONS

- A. **Computer Evidence:** Images, audio, text and other data that can be easily altered or destroyed but may be indications of a crime.
- B. **Probable Cause:** A reasonable ground of suspicion supported by circumstances sufficiently strong in themselves to warrant a cautious and prudent officer to make a similar judgment.

IV. PROCEDURES

- A. **Recognizing Potential Evidence:** The computer may be contraband, fruits of the crime, a tool of offense, or a storage container holding evidence of the offense.
- B. **Answers to the following questions will help determine the role of the computer in the crime:**
 - 1. Is the computer contraband or fruits of the crime, i.e. was the computer software or hardware stolen?
 - 2. Is the computer system a tool of the offense, i.e. was the system actively used by the defendant to commit the offense?

Directive	Electronic Evidence	700-4	2 of 9
Effective Date	January 1, 2010		

3. Were fake IDs or other counterfeit documents prepared using the computer, scanner and color printer?
 4. Is the computer system only incidental to the offense, i.e. being used to store evidence of the offense?
 5. Is a drug dealer maintaining his trafficking records in his computer?
 6. Is the computer system instrumental to the offense and a storage device for evidence?
 7. Did the computer hacker use their computer to attack other systems and use it to store stolen credit card information?
- C. Once the investigator understands the computer's role, the following essential questions should be answered:
1. Is there probable cause to seize hardware?
 2. Is there probable cause to seize software?
 3. Is there probable cause to seize data?
 4. Where will the search be conducted?
 5. Is it practical to search the computer system on site or must the examination be conducted at a field office or a lab?
 6. If law enforcement officers remove the system from the premises to conduct the search, must they return the computer system, or copies of the seized data, to its owner/user before the trial?
 7. Considering the incredible storage capacities of computers, how will experts search this data in an efficient, timely manner?

V. SEARCH AND SEIZURE

- A. Using evidence obtained from a computer in a legal proceeding requires the following:
1. Probable cause for issuance of a warrant or an exception to the warrant requirement. If you encounter potential evidence that may be outside the scope of your existing warrant or legal authority, contact the District Attorney's Officer as an additional warrant may be necessary.

Directive	Electronic Evidence	700-4	3 of 9
Effective Date	January 1, 2010		

2. Use of appropriate collection techniques so as not to alter or destroy evidence.
3. Forensic examination of the system completed by trained personnel in a speedy fashion, with expert testimony available at trial.

B. Securing the Scene:

1. Officer safety is paramount.
2. Preserve area for potential fingerprints.
3. Immediately restrict access to computer(s).
4. Isolate from telephone lines, because data on the computer can be accessed remotely.

C. Securing the Computer as Evidence:

1. If computer is off do not turn on
2. If computer is on do the following:
 - a. If it is a stand-alone computer, non-networked, consult a computer specialist.
 - b. If a specialist is not available photograph screen, then disconnect all power sources.
 - c. Unplug the computer power cord from the wall and the back of the computer.
 - d. Place evidence tape over each drive slot.
 - e. Photograph/diagram and label back of computer components with existing connections.
 - f. Label all connectors/cable ends to allow re-assembly as needed.
 - g. If transport is required, package components and transport/store components as fragile cargo.

Directive	Electronic Evidence	700-4	4 of 9
Effective Date	January 1, 2010		

- h. Keep away from magnets, radio transmitters and otherwise hostile environments.

D. Networked or Business Computers

- A. Consult a computer specialist for further assistance; pulling the plug could cause the following to occur:
 1. Severely damage the system
 2. Disrupt legitimate business
 3. Create officer and Department liability

E. Other Electronic Storage Devices

- A. Electronic devices may contain viable evidence associated with criminal activity. Unless an emergency exists, the device should not be accessed. Should it be necessary to access the device, all actions associated with the manipulation of the device should be noted to document the chain of custody and insure its admission in court.
- B. Wireless Telephones
 1. Potential Evidence Contained in Wireless Devices:
 - a. Numbers called
 - b. Numbers stored for speed dial
 - c. Caller ID for incoming calls
 2. Other information contained in the memory of wireless telephones
 - a. Phone/pager numbers
 - b. Names and addresses
 - c. PIN Numbers Voice mail access number
 - d. Voice mail password
 - e. Debit card numbers

Directive	Electronic Evidence	700-4	5 of 9
Effective Date	January 1, 2010		

- f. E-mail/Internet access information
- g. The on screen image may contain other valuable information

C. On/Off Rule

1. If the device is on do not turn it off. Turning it off could activate lockout feature. Write down all information on the display and photograph if possible. Power down before transport. Take any power cords present.
2. If the device is off, leave it off. Turning it on could alter evidence on device, same as computers. Upon seizure get it to an expert as soon as possible or contact local service provided. If an expert is unavailable, use a different telephone and contact 1-800 LAWBUST, a 24 x 7 service provided by the cellular telephone industry.
3. Make every effort to locate any instruction Documents pertaining to the device.

