



First responders guidelines for digital images and audio

1. Follow the law!
2. Recognizing audio and video evidence
 - training using documents with pictures having protocols written
3. What to do with the evidence?
 - Do no harm
 - Preserve most fragile evidence
 - physical evidence
 - digital evidence
 - Follow protocols for documenting the scene, photography, diagrams
 - Call for help, if available
 - Collect evidence according to protocols

EVIDENCE MAY BE DESTROYED BY MANIPULATION, SAFEGUARDS MUST BE TAKEN:

- Preservation
- Stop others from tampering
- Determine if the devices are active
- Document all
- Consider photographing
- Document power system – i.e. connected mains? Battery
- Remove external connections from telephone answer phones to stop deletion from outside
- Also fax/voice/ modems –(danger of data stored on volatile Ram only)
- Mark objects and record location
- Draw A PLAN
- VIDEO
- PHOTOGRAPH
- Consider traditional forensics, fingerprints/dna
- Copy the video / audio directly at the scene of crime, if possible
- Take information about the camera or/and the recorder.

Recognize the next kind of equipment:

Video cameras

Identify types of devices

- digital still cameras
- web cameras
- GPS-systems
- surveillance cameras
- public door access
- Video conferencing systems –standalone or PC based
- Media
- Image files stored on mp3 players
- CD-ROM/DVD
- Floppy disks

- Memory sticks
- Flash memory

Preserve Evidence on devices

Do not try to access the device.

Determine if the devices are active

Document power system – i.e. connected mains? Battery

ON OFF RULE : follow department protocols

Record any information located on the screen of the device (write or photograph it)

Don't let the subject touch the device for any reason

Properly label, store, handle and transport the device so no damage occurs

Record location of the devices, draw a plan

Take the evidence to the appropriate lab for examination as soon as possible, evidence could be lost when battery dies in only short numbers of hours.

Document all

Consider photographing

Consider traditional forensics, fingerprints/dna

Special considerations regarding this device

- Remove external communication connections to stop deletion from outside
- Copy the video directly at the scene of crime, if possible
- Take information about the camera or/and the recorders
- Record the system time and compare to the real time
- Record the parameters such as recording interval, recording speed

Audio

Identify Types of Devices

- Recorders
- Dictaphones
- Answering machines
- Mobile telephones
- On videos
- Memory sticks
- Telephone systems
- Voice over IP – computers
- Also fax/voice/ modems -
- PDA/personal organiser

Preserve Evidence on devices

Do not try to access the device.

Determine if the devices are active

Document power system – i.e. connected mains? Battery

ON OFF RULE : follow department protocols

Record any information located on the screen of the device (write or photograph it)

Don't let the subject touch the device for any reason

Properly label, store, handle and transport the device so no damage occurs

Record location of the devices, draw a plan

Take the evidence to the appropriate lab for examination as soon as possible, evidence could be lost when battery dies in only short numbers of hours.

Document all

Consider photographing

Consider traditional forensics, fingerprints/dna

Special considerations regarding this device

- Remove external communication connections to stop deletion from outside
- Also fax/voice/ modems –(danger of data stored on volatile Ram only)
- Copy the audio directly at the scene of crime, if possible
- Take information about the recorder.
- Record the system time and compare to the real time
- Record the parameters such as recording interval, recording speed