

"VERIFYING THE INTEGRITY OF AUDIO AND VIDEOTAPES"

By Steve Cain

An ever-increasing reliance on tape evidence in criminal prosecutions, especially in organized crime and drug cases, under scores the importance of tape integrity and the methods used to qualify or disqualify tape evidence.

This article will discuss some of the procedures utilized in analog and digital editing of tapes and assess their potential threat vis-a-vis tape tampering issues; the "legal admissibility" issue surrounding tape recorded evidence to include defining strategies for the defense to require the government to release the 'best evidence' for analysis purposes; and an overview of the accepted techniques for the scientific analysis of recorded tape evidence.

Tape Editing Technology,

The forensic examination of "tampered tapes" should include an inspection of the original tape(s) and the recorder(s) used to produce the tape(s). In the simple case, the existence of an electronic edit and/or evidence of physical splicing will produce acoustic irregularities which can be viewed with instruments and documented.

Modern day technology was apparently used in the electronic editing performed on the disputed Gennifer Flowers/Gov. Bill Clinton tape recordings. The Cable News Network (CNN) asked that I provide an expert opinion on Mr. Clinton's voice and also asked that I examine the tape submitted by the STAR News Magazine for any evidence of possible tampering. The later examination disclosed a number of suspicious acoustic events (anomalies) including: a total loss of signal (dropouts) ;a change in the speakers' frequency response during different telephone conversations; and "spikes" (audible sounds of short duration which are often attributable to normal stop/start and pause functions of the recorder).

In order to provide any definitive conclusion, I requested the original recorder and tape to determine if these electronic edits were intentional edits or possible malfunction/anomalies of the recorder/microphone equipment. CNN has never received the requested tape or recorder from the *Star News Magazine*.

Digital editing of both audio and video tapes, however, greatly complicates the issue and increases the likelihood that altered tapes can escape detection.

The Federal Bureau of Investigation (FBI) Signal Analysis Branch has already acknowledged, "It is difficult to detect some alterations when a recording is digitized into a computer system, physically or electronically edited and recopied on to another tape." *1*

The days of utilizing a razor blade and splicing tape to effectively alter or "doctor" a recorded conversation are all but gone. Right now there are at least twenty manufacturers of desktop computer editing work stations or digital

recorders which can be used as "turn key" editing systems. Software and add on computer cards can transform an IBM personal computer or a Macintosh computer into a sophisticated digital audio editing machine. Some of the systems require a digital audio recorder for initial conversion of the analog format before accessing the computer hardware. These editing work stations were developed to save the motion picture and recording industries money by precluding the necessity of recording sessions or to correct subtle errors in multi track releases.

Some computer boards and software cost less than a \$1000, and provide both recording and editing of sound in an IBM compatible or Mac personal computer format. Editing options are practically inexhaustible thus giving the operator the ability to alter the tape in a word processor type of mode (i.e. cut and paste, copy, delete, etc.) while selected playback files utilize subdue cross fading effects that can "shape" the sound. The typical telltale signs of traditional analog recorder editing including "clicks, pops" and other short duration sounds, can now all be effectively removed without any detectable, audible clue.

Traditional Editing Techniques

Present tape editing practices include either physical splices or electronic editing on one or more analog tape recordings whenever portions of selected conversations are over recorded (i.e. erased) or the original recorder was stopped and restarted inappropriately. While listening to the tape, the attorney may first suspect an alteration by noting either unexplained transients, equipment sounds, extraneous voices, or inconsistencies with provided written information.

The major categories of tape alterations include; (1) Deletion; (2) Obscuration; (3) Transformation; and (4) Synthesis *2* Deletion of unwanted material can readily be done through splicing or by using one or more recorders to erase, rerecord, or stop/pause the recorder at strategic points within the conversation. Obscuration involves the distortion of a recorded signal with the purpose of rendering selective portions unintelligible. This method, for example, was used during the editing of the infamous 18minute gap in the Watergate tapes. This technique is also used to .mask splices, clicks, or suspicious transients and is more difficult to detect than deletion methods. By judicious use of two tape recorders, one may add "noise" to the copy and thereby mask the original recording and render it less intelligible. One can also reduce the volume of the slave recorder and thus weaken the amplitude of target conversations on the original tape.

Transformation involves the alteration of portions of a recording so as to change the meaning of what is said. The technique is similar to deletion practices but greater skill and care must be applied as a knowledge of acoustic phonetics is required to avert a suspicious edit.

