JOURNAL OF FORENSIC SCIENCES

J Forensic Sci, January 2012, Vol. 57, No. 1
doi: 10.1111/j.1556-4029.2011.01899.x
Available online at: onlinelibrary.wiley.com

CASE REPORT

DIGITAL & MULTIMEDIA SCIENCES

Bruce E. Koenig,[1] *M.F.S. and Douglas S. Lacey,*[1] *B.S.*

An Inconclusive Digital Audio Authenticity Examination: A Unique Case

ABSTRACT: This case report sets forth an authenticity examination of 35 encrypted, proprietary-format digital audio files containing recorded telephone conversations between two codefendants in a criminal matter. The codefendant who recorded the conversations did so on a recording system he developed; additionally, he was both a forensic audio authenticity examiner, who had published and presented in the field, and was the head of a professional audio society's writing group for authenticity standards. The authors conducted the examination of the recordings following nine laboratory steps of the peer-reviewed and published 11-step digital audio authenticity protocol. Based considerably on the codefendant's direct involvement with the development of the encrypted audio format, his experience in the field of forensic audio authenticity analysis, and the ease with which the audio files could be accessed, converted, edited in the gap areas, and reconstructed in such a way that the processes were undetected, the authors concluded that the recordings could not be scientifically authenticated through accepted forensic practices.

KEYWORDS: forensic science, forensic audio, audio authenticity, digital authenticity, recording, inconclusive

As background, authenticity examinations of analog and digital audio recordings are regularly conducted by private and government laboratories throughout the world to determine originality, continuity, and the presence of alterations (1–3). Based on the authors' over 50 years of experience, almost all such authenticity examinations result in conclusive results when conducted by qualified examiners in properly equipped laboratories. Exceptions may exist in very few cases involving digital recordings, where a cautionary statement is included by the examiner in the laboratory report regarding possible, but often unusual, scenarios that might escape detection based on the present protocol.

In this case report, a private attorney on the west coast of the U.S. hired a private investigator (PI) to perform investigative tasks involving a civil family law matter. Partially based on a physical search of the PI's offices by law enforcement personnel, the attorney and the PI were criminally charged with both conspiracy to intercept and the actual interception of wire communications involving the opposing parties in the civil matter (4–6). Even though no recordings were ever recovered by the government involving the alleged wiretaps, other encrypted digital audio files were found on a computer hard drive in the PI's private office. These files were decrypted by the government and determined to be mostly telephone conversations between the attorney and the PI regarding the civil matter. These files, recorded at the PI's office, could not be authenticated by direct testimony, because neither defendant gave a statement to government investigators regarding the conversations or the recording procedures nor were either expected to testify at trial. In fact, the attorney's lawyers argued that he had no knowledge of the recordings prior to the criminal proceedings. The authors of this article were contacted and asked to scientifically determine whether the recorded digital telephone conversations were authentic and, if necessary, provide expert testimony at trial. As an added facet to this authenticity analysis, the PI is also a forensic audio authenticity examiner who has authored an article (7) and coauthored a book (8) on the subject, been the head of a professional audio society's writing group for authenticity standards (9), given related presentations at professional forensic society meetings, and testified as an expert for both the government and private organizations. It is also noted that one of the authors of this case report was familiar with the PI's voice from prior contacts regarding his authenticity and other forensic activities.

[1]BEK TEK LLC, 12115 Sangsters Court, Clifton, VA 20124-1947.

Received 11 Aug. 2010; and in revised form 8 Nov. 2010; accepted 14 Nov. 2010.

Materials

The authors were provided, in part, with the following computers, software, media, and documents for examination:

- An Apple Power Mac G4 computer, model M8493, with an OS 9.2 operating system, containing various files and software (designated as specimen Q1 by BEK TEK LLC). The computer make and model, operating system version, file system and contents (files and software) were identical to that seized from the PI's office by the Federal Bureau of Investigation's (FBI's) Computer Analysis & Response Team (CART).
- An Apple iMac computer, model M5521, with an OS 9.2 operating system, containing various files and software (designated as specimen Q7 by BEK TEK LLC). The computer make and model, operating system version, file system and software were identical to a second computer seized from the PI's office by CART. Additionally, the contents of an external hard drive attached to this computer (as imaged by CART) were also contained on specimen Q7. Included as part of the contents of this external hard drive were 35 proprietary-format audio files.

