

Quick Steps for Seizing Computer Evidence

Secure the scene.

- Immediately Restrict Access to Computer(s).
 - Keep everyone away from computers.
 - Isolate from remote access (cable/phone).
- Determine if destructive program is running
 - If yes, pull power plug immediately



Destructive Program



Digital Movie Camera

- Isolate computers from any cameras
- If the Computer is "OFF" DO NOT TURN IT "ON"

Photograph and sketch the entire scene.

- Pay attention to the computer work area.
- For multiple computers, number each computer before they are moved or taken down.

IDENTIFYING THE OPERATING SYSTEM

Two types of interface

- GUI (Graphical User Interface)
- Command line

Windows O/S (GUI)

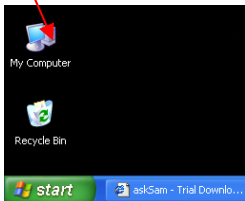


Indications

- My Computer
- Recycle Bin
- Start Button

Shutdown Method:

- Hard shutdown most situations
- Soft shutdown on Intrusion type cases

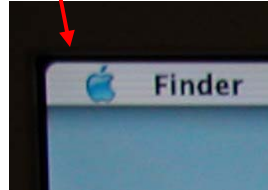


Apple (Macintosh) (GUI)



Indications:

- Apple symbol on screen or keyboard
- Macintosh HD Icon
- Trash Can vs Recycle bin



Shutdown Method for "Macs"

- Hard Shutdown

Linux X-Windows (GUI)



Indications:

- No Recycle Bin or Trash Can
- No "My Computer"
- No "Macintosh HD"

Shutdown Method

- Soft / Gradual

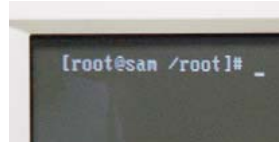
DOS Command Line



Indications:

- Drive Letter
- Shutdown Method: Hard Shutdown

LINUX/UNIX Command Line



Indications:

- No Drive Letter
- Symbols such as #, %, or !

Shutdown Method:

- Soft

If the Computer is "ON", follow these guidelines:

SHUTDOWN METHODS

Two methods of shutting a computer down

- Hard or Violent Shutdown (Pulling power plug)

- Windows
- DOS
- Mac

- Soft or Gradual Shutdown (Normal shutdown)
- Windows Intrusion Cases
- Linux/Unix
- Networks (Call for assistance!)

STAND ALONE DESKTOP(S) One or more computers not connected together



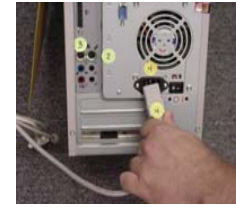
• Photograph the scene



• Photograph Screen



• Label Connections



• Pull the power plug



• Seal power port and case



• Transport / Impound

Important Notes

- Location of any computers you plan to seize on your notes.
- The time and date that you shut any computer systems down.
- Package ALL components and transport / store components as fragile cargo.
- Keep away from heat, magnets, radio transmitters, and other hostile environments.

NETWORKED COMPUTERS

Two or more computers connected together

- Consult a Computer Forensic Examiner.

- **DO NOT UNPLUG THE NETWORK COMPUTER POWER SOURCE.** Pulling the plug could:

- Severely damage the system.
- Disrupt legitimate business.
- Create Agent and department liability.

- Secure the scene until a Computer Forensic Examiner can be contacted.

LAPTOP COMPUTERS

- Photograph laptop computer screen if needed.
- Remove battery from the laptop.
- Unplug from the laptop and the wall.
- If unable to locate or disconnect battery, press power button for approximately 30 seconds for hard shutdown
- Seize the computer case and all the laptop parts you find. The laptop power supply is very important.
- Place in paper sack and seal with evidence tape



Non-DOS/Windows/Apple Systems

Contact a Computer Forensic Examiner for assistance in taking these systems down.

Personal Digital Assistants (PDAs)

- PDAs store information on RAM type memory
- When the battery is dies, all the data is lost



When seizing PDA's

- Package separately
- Mark clearly
- Seize charging / synch cradle
- Bring to RCFL ASAP

EQUIPMENT LIST FOR SEARCH KIT

- Camera
- Needle Nosed Pliers
- Indelible Ink Pen (Sharpie)
- Tamper Resistant Tape
- Screw Drivers (Phillips and flat head)
- Flashlight
- Regular Pliers
- Masking Tape
- Labels/ Post it Notes

CENTRAL PROCESSING UNITS – (CPU)