Lastly, synthesis is the generation of artificial text by adding background sounds or conversation to the tape copy which were not present on the original recording. The addition of selective phrases can be accomplished if a sufficient data base library of recorded conversations is available. It must be emphasized that all of the traditional analog methods of altering audiotapes can be more efficiently and surreptitiously accomplished through the use of digital editing work

stations.

Tape Authentication And Detection Of Edits

With the threat of digital editing looming larger, it is more imperative than ever that both the official tapes and recorders be made available for inspection.

The FBI's Signal Analysis Branch has developed a set of well defined procedures for the acceptance of authentication requests which provides an excellent overview of what the government considers to be essential for a scientifically valid tape analysis:

1. Sworn testimony or written allegations by defense, plaintiff, or government witnesses of tampering or other illegal acts. The description of the problem should be as complete as possible, including exact location in recording, type of alleged alteration, scientific test performed, and so on;
2. The original tape must be provided. Copies of a duplicate tape cannot be authenticated and are normally not accepted for examination by the FBI;
3. The tape recorders and related components used to produce the recording must be provided; and,
4. Written records of any damage or maintenance done to the recorders, accessories, and other submitted equipment must be provided.

In addition, there must be a detailed statement from the person or persons who made the recording describing exactly how it was produced and the conditions that existed at the time, including:

A. Power source, such as alternating current, dry cell batteries, automobile electrical system, portable generator.

B. Input, such as telephone, radio, frequencies (RF) transmitter/receiver, miniature microphone, etc.

C. Environment, such as telephone transmission line, small apartment, etc.

D. Background noise, such as television, radio, unrelated conversations, computer games, etc.

E. Foreground information, such as number of individuals involved in the conversation, general topics of discussion, closeness to microphone, etc.

F. Magnetic tape, such as brand, format, when purchased and whether previously used.

G. Recorder operation, such as number of times fumed on and off in the record mode, type of keyboard or remote operation for all known record events, use of voice activated features, etc.

Also recommended is a typed transcript of the recording, to include both English and foreign language versions ^{*3*}

It is essential in all tape authentication exams to obtain the original recorder and tape, as copies cannot normally be authenticated. If the defense is 'encountering difficulties in obtaining the necessary "originals they may wish to cite Koenig's article'^{*4*} as an authoritative resource which specifies the reasons why the original evidence is essential in any tape tampering request.

If the original tape and recorder are not available for inspection, the forensic expert can still conduct a preliminary examination of the submitted "copy" for any evidence of discontinuous recorder operation, although all conclusions must

necessarily be qualified regarding possible editing effects. The examination process normally includes both an aural, physical, and instrumental analysis of the evidential tape. Phase continuity, speed determination, azimuth determination, waveform analysis, spectrographic and narrow band spectrographic analysis are among the techniques employed to evaluate the tape.

The techniques and tests are usually adequate in the detection of altered analog recordings. Fortunately, the vast majority of altered tapes today are still analog tapes.

Defense counsel should have a working knowledge of how tapes are analyzed.

First, there is a physical inspection of the submitted tape, the tape housing, the tape recorder and all ancillary equipment used to make the original recording: microphones, telephone couplers, transceivers, etc. A magnetic development test involves the application of a special fluid which under proper magnification will make visible the head track configuration, off-azimuth recordings, start/stop functions, damage to recording heads, etc. The forensic expert can subsequently determine whether the submitted tape is a copy, has been over-recorded, or was made on a different recorder than the one submitted. The original recorder can be detected by slight speed fluctuations and deformities in the rotating parts which provide a unique "wow and flutter" signature which can be measured. Also, spectrum analysis can be used to measure slightly different signals transmitted through the microphone or telephone equipment. All of the signal analysis equipment can be useful in answering questions related to bandwidth, distortion effects, or unique tones generated during the original recording process.'

Forensic Video Examinations

The forensic video examiner is concerned with the authenticity and integrity of the signal. Questions relating to whether the tape is a copy, a compilation of other tapes or an edited version are of important consideration. Forensic examinations of videotapes usually consist of both a visual and aural examination. One of the more important pieces of equipment used in forensic video examinations is a waveform monitor which is a specialized oscilloscope. It displays the voltage versus time modes and has specialized circuits to process the signal. If any editing occurs, then it is possible to display the signal aberration on the display screen of the instrument.*5*

Additional tests include measurements of the chrominance, hue and burst of the color videotape by using a vector scope. The vector scope measures the chrominance information and allows for the examination of matching bursts of multiple signals. It also permits the investigation of edit points.