- A Verbatim DVD-R disc (designated as specimen Qc2 by BEK TEK LLC), written in a data format and containing 35 Pulse Code Modulation (PCM) wavefiles. These files were represented by the FBI as having been converted from the 35 proprietary-format audio files found on specimen Q7.
- Various documents including CART forms, testimony from a previous criminal trial involving the PI, and FBI laboratory reports and work notes, which reflected in part the following:
  - The telephone conversations occurred and were recorded by the PI during the period of March to May 2002.
  - The digital recordings of the telephone conversations were seized by government personnel on November 21, 2002 during the search of the PI's private office.
  - The search revealed that the PI's desk telephone was directly connected to an Apple iMac computer, which had an external hard drive for backing up certain data. This system contained the 35 digitally recorded telephone files, the TeleSleuth Jr. recording program, and the TeleSleuth Player program. The 35 files were recorded in the proprietary TeleSleuth Jr. format.
  - Also, in the PI's office was an Apple Power Mac G4 that contained a professional audio editing program and the Forensic Audio Sleuth software, which allowed the playback, analysis, and editing of digital audio recordings including those in the proprietary TeleSleuth Jr. format.
  - The TeleSleuth Jr., TeleSleuth Player, and the Forensic Audio Sleuth programs were all developed by the PI and a software developer who was a codefendant with the PI in a previous criminal case.

Methods

Detailed examinations of the 35 digital files, in the TeleSleuth Jr. format, and the provided proprietary software on specimens Q1 and Q7 were conducted using the following nine laboratory steps of the peer-reviewed, published 11-step digital audio authenticity protocol (1): (i) evidence marking; (ii) playback/conversion optimization; (iii) critical listening; (iv) high-resolution waveform analysis; (v) narrow-band spectrum analysis; (vi) spectrographic analysis; (vii) digital data analysis; (viii) miscellaneous examinations (regarding the functionality of the various software); and (ix) work notes and reporting. The two protocol steps not performed were the physical inspection, because the recordings were imaged digital computer files and not on original media, and the digital data imaging, since the FBI's CART examiners had already performed that function. Additionally, information regarding the evidence marking, and the work notes and reporting steps are not listed in this case report. It is noted that the nine steps listed later in this article are not presented in the same order as aforementioned.

Critical Listening (Preliminary Review)

A preliminary review of the 35 proprietary files on the computer hard drive of specimen Q7 and the FBI laboratory reports and work notes revealed that the files were all encrypted audio recordings, which could be opened with a provided decryption key in either the TeleSleuth Player or the Forensic Audio Sleuth (on specimen Q7) programs. The audio files were all determined to be monaural, recorded with a sampling rate of 8820 hertz (Hz) and 16-bit PCM quantization. Each of the file names included the date (year/month/day), recording start time (military formatting), and recording duration (in minutes and seconds); for example, a 3 min 21-sec recording, starting at 4:39:10 PM on April 15, 2002 would be named "02/04/15 @ 16.39.10 – 03m 21s."

Miscellaneous Examinations

A review of the TeleSleuth Jr. interface window for its recording function revealed an icon button for starting the recording (a red circle), which changes to a stop button (a white square) once the recording is in progress; additionally, there are an audio level indicator and a pause button that changes from gray to red when activated. Figure 1 is a grayscale representation of the TeleSleuth Jr. interface window.

To create a recording, the operator clicks the record icon at the beginning and then the stop button to end the process. The pause button can be used during the recording process to momentarily stop and then restart the recording during the same file creation. Preliminary test recordings of sample speech information were produced using TeleSleuth Jr., which revealed that the general file and default naming characteristics are consistent with the 35 proprietary-format recordings on specimen Q7.

Recordings produced using the TeleSleuth Jr. program are both in a proprietary format and encrypted. TeleSleuth Player and Forensic Audio Sleuth are the only programs, known to the authors, that allow playback of TeleSleuth Jr. files. The TeleSleuth Player allows the user to open a TeleSleuth Jr. recording only when the decryption key or phrase is known. Once the file is opened, the software displays a low-resolution, visual representation of the recorded audio in the form of a time waveform (time on the horizontal axis and amplitude on the vertical axis). The software interface also includes controls for playing back the file from the current location or from a user-defined point in the file, the ability to define segments within the file, and functions for the export of the segments as separate files and the concatenation of the segments into a single, composite file. Figure 2 illustrates the TeleSleuth Player interface.