Tower Mini Tower Mid-tower Desktop Computer Network Server

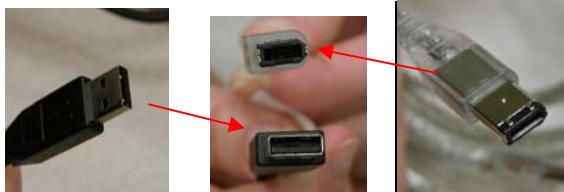
PERIPHERAL INTERFACE DESCRIPTIONS - CABLES



Parallel Cable (25 pin male (Printer)) Serial Cable (9 pin female) Video Cable (14 Pin male)

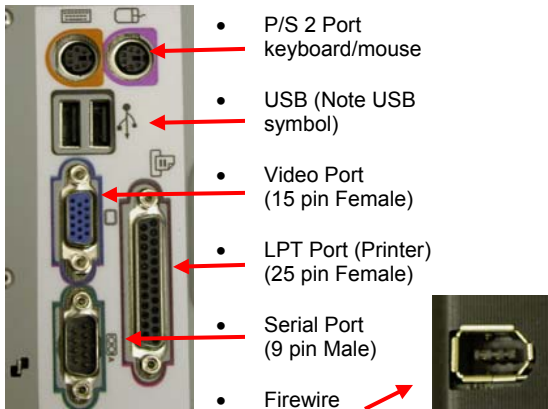


P/S 2 Connector Mouse/keyboard AT Connector Older keyboard RJ-11 Telephone (4 wires) RJ-45 Network (8 Wires)



USB (Rectangle) Firewire One side Triangle

PERIPHERAL INTERFACE DESCRIPTIONS – PORTS



- P/S 2 Port keyboard/mouse
- USB (Note USB symbol)
- Video Port (15 pin Female)
- LPT Port (Printer) (25 pin Female)
- Serial Port (9 pin Male)
- Firewire

Storage Media



Hard Drives Laptop (2 1/2 inch) Standard Internal (3 1/2 inch)



Thumb Drive and Smart Media

Packaging and Transporting

- Package all systems separately -
 - CPUs
 - Laptops
 - PDA's
 - Loose Hard Drives
- Always maintain chain of custody per your Agency's policies and Procedures.
- Store computer media in anti-static or paper bags.
- Keep computer media away from heat, moisture, and magnetic fields.

RCFL

Frequently Asked Questions

How do I request field assistance or Lab work?

For field assistance or lab work you must complete an RCFL "REQUEST FOR SERVICE" form. If you have multiple search sites, you must complete an individual request for each site. Similarly, a separate request is needed for lab work from each site. You may send your requests by mail or facsimile. Forms are available at our website at www.rcfl.org.

Who can submit digital evidence to the RCFL?

Any local, state or federal law enforcement agency in San Diego or Imperial Counties may submit digital evidence for examination.

What type of cases will the RCFL accept?

The RCFL will accept any criminal casework involving computers or digital evidence. The details of your case will remain confidential. All Examiners are bound by a non-disclosure agreement and maintain a Top Secret Security Clearance. All examiners are Certified FBI CART (Computer Analysis Response Team) Field Examiners

Will the RCFL take custody of the digital evidence from the search site?

No, RCFL Examiners will assist with shutting down computers, disassembly of peripherals and packaging of pertinent digital evidence. It is incumbent upon each agency to collect and inventory all digital evidence from the scene in accordance with their individual agency guidelines.

How much advance notice is required for RCFL assistance with field searches?

We recommend at least 48 hours notice, however, Examiners are available to respond 24/7 for emergencies.

Will the RCFL assist me with search warrant language for digital evidence?

Yes, Examiners will provide assistance with proper language to ensure digital evidence is properly covered within your search warrant.

Can the RCFL crack passwords?

Yes, the RCFL has advanced software & hardware tools, which can be successful in cracking passwords and encryption.

If I find a computer running, will it really hurt anything if I look around at some of the files?

Yes, it can jeopardize your case. Unlike traditional evidence, digital evidence can be destroyed if not handled properly. Accessing computer files can lead to deleted files, accidental file encryption, activation of destructive programs, and allegations of evidence tampering.

GUIDELINES FOR THE HANDLING AND SEIZURE OF DIGITAL EVIDENCE



The RCFL is located at:
9737 Aero Drive
San Diego, CA, 92123

Tel: (858) 499-7799
Fax: (858) 499-7798
Web: www.rcfl.org

Lab Hours: 8:00 a.m. to 4:30 p.m.
Emergency Contact: FBI Switchboard (858) 565-1255
Request the RCFL / CART Duty Examiner

Copyright 2003, © All rights reserved. For permission to reproduce, please contact the SD RCFL Director