



Seizure of Electronic Evidence

ENSURE OFFICER SAFETY

1 Determine The Computer's Role

- ✓ Is the computer contraband or fruits of the crime?
- ✓ Is the computer system a tool of the offense?
- ✓ Is the computer system instrumental to the offense and a storage device for evidence?

2 Essential Information

- ✓ Is there probable cause to seize hardware?
- ✓ Is there probable cause to seize software?
- ✓ Is there probable cause to seize data?

3 Preparing For the Search and / or Seizure

- ✓ Use appropriate collection techniques so as not to alter or destroy evidence
- ✓ Forensic examination of the system completed by expert personnel

4 Conducting the Search and / or Seizure

- ✓ Preserve area for potential fingerprints
- ✓ Immediately restrict access to computer(s)
 - Isolate from phone lines

5 Secure the Computer as Evidence

- ✓ If computer is "OFF"— DO NOT TURN "ON"
- ✓ If stand-alone (non-networked) computer is "ON"
 - Consult computer specialist
- ✓ If computer specialist is not available
 - Photograph screen, disconnect from power sources, unplug from wall AND back of computer
 - Place evidence tape on each drive slot
 - Photograph / diagram & label back of computer components with existing connections
 - Package components & transport / store as fragile cargo
 - Keep away from magnets, radio transmitters or other hostile environments



- ✓ If networked or business computer, consult a computer specialist—pulling the cord could cause severe damage

6 Other Electronic Storage Devices

- ✓ Wireless telephones, pagers, fax machine, caller ID device, smart cards