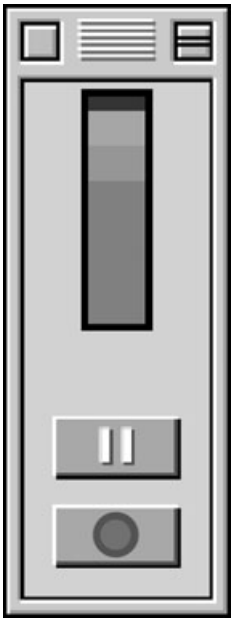

FIG. 1—*TeleSleuth Jr. recording interface in the record-ready mode, with the input level meter at the top, the pause button in the middle, and the record button at the bottom.*

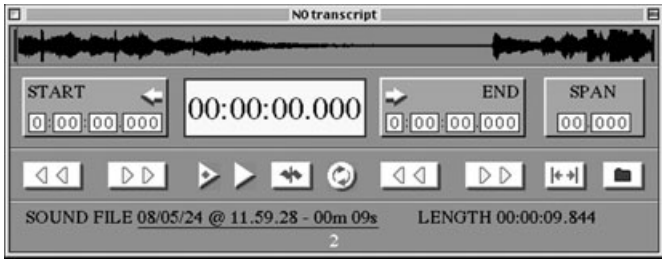

FIG. 2—*TeleSleuth Player display for an audio file named "08/05/24 @ 11.59.28 – 00m 09s."*

For a cursory check of the integrity of a file, an "authenticate" function is available within the TeleSleuth Player that compares information about the file in its present state with corresponding, predetermined values contained in the resource fork of the native, Macintosh-format file (10). Based on a source code review conducted by computer forensics experts in this case, the comparative information includes the following:

- A numerical representation (or checksum value) computed for the first 256 bytes of the resource fork data;
- A checksum value of the audio data in its entirety;
- A checksum value of the file name text; and
- A confirmation that the file is original and not a composite file created from user-defined segments.

If a file passes the "authenticate" process, the following phrase will appear as a result: "The sound file <file name> HAS NOT been modified," with "HAS NOT" in flashing text. Prior to conducting any further analyses of the 35 encrypted audio files, they were subjected to the "authenticate" feature of TeleSleuth Player and each passed the integrity check.

A detailed review of the TeleSleuth Player menus and the preparation of appropriate test recordings revealed a number of functions for modifying/filtering the audio content and/or the administrative data of a TeleSleuth Jr. recording, including the following:

- The ability to manually mark segments within a recording, which can then be saved as separate audio files or as a composite file consisting of only the segmented portions concatenated to one another.
- The ability to add or subtract an amount of time from the recorded time of a file (as included in the file name). The name of the file is changed to reflect the entered offset, but the length of the recording and the audio data itself remains the same. This process can also be applied to multiple files within a single folder.
- The ability to add, remove, or change embedded text data—such as dual tone multi-frequency (DTMF) information—manually or through a batch process. If a recorded file contains embedded text, this text appears at the bottom of the TeleSleuth Player window during playback.
- The ability to change the "encryption phrase" of one or more files as part of a batch process. The original files are deleted and newly encrypted files are created using a manually entered encryption phrase.
- The ability to apply one or more notch filters at certain frequencies, in an effort to enhance the recording.
- The ability to change the overall "gain" or amplitude of the audio recording.

Each of these functions was independently applied to test recordings to ascertain their effects on the "authenticate" function within TeleSleuth Player. It was determined that the employment of some of these functions, such as the segmentation and call information modifications, causes the "authenticate" feature to flag a file as being an "edited copy" or as having been "modified." However, the notch filter and gain change functions did not change the "authenticate" results.

In addition to allowing for the playback of TeleSleuth Jr. files, the Forensic Audio Sleuth software provides advanced editing, analysis, processing, and file saving capabilities. When opened in the Forensic Audio Sleuth program, a TeleSleuth Jr. file must first be converted to the native Forensic Audio Sleuth format (as prompted by the software), after the correct decryption key or phrase is entered. Edits such as muting, deleting, inserting, or rearranging segments within a file or across multiple files can then be readily performed, and the modified results can be saved in a number of different file configurations including the native and PCM wavefile formats. Files in the Forensic Audio Sleuth format can also be opened in TeleSleuth Player and converted into encrypted TeleSleuth Jr. files. Figure 3 is an example of an audio file opened in the Forensic Audio Sleuth software.

Playback/Conversion Optimization

Using the Forensic Audio Sleuth software, the 35 TeleSleuth Jr. files were opened, converted by default to the native Forensic Audio Sleuth file format, and then saved in the PCM wavefile format, with the converted files containing monaural audio data recorded at a sampling rate of 8820 Hz and 16-bit PCM quantization. Aural review and comparison of the Forensic Audio Sleuth files and the PCM files revealed no obvious loss of quality or added/removed content as a result of the conversion processes. Additionally, the newly produced PCM files were compared to the corresponding PCM files on specimen Qc2, which were created by the FBI through a different, in-house conversion process. This examination entailed direct waveform comparisons between the corresponding files which revealed that the respective audio recordings were identical in length. Through phase inversion and mixing processes, the files' contents were also found to match, except that some of the sample values had an absolute difference of one quantization level (i.e., one out of 2^{16} or 65,536 total values), possibly attributable to the different methods of PCM conversion.