D. Electronic Paging Devices

1. Potential Evidence Contained in Paging Devices
 - a. Numeric pagers receive only numeric digits; can be used to communicate numbers and code.
 - b. Alphanumeric pagers receive numbers and letters and can carry full text.
 - c. Voice pagers can transmit voice communications, sometimes in addition to alpha numeric.
 - d. 2-way pagers contain incoming and outgoing messages.
2. Once a pager is no longer in proximity to suspect, turn it off. Continued access to electronic communications over a pager without proper authorization can be construed as unlawful interception of electronic communication.
3. Search of stored contents of pager Incident to Arrest, with probable cause and exception or with consent.

Directive	Electronic Evidence	700-4	6 of 9
Effective Date	January 1, 2010		

E. Facsimile Machines

1. Fax machines can contain the following:
 - a. Speed dial lists
 - b. Stored incoming and outgoing faxes
 - c. Incoming and outgoing fax transmission logs
 - d. Header line
 - e. Clock setting
2. If fax machine is found on powering down may cause loss of last number dialed and/or stored faxes.
3. Search Issues include the following:
 - a. Record telephone line number into which the fax is plugged.
 - b. Header line should be the same as the phone line --user sets header line.
 - c. All Documents should be seized with equipment if possible.

F. Caller ID Devices

May contain telephone and subscriber information from incoming telephone calls Interruption of the power supply to the device may cause loss of data if not protected by internal battery back up. Document all stored data before seizure or loss of data may occur.

G. Smart Cards

1. A smart card is a plastic card the size of a standard credit card that holds a microprocessor chip capable of storing monetary value and other information.
2. Awareness
 - a. Physical characteristics of the card

Directive	Electronic Evidence	700-4	7 of 9
Effective Date	January 1, 2010		

- b. Photograph of the smart card
 - c. Label and identify characteristics.
 - d. Features similar to credit card/driver license
 - e. Detect possible alteration or tampering
3. Uses of Smart Card
- a. Point of sale transaction
 - b. Direct exchange of value between cardholders
 - c. Exchange of value over the Internet
 - d. ATM capabilities
 - e. Capable of storing other data and files similar to a computer
4. Circumstances Raising Suspicion Concerning Smart Cards
- a. Same as credit cards
 - b. Numerous cards with different names or same issuing vendor
 - c. Signs of tampering
 - d. Cards are found in the presence of computer or other electronic devices
5. Questions to Ask When Encountering Smart Cards
- a. Who is card issued to - the valid cardholder?
 - b. Who issued the card?
 - c. What are the uses of the cards?
 - d. Why does the person have numerous cards?
 - e. Can this computer or device alter the card?

Directive	Electronic Evidence	700-4	8 of 9
Effective Date	January 1, 2010		

6. Smart Card technology is used in some cellular telephones and may be found in or with cellular devices.

H. Tracing an Internet E-Mail

1. When an Internet e-mail message is sent, the user typically controls only the recipient line(s), i.e. to: and Bcc: and the Subject: line. Mail software adds the rest of the header information as it is processed.

2. Reading an E-Mail Header:

Sample E-Mail Header:

- a. Return-path:
 - b. Received: from in50210.cc.nps.navy.mil by nps.navy.mil (4.1/SMI-4.11) id AA08680; Thur, 7 Nov 96 17:51:49 PST
 - c. Received: from localhost by in50210.cc.nps.navy.mil (4.1/SMI-4.1) id AA16514; Thurs, 7 Nov 96 17:50:53 PST
 - d. Message-Id: <9611080150.AA16514@ in50210.cc.nps.navy.mil>
 - e. Date: Thur, 7 Nov 1996 17:50:53 -0800 (PST)
 - f. From: "Albert M. Bottoms"
 - g. To: Tim White
 - h. Cc: Real 3D
3. Line (1) tells other computers who really sent the message, and where to send error messages, i.e. bounces and warnings.
 4. Line (2) and (3) show the route that the message took from sending to delivery. Each computer that receives this message adds a Received: field with its complete address and time stamp that helps in tracking delivery problems.
 5. Line (4) is the Message ID, a unique identifier for this specific message. This ID is logged and can be traced through computers on the message route if there is a need to track the mail.

Directive	Electronic Evidence	700-4	9 of 9
Effective Date	January 1, 2010		

6. Line (5) shows the date, time, and time zone when the message was sent.
7. Line (6) tells the name and e-mail address of the message originator or "sender".
8. Line (7) tells the name and e-mail address of the primary recipient that may be the following:
 - a. A mailing list
 - b. A system-wide alias
 - c. A personal username
9. Line (8) lists the names and e-mail addresses of the "courtesy copy" recipients of the message.
10. There may be "Bcc:" recipients as well. Blind carbon copy recipients get copies of the message, but their names and addresses are not visible in the headers.

VI. REFERENCES

CALEA 83.2.5