Vertical, interval and horizontal information known as video synchronizing information can be observed on a cross pulse monitor. This "cross pulse" information can be viewed on a cross pulse monitor and with proper application, one can often determine if the videotape is a copy or an original. In cases where the helical heads are out of alignment, a set of marks could exist for each succeeding generation or copy.*6* Lastly, if one suspects videotape editing, the

examination will require a frame by-frame inspection, with the use of wave form monitors, vector scopes, and a cross pulse monitor together with other forensic equipment as deemed appropriate. It must be noted that there are sophisticated production studios that can edit video tapes in such fashion that traditional methods of detection are no longer adequate. Studios capable of producing such tapes are, for now, generally limited to larger metropolitan areas.

Legal Issues/Admissibility

In their article, "Attacking The Weight Of The Prosecution's Science Evidence,"^{*7*} authors Edward J. Imwinkelried and Robert Scofield explore the thesis that the accused has a constitutional right to introduce expert testimony which can generate a reasonable doubt. The authors warn, however, that this right to relevant criminal evidence is in fact very limited in scope, namely; (1) important or "crucial evidence" and; (2) the defense must show that the evidence is "trustworthy."

Likewise, authors Nancy Hollander and Lauren Baldwin point out that the admissibility of an expert's testimony is often dependent on whether the expert is testifying for the defense or for the prosecution ."^{*8*}

In the field of forensic tape analysis, there exists few competently trained and certified experts available to the defense to challenge the accuracy of government tapes and/or the conclusions of the government experts. Even though I have over twenty years experience in federal law enforcement and as a Treasury Department crime laboratory supervisor, I am routinely subjected to concerted efforts by the prosecution to attack my credibility and the accuracy of my conclusions. As you would expect, as a government expert, I *never* received any criticisms from the prosecutor concerning my credentials or accuracy of my findings.

Access To Evidence

More and more courts are being forced to address the question of whether the government has the privilege to withhold technical data from a defendant challenging the integrity of electronic surveillance evidence. A few courts have recognized "qualified privilege" for the government to such data (by drawing an analogy to an "informer's privilege"), but have not been very sensitive to the unique nature of electronic surveillance evidence nor defined the showing required to overcome the government's "qualified privilege." Under the due process clause, criminal defendants should be afforded a meaningful opportunity to present a complete defense.^{*9*} To safeguard this right the court has recognized the principle of "constitutionally guaranteed access to evidence"^{*10*} This access to evidence however, is not absolute as indicated in *Roviaro v. United States*,^{*11*} wherein the court recognized the government's limited privilege to withhold the identity of informers. Two circuit courts of appeal have extended the limited privilege recognized in *Roviaro* to the nature and location of electronic surveillance equipment."^{*12*}

In *Angiulo and Cintolo*, the appellants asserted that the district court had mistakenly barred questions concerning providing them the precise location of

micro- phones hidden in an apartment. Trial motions for the information had not been made nor had the defendants offered any technical basis for the value of the information. The government successfully objected to the questions concerning the microphones location on the grounds that it would reveal sensitive surveillance techniques anti jeopardize future criminal investigations.

In upholding the district court, the First Circuit, citing *Van Horn* ^{*13*} and *United States' v. Harley*,^{*14*} and making an analogy to the informer's privilege in *Roviaro* held that a qualified privilege against compelled government disclosure of sensitive investigative techniques exists."^{*15*} The privilege can be overcome, however, by a sufficient showing of need. The defendant must show that, "he needs the evidence to conduct his defense and that there are no adequate independent means of getting at the same point."^{*16*} The *Cintolo* court stressed that the extent to which adequate alternative means could have substituted for the proper testimony is, "a key to evaluating this claim of necessity."^{*17*}

As technological advances have occurred in digital editing, there likewise has been a tremendous increase in the number of body worn FM transmitters and other recording devices used by law enforcement to collect evidence against defendants. It should be emphasized, however, that some of this evidence may not be admissible in court if the agencies do not comply with several Federal Communication Commission (FCC) regulations. First, all nonfederal agencies must use only transmitters that are approved by the FCC and without this approval the transmitter is not considered a legal transmitting device and therefore cannot be legally used to gather evidence. Secondly, state and local agencies must be licensed in the FCC's Police Radio Service and thus far most departments reportedly have not met this requirement. These observations are part of the information contained in "Equipment Performance Report: Body Worn FM Transmitters," a report of the Technology Assessment Program (TAP). This program tested nine Body-Worn FM transmitters in accordance with National Institutes of Justice (NIJ) Standard 0214.01. These standards require transmitters passing the test to provide intelligible audio signals that result in acceptable quality voice recordings.^{*18*} As noted in the *Cintolo* and *Angiulo* decisions, the defense failed to provide a sufficient showing of necessity, thus, it is imperative that defense experts vouch for the necessity of access to the government evidence as soon as possible.