Digital Data Analysis

Review of the contents of the data forks (10) for the 35 TeleSleuth Jr. files in digital data analysis software revealed that they contained the identical number of bytes compared with the audio data portions of their respective PCM files. This was an indication that the data forks contained only the recorded audio data in the same format as the PCM files (monaural, 16-bit, 8820 Hz); however, the actual values of the audio data bytes differed for each pair of respective files. These differences were accounted for by the encryption employed by the recording system during the creation of the original TeleSleuth Jr. files.

It was also noted that while the number of encrypted audio bytes in a TeleSleuth Jr. file did not change after the file was subjected to a notch filter or gain change process, the actual values of the encrypted bytes were modified from their original encrypted values. Despite passing a subsequent "authenticate" process, resulting in a message indicating that "(t)he sound file… HAS NOT been modified," the audio data in the processed file actually did undergo modifications.

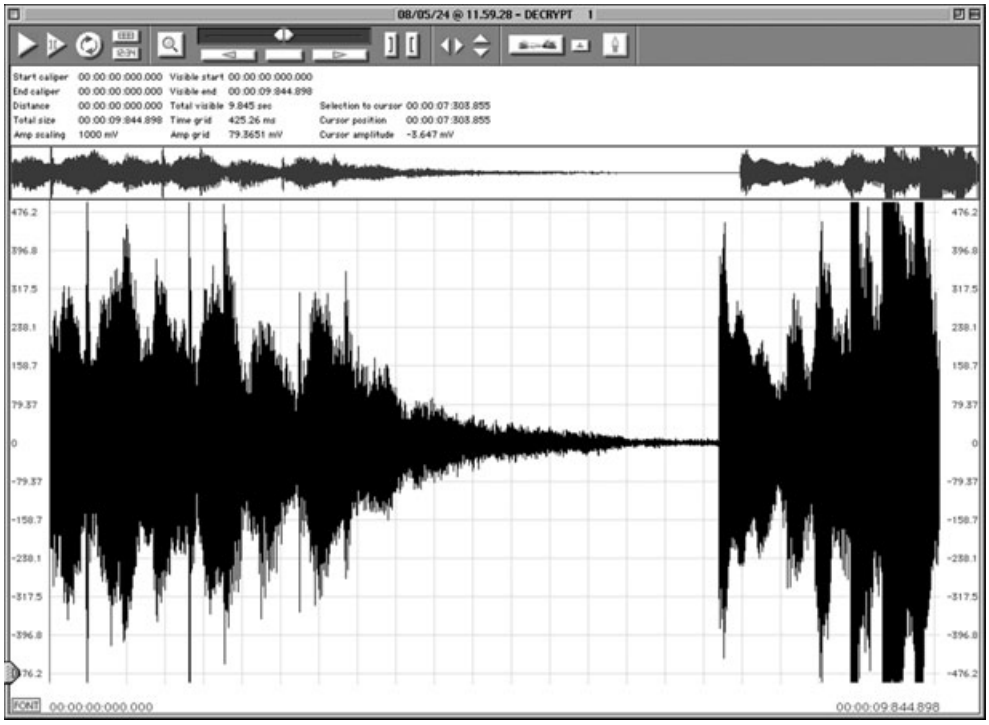

FIG. 3—*Forensic Audio Sleuth workspace for the same audio file as pictured in Fig. 2.*

Detailed byte-for-byte reviews and comparisons between the newly produced PCM files and the corresponding PCM files on specimen Qc2 corroborated the one quantization level absolute differences noted in the "Playback/Conversion Optimization" examinations. The values of the bytes associated with an audio sample exhibiting a difference were offset by ±1 quantization level.

Based on discussions with the computer forensic experts in this case, a history of changes made to the internal clocks of specimens Q1 and Q7 would not have been retained by the operating systems. Therefore, when clock settings are changed on these systems, there are no surviving records of the modifications.

