Diamond Cut Productions, Inc.

Application Notes
AN-19

Forensics Audio Laboratory Security Set-up and Procedural Tips

Here are a few security tips one should consider when setting up a Forensics Audio Laboratory:

1. The laboratory should be secured in a manner in which only authorized personnel are permitted entry into the Forensics audio laboratory proper. A log should be maintained showing lab activity in terms of persons and dates / times.

2. When unauthorized persons need to gain access to the laboratory area, written protocols should be established and strictly followed to allow clients and visitors entry into the laboratory (including the sign-in/sign-out sheets). But, these persons should never be provided with unfettered access to the lab; these persons should be made to leave the lab area when there are no authorized persons therein.

3. Unauthorized persons should never be left alone in a Forensics Audio Lab. This is very important and that is why we repeat it.

4. A security system should be installed in the laboratory portion of your Forensics facility. This should include intrusion detectors on windows, passive infrared detectors, and a keypad or biometric entry system coupled to an electrically activated locking system on the labs entrance.

5. An independent computer system (not associated with your Forensics Audio Workstation) should be used to monitor the security system. This system should be hard-wire monitored by a central security service.

6. Video cameras located in the lab area are recommended and should be enabled 24/7.

7. Your Audio Forensics Workstation computer(s) should NOT be connected to the internet in any way. Wireless connections to these workstations should be disabled. You need to be able to assure clients and the legal process that files on these computers were not tampered with in any way. One way to reduce that possibility of tampering is to eliminate outside communications connections with your Forensics Audio Workstations (wired or wireless).

8. Another major security risk are portable USB drives. Extreme care need to be taken when using a portable USB drive. These drives can carry virus files to your system and be used to extract critical information. The use of USB (thumb-drives) should be controlled. Signage should be posted outside the lab indicating that no un-authorized digital media is permitted inside the lab proper.

9. Your Forensics Audio workstation(s) should not be networked with computers outside of the audio forensics laboratory proper. The network within the lab should be hard-wired via a hub and not wireless and should have no internet connectivity. The administrative area’s computers outside of the lab proper should be the only ones connected to the outside world, like the internet.

10. Keep only software programs that are absolutely necessary for your Forensics Audio work on your Digital Audio Workstation (DAW). Billing and admin computers should be located elsewhere in the facility and not networked with the Forensics audio workstation(s).

11. Software registration should be performed manually. Use an administrative computer outside the lab area proper to obtain the necessary registration codes for your software and "sneaker-net" that information to your Forensics Audio Workstation(s).

12. Master (originals) audio materials should be stored in a fireproof safe. Backup copies of these audio materials should be kept in a secure area off-site. Audio materials should always be kept under lock when not being transferred to your Forensics Audio Workstation Computers.

13. Client Audio materials of any type should never be left unattended and accessible outside of the laboratory proper.

14. Master hard-copies of your clients source materials, audio restoration software and work-product files should be kept in the laboratories fireproof safe and this safe should be locked when the hard copy materials are not needed.

15. Cell phones should not be allowed to be used within a Forensics Audio Laboratory. They should be turned off (not just silenced) or left outside the laboratory proper. They should be held in the administrative area of the facility. This rule should apply to authorized personnel and visitors to the lab. A single land-line phone that is well controlled is permitted within the lab proper, so long as it is not connected to any of the DAW computers.

Forensics Audio Handling & Chain of Custody

If you are dealing with Forensics Audio materials or evidence, certain protocols need to be followed. There are several reasons for this.

1. The need to protect the evidence from potential tampering by anyone, especially third parties.

2. The need to prevent accidental damage from occurring to the materials while in transition or while they are in your possession.

3. The need to survive legal scrutiny under examination in a legal venue pertaining to the proper handling of the materials.