The Need For Original Recording Equipment And How To Get It

There are a number of valid scientific reasons for accessing original tapes, recorders, and related equipment to conduct a proper analysis.

In practically every creditable forensic publication dealing with forensic tape analysis procedures, the authors emphasize the necessity of examining the original evidence or a direct patch cord copy. In many cases, however, experience has shown an unwillingness of the government prosecutor and agents to provide such materials to the defense for examination purposes. The government may object that the defense never requested the original or direct copy recordings and therefore, their motions for access at the eleventh hour are basically "delay strategies." This argument can be effectively countered if the

defense obtains an appropriate court order requesting the defense expert be provided access to the required "best evidence recordings."

Secondly, the government may contend that it has a qualified (if not absolute) privilege of withholding technical data from the defense counsel citing "National Security" or indicating that such release may jeopardize future criminal investigations. The *Angiulo* and *Cintolo* decisions provide the defense counsel relief from such government actions. Counsel must show the need for the evidence to conduct the defense and that there "is no adequate independent means of getting at the same points."

The importance of the defense obtaining the original or at least a direct patch cord copy of all evidential recordings can not be over emphasized. In -practically every case I have seen, the copy initially provided by the government was not adequate for the best voice identification, tape enhancement or tape authentication examination. Subsequent motions filed by the defense citing the aforementioned requisite need for the Original evidence often results in its release by the court. As reflected in the newly approved International Association for Identification standards for analysis of questioned voice recordings, the, "unknown and known voice samples must be original recordings, unless listed as a specific exception"^{*19*}

Notes:

1. Bruce E. Koenig, *Authentication of Forensic Audio Recordings*, JOURNAL OF AUDIO ENGINEERING, 38 No. 1/2, 1990, Jan/Feb, page 4.
2. National Commission For The Review of Federal and State Wiretapping Laws, pp 223225,1972.
3. Steve Cain, *Voiceprint Identification*, NARCOTICS, FORFEITURE, AND MONEY LAUNDERING UPDATE NEWSLETTER, U.S. Department of Justice, Criminal Division, (Winter 1988).
4. Bruce E. Koenig, *Authentication of Forensic Audio Recordings*, JOURNAL OF AUDIO ENGINEERING SOCIETY, 38 No. 1/2, 1990, Jan/Feb. page 4.
5. Tom Owen, *Forensic Audio and Video Theory And Applications*, JOURNAL OF AUDIO ENGINEERING SOCIETY, Vol. 36, No. 1/2. 1988, Jan/Feb, page 39.
6. *Ibid* page 40.
7. Edward J. Imwinkelried, and Robert G.Scofield, *Attacking The Weight Of Prosecution ~Scientific Evidence*, THE CHAMPION, PDN, April 1992.
8. Nancy Hollander and Lauren M. Baldwin, *Testimony In Criminal Trials: Creative Uses,Creative Attacks*, THE CHAMPION, December 199 1.
9. California v. Trombetta, 467 U.S. 479, 485 (1984).
10. United States v. Valenzuela Bernal, 458 U.S. 858, 867 (1982).
11. 353 U.S. 53 ().
12. See United States v. *Angiulo*, 847 F.2d. 956,98182 (1st Cir. 1988); and United States v. *Cinto1o*, 818 F.2d. 980, 100103 (1st Cir. 1987); United States v. Van Horn, 789 F.2d. 1492, 150708 (11th Cir. 1986).
13. 798, F.2d. 1492 ().
14. 682 F.2d. 1018, 1020 (D.C. Cir 1982).
15. *Cintolo*, 818 F.2d. 1002.
16. See Harley, *supra*.
17. *Cintolo*, 818 F.2d. 1003.
18. Copies are available at no charge from the Technology Assessment Program Information Center (TAPIC), tollfree number 800-248-2742 or (301) 251-5060.
19. *IAI Voice Comparison Standards*, JOURNAL OF FORENSIC IDENTIFICATION, January/February, 1992