Critical Listening

Critical listening processes were conducted with professional high-fidelity headphones and an external computer sound card system of both the TeleSleuth Jr. and the converted PCM wavefile copies of the 35 encrypted telephone recordings, using the following four steps: (i) a preliminary overview (as previously set forth); (ii) identification of possible record stops/starts, pauses, and edits; (iii) review of the background sounds; and (iv) examination of the louder foreground voices and other sounds (1). These listening analyses found that the 35 recordings contained only telephone conversations. The general quality and voice intelligibility were very high for telephone recordings, with very low-amplitude system noise, limited environmental noise, and almost undetectable nonlinear distortion (such as from over driven electronics or peak clipping). However, there were numerous "gaps," mostly between speech segments, which contained only low-amplitude, recording system noise and no telephone line information. It was also noted that some of the conversations were not recorded in their entirety and that most contained no telephone signaling events. In general, the recorded information had no aural indications of duplication degradations; added digital compression; obvious editing; record stops, starts or pauses; background or foreground discontinuities (except for the gaps); inconsistent room reverberation; unnatural vocal sounds; or high-amplitude 50 or 60 Hz components.

In addition, aural reviews were conducted of test recordings prepared using the TeleSleuth Jr. program, in which pause stop/start events were manually introduced during speech information and during segments with no high-amplitude acoustical input. These reviews indicated that the pause stop/starts themselves introduced no audibly detectable events, although the discontinuities in the recorded speech information introduced by the pauses were aurally obvious.

High-Resolution Waveform Analysis

Waveform analyses were performed of all 35 wavefiles, in their entirety, using a professional audio editing program, an on-screen computer display of time (horizontal axis) versus amplitude (vertical axis), a fast dual-video card, and a high-resolution monitor (2560×1600 pixel resolution). Additionally, using specialized waveform analysis software that utilizes the full resolution of the 1200 dots per inch resolution of a laser printer (not a "screen dump") (1), appropriate hardcopy waveform charts were prepared of pertinent events within the digital files.

These waveform analyses revealed numerous gaps with no high-amplitude recorded information, but only low-amplitude computer system noise (no voice, telephone system, or environmental sounds). A detailed review of all 35 files, whose total duration was exactly 6 h, 34 min, and 50.22 sec, revealed 6184 gaps, with each lasting 70 msec or longer. This equated to an average of one 70 msec or longer gap every 3.83 sec. There were also numerous gaps with lengths of less than 70 msec. Most of the gaps were determined to have root mean square amplitudes of *c.* −69 decibels (dB), which is 69 dB below the maximum amplitude of the digital file. Figures 4 and 5 are waveform examples of gap areas