In terms of maintaining a traceable “Chain of Custody”, the following procedures should be followed:

1. Shipment to or from a client should be traceable via Registered or Certified US Mail.

2. A packing slip or letter should be included with the shipment describing the material enclosed.

Certain precautions should be followed when shipping Forensics Audio materials to assure its integrity throughout the process. The following recommendations should be followed:

1. Do not ship the audio materials in the same container with any other non-related items.

2. Six inches of packing material should be provided around the extreme dimensions of the media. This is to minimize the effects of shock and magnetic fields on magnetic based materials such as analog tapes, diskettes, or hard drives.

3. Use only non-shedding packing materials such as bubble wrap. Do not use shredded newspaper or anything similar since fibers can negatively affect tape mechanisms.

4. Use anti-static packing materials whenever possible (like pink colored bubble wrap).

5. Keep a written and photographic record of the packing process used and maintain that in a document folder for your client's project.

When you receive Forensics Audio materials from a client, it is advisable to follow this procedure:

1. Immediately inspect the outside of the package for damage. If there is any damage to the package, photograph it and document your findings in writing and place that documentation in the clients project folder or container. Immediately notify the carrier of the damage noted on the shipping material and inform your client of the damage noted and document your communications.

2. Open the container and inventory the contents found therein. Compare the contents against the packing list or letter. If there are any discrepancies, note these in writing, place those notes in the client's project folder and inform your client of your findings.

3. Save all shipping labels & documents attached to the shipping materials/package.

4. Carefully inspect all packing material to be sure nothing of evidentiary value is discarded.

5. Photograph the recording(s) media as received.

6. Date and mark the recording(s) for identification.

7. Conduct a detailed physical examination of the recordings. Points of interest should be photographed. Keep detailed written notes as you examine the materials and maintain those notes in the client's project folder.

8. If not already removed, remove the safety recording tab(s) from analog Cassette tapes before playing. Do not discard the tab(s). Put each tab in a labeled and separate envelope. Identify the original location of each of the tabs. Seal the envelopes and document their contents and keep this in the client's project file.

Use the following guidelines whenever handling a client’s magnetic audio evidence:

1. Use white cotton gloves whenever handling Forensics Audio materials (like tapes or discs). Alternatively, you can thoroughly wash your hands prior to handling the materials. Only handle the material when absolutely necessary for examination, playback, or return to the client. Avoid any unnecessary handling of the material and be sure not to touch the actual media recorded surface with a bare hand or ferrous tool.

2. Create a direct digital copy of the material onto your DAW. Perform all of your analysis using the digital copy rather than working continuously with the original. Using the Diamond Cut recorder, transfer the recording with 24 bit resolution and a 96 KHz sampling rate. Keep a written record of the time that the recording was transferred and the file name assigned. Make a backup copy of the digital recording on a CD, DVD, USB thumb drive, or external hard-drive. Keep this copy in a secure location off-site.

3. Always be sure to keep magnetic media away from all sources of magnetic fields such as computer monitors, loudspeakers, permanent magnets, power amplifiers, backup power supplies, power tools, etc…

4. Make sure that the analog playback machine’s heads and tape guides had recently been de-magnetized (degaussed). This is an operation that should be performed outside the forensics laboratory proper and at least ten feet away from all client magnetic based media.

When you are not using the Audio Evidence, you should abide by the following rules:

1. Limit access to the material to those in your laboratory who have a need to know based on their involvement with the project.

2. Keep the material in a fireproof safe which is kept locked. Preferably, this safe should be located in the basement of your building near a 90 degree corner of a foundation wall.

3. Assure that the material is kept in a constant temperature and constant humidity environment, keeping it stored away from any source of magnetic fields. Ideally, storage temperatures should be around 60 degrees F and the relative humidity should be 40% or less.

Keep your Diamond Cut Audio Forensics Software up to date. We keep a log of potential bugs as they are reported. When they are verified, they are fixed by the company and updates are provided on a scheduled basis. Check for updates or upgrades periodically at www.diamondcut.com.

DIAMOND CUT
PRODUCTIONS®