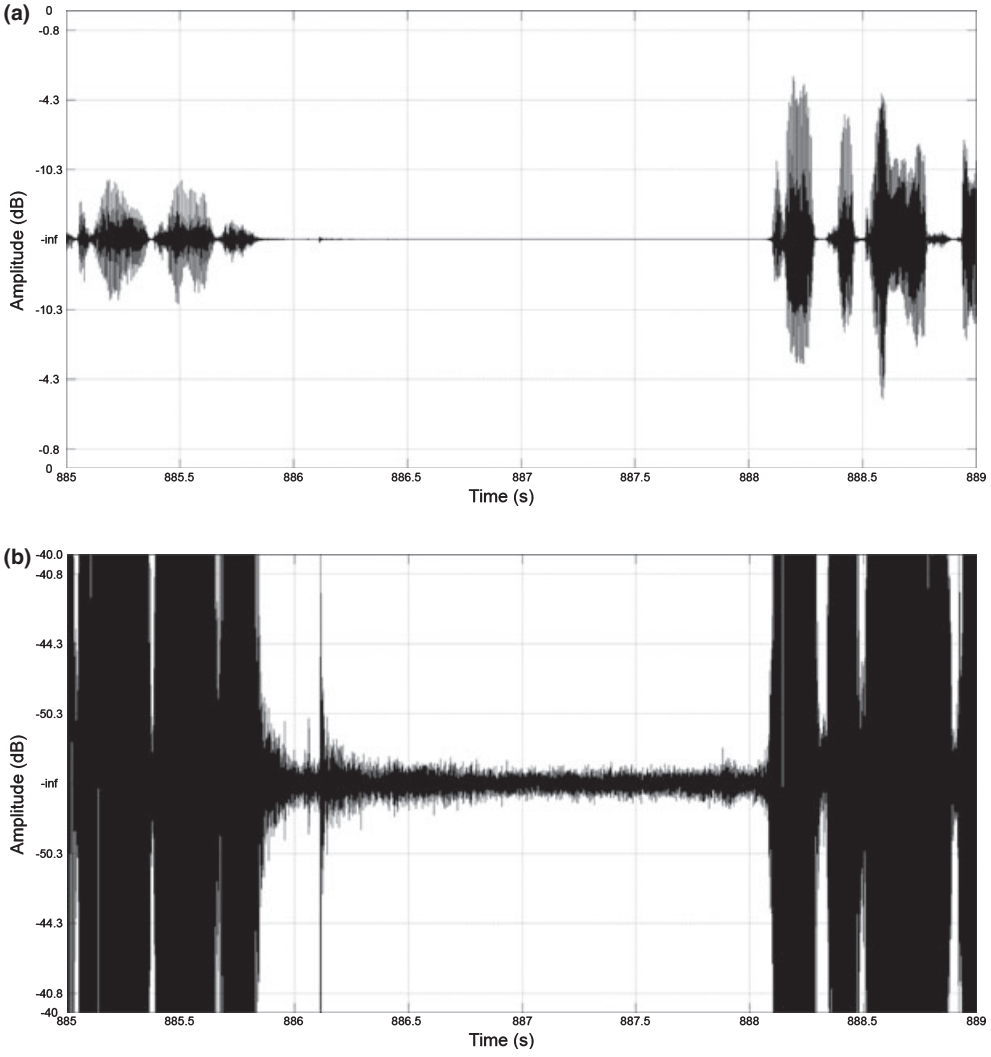

FIG. 4—*Waveforms of a single gap area between two speech segments at (a) 16-bit full scale amplitude and (b) 1/100th of 16-bit full scale amplitude. Time is represented on the horizontal axis over 4 sec, and amplitude is on the vertical in quantization levels.*

present in the examined files. The gaps contained low-amplitude, low-frequency noise, and limited sinewave information.

Detailed analyses of the pause stop/start test recordings prepared using TeleSleuth Jr. further revealed no noticeable indications of the events in the recorded waveforms. However, as with the critical listening examination, obvious waveform discontinuities were usually noted for those pause events introduced during recorded speech information. Further, the waveform analyses revealed no analog record events, no significant DC offsets, over driven or clipped samples, or obvious artifacts of digital editing.

Narrow-Band Spectrum and Spectrographic Analyses

Narrow-band spectrum examinations were performed on all 35 wavefiles, in their entirety, using a standalone, real-time, fast Fourier transform (FFT) analyzer, which displays frequency on the horizontal axis and amplitude on the vertical. The wavefiles were also analyzed in their entirety using sound spectrographic software, a fast dual-video card, and a high-resolution monitor (2560 × 1600 pixel resolution), with time displayed on the horizontal axis, frequency on the vertical axis, and amplitude/energy as gray scaling (1); appropriate hardcopy charts were prepared of pertinent events within the digital files.

The FFT and spectrographic analyses revealed that: (i) the far-party telephone talkers had a frequency range of *c.* 180–3700 Hz and the near-party PI's voice ranged from 100 to 3900 Hz; (ii) many of the gaps contained a comparatively higher-amplitude discrete tone of 15.75 Hz (Δ0.25 Hz); and (iii) some gaps contained very low-amplitude 60 and/or 120 Hz (Δ0.25 Hz) tones, which were usually masked in the nongap portions. The limited electrical network frequency and the 15.75 Hz discrete tone within the files were of insufficient quality and duration to allow meaningful phase analyses or comparisons to known references.

Conclusions

After completion of the audio authenticity examination, the authors concluded that the 35 TeleSleuth Jr. audio files contained on specimen Q7 could not be authenticated through published, scientific digital authenticity techniques. This decision was based on the following laboratory findings and observations:

- The proprietary recording software produced TeleSleuth Jr. files that, although encrypted, have no audio data complexity (consisting solely of raw PCM audio data) and an independent recording structure; that is, there is no dependence on recordings

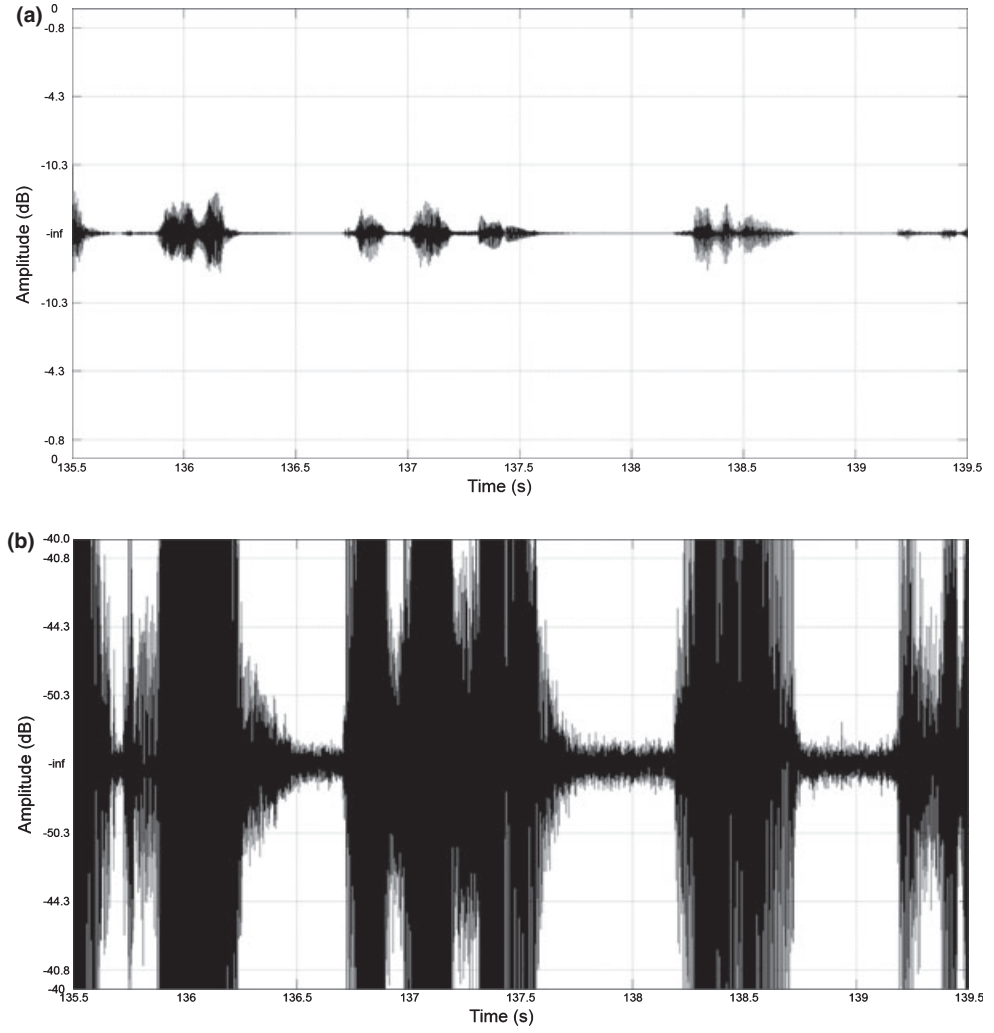

FIG. 5—*Waveforms of multiple gap areas between speech segments at (a) 16-bit full scale amplitude and (b) 1/100th of 16-bit full scale amplitude. Time is represented on the horizontal axis over 2 sec, and amplitude is on the vertical in quantization levels.*

made before, during, and after them. Therefore, no transcoding of the raw PCM audio data is required when using standard audio editing software, and individual recordings can be decrypted, converted, and deleted without deleterious effects on other recordings.

- Once decrypted, the TeleSleuth Jr. files are convertible to both the Forensic Audio Sleuth and PCM wavefile formats, which can be easily edited through the use of Forensic Audio Sleuth or audio editing software available on either specimen Q1 or Q7. This editing could have produced changes to the audio information, which would not be detected by the published audio authenticity protocol.
- There were over 6000 gaps in data lasting 70 msec or longer (and numerous shorter gaps) that only contain low-amplitude system noise, with no voice, telephone system signaling, or environmental sounds. These gaps are the ideal places to electronically edit the recordings without detection, and these edits, if performed appropriately, would not be detected with the published audio authenticity protocol.
- The pause stop/start events themselves, as produced by TeleSleuth Jr., were not detected by any of the measurements or observations made. This means the recordings could have been paused and restarted during the original recording processes by the operator, without being identifiable during the authenticity examination.
- A simple rerecording process using TeleSleuth Jr. or a more complex, direct file manipulation would reproduce or modify the metadata information, such that it was consistent with the original file. If the rerecording method was utilized, an individual could easily change the clock settings on the Mac computer beforehand to replicate the date and time of an edited file to match the original digital file.
- The original, unaltered files and any copies on the hard drives or other media could have been appropriately deleted to avoid later detection and recovery by computer forensic experts during their imaging and analysis processes. Even without these measures being taken, the authors were advised by computer forensic experts in this case that the nature of the Mac operating systems prior to OS 10.2 (10,11), combined with the proprietary, encrypted format of the TeleSleuth Jr. files, created a scenario in which usable recovery of any deleted files would be extremely difficult, if not impossible.

As an example of a process which would produce an edited TeleSleuth Jr. file that would go undetected when analyzed using the described protocol, an original TeleSleuth Jr. recording could be

opened and converted to the Forensic Audio Sleuth format using the Forensic Audio Sleuth software present on a separate Mac system from the one which recorded it. The file could then be edited by removing a segment of voice information using the gap areas as start and end points. The edit points would be chosen carefully such that the underlying system noise present in the gaps is "continuous" through the edit. Artifacts which forensic examiners look for when identifying alterations, such as phase differentials for discrete tonal sounds and unnatural transitions between consecutive samples, would not be present in this properly edited file. Following the production of the edited file, the analog audio output of the Mac system used for the editing process could be cabled directly to the analog audio input of the Mac system containing the TeleSleuth Jr. software. The clock of the Mac system containing the TeleSleuth Jr. software would be changed to some point just ahead of the date and time that the original telephone call was placed and recorded. At the appropriate time, playback of the edited file and a new recording on the TeleSleuth Jr. system would be initiated, producing a new recording which appears to have been produced at or around the date and time of the original recording. Deletion of the original file and the edited intermediate file(s), followed by "cleaning" processes on the hard drives and other media, would then be performed to remove recoverable remnants of the prior files. The clock of the Mac system containing the TeleSleuth Jr. software would then be reset, as appropriate. The modified recording, having been rerecorded and converted back into the TeleSleuth Jr. format, would then pass the "authenticate" feature of the TeleSleuth Player software.

Numerous test recordings were prepared following the example process above and analyzed using the described protocol. Despite knowing the exact editing processes that occurred, the edits could not be detected. Further review of the newly created TeleSleuth Jr. files and specimens Q1 and Q7 by the computer forensic experts in this case revealed no artifacts of the editing processes.

The authors provided expert testimony and presented demonstrations at trial regarding their authenticity procedures, results, and conclusions.

Discussion

The authors wish to stress the uniqueness of this case, which is based considerably on the PI's direct involvement with the development of the encrypted audio format, his experience in the field of forensic audio authenticity analysis, and the ease with which the audio files could be accessed, converted, edited in the gap areas, and reconstructed in such a way that the processes were undetected. These distinctive features, and the direct analysis of the recordings themselves, led to the authors' opinion that the 35 audio recordings could not be scientifically authenticated through accepted forensic practices.

Acknowledgments

The authors wish to thank the following individuals who reviewed this case report and provided important technical and grammatical improvements: Suzana Galić Price (BEK TEK LLC, Clifton, Virginia); Catalin Grigoras (National Center for Media Forensics, University of Colorado, Denver, CO); David J. Hallimore (Forensic Audio/Video Laboratory, Houston Police Department, Houston, TX); and Jason Ferridge (Victoria Police Forensic Services Department, Victoria, Australia).

References

1. Koenig BE, Lacey DS. Forensic authentication of digital audio recordings. J Audio Eng Soc 2009;57(9):662–95.
2. Koenig BE. Authentication of forensic audio recordings. J Audio Eng Soc 1990;38(1/2):3–33.
3. Bolt RH, Cooper FS, Flanagan JL, McKnight JG, Stockham TG Jr, Weiss MR. Report on a technical investigation conducted for the U.S. District Court for the District of Columbia by the Advisory Panel on White House Tapes. Washington, DC: U.S. Government Printing Office, 1974:8–11, TN 1.1-15, TN 2.1-2.37.
4. *United States v. Anthony Pellicano, et al.*, CR 05-1046(E)-DSF (2005).
5. Third Superseding Indictment [CR No. 05-1046(C)-RMT], http://www.justice.gov/usao/cac/pressroom/pr2006/Pellicano_Indictment.pdf. (2005) (accessed July 28, 2011).
6. Mrozek T. Terry Christensen, Anthony Pellicano convicted of federal conspiracy and wiretapping charges [press release]. Central District of California: United States Attorney's Office, 2008; Release No. 08-123.
7. Pellicano AJ. Forensic audio tape analysis and the defense lawyer, part II. VOICE for the Defense, 1989.
8. Gruber JS, Poza F, Pellicano AJ. Trials: audio recordings: evidence, experts and technology. Rochester, NY: Lawyers Cooperative Publishing Co., 1993.
9. Audio Engineering Society. AES43-2000, 2000: AES standard for forensic purposes—criteria for the authenticity of analog audio tape recordings. New York, NY: Audio Engineering Society, Inc., 2000.
10. Kokocinski A. Macintosh forensic anlaysis. In: Casey E, editor. Handbook of digital forensics and investigation. Burlington, MA: Elsevier Inc, 2010;353–82.
11. Burghardt A, Feldman AJ. Using the HFS+ journal for deleted file recovery. J Digital Investigation 2008;5(Suppl. 1):S76–82.

Additional information and reprint requests:
Bruce E. Koenig
BEK TEK LLC
12115 Sangsters Court
Clifton, VA 20124-1947
E-mail: BEKTEK@cox.net
Website: www.BEKTEKLLC.com