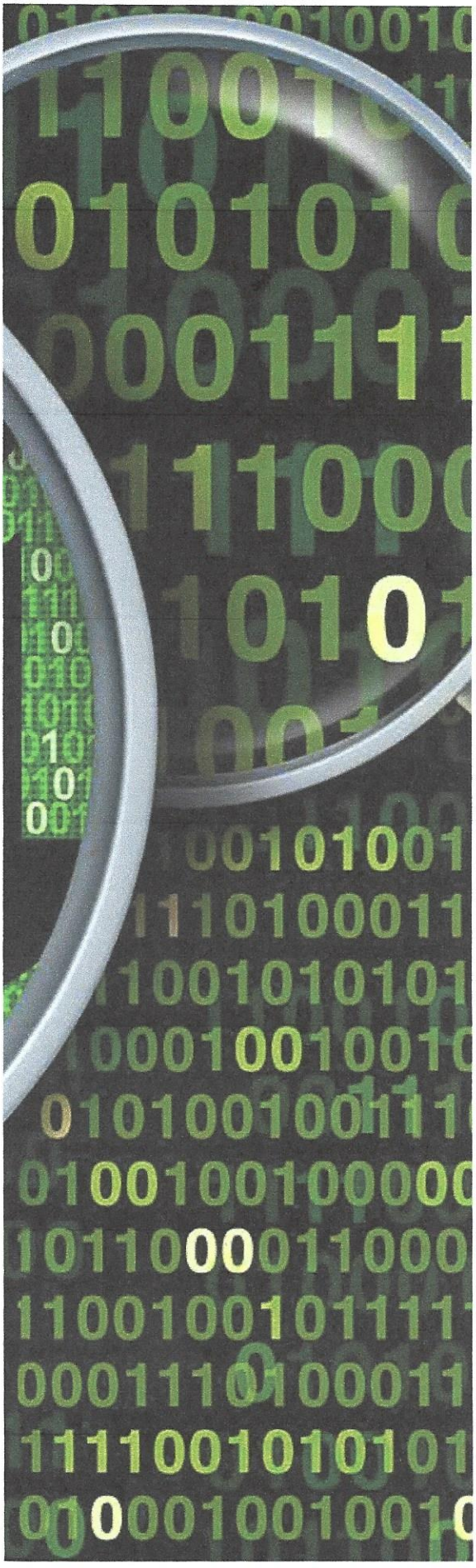


The Digital Detectives

The Key to Understanding Digital Evidence

BY **JENNIFER E. OWEN**

In today's world of non-stop selfie snaps, Instagram and Facebook posts, CCTV surveillance, dashcams, and cellphone use, recorded evidence has become an essential part of most investigative practices. When dealing with multimedia evidence, the "digital detective" needs to understand what is actually possible and what is the "CSI effect." The "CSI effect" occurs when the average person watches too many crime shows and believes that video enhancement takes two seconds, all license plates are recoverable and a newspaper can be magnified to read the headline three miles away — and all of this is possible before the first commercial break. The information in this article will assist you in achieving a better understanding of digital, audio and video evidence, and help you to separate fact from fiction.

Forensic Audio: Audio enhancement is the process of "cleaning up" the audio recording to improve and clarify audible intelligibility of the recording. Important evidence is often recorded in real-world situations and not pristine audio conditions. Most problems that need to be addressed in audio may include:

- Removing hum, static and background noise
- Isolating and amplifying speech
- Decreasing or removing unwanted traffic noise, restaurant chatter and the like
- Increasing intelligibility of the speech recorded

Most investigators contact me with poor digital recordings that have been recorded on a handheld device. There may be the presence of air conditioning hum, traffic, competing voices and poor volume levels. Due to these recording problems or poor acoustics, the speech needs to be clarified to a level of intelligibility. The solution is sometimes simple — enhance the recording using digital software to correct speed playback problems, increase volume, decrease noise, rumble, hisses and echoes and isolate specific dialogue from noisy backgrounds.

One of the most common problems Owen Forensic Services encounters is when someone with no audio experience downloads free software and tries to enhance a recording themselves. This usually results in overzealous processing and can actually insert audio artifacts and sounds that shouldn't be there or may mimic speech that was never there to begin with. Another common misconception is that audio can be enhanced to crystal-clear perfection. No, that's another "CSI effect." You cannot eliminate ALL noise or you may eliminate speech.

Upon receipt of the audio materials, it is best-practice to have them in a file format that does not use compression. Compression degrades the quality of the recording. Most recordings such as MPEG or MP3 use compression schemes. In simplest terms, when audio is compressed, artifacts are added to the recording and there is a reduction of intelligibility. Artifacts are small flaws created by the loss of actual data when compressed. You are already starting with an inferior recording if it is compressed. A WAV file format is the best quality of an audio file. If the original recording was recorded in a digital format, a copy can be used. Do not convert audio files to lesser file formats such as MP3s to send via email just to save space. If possible, have the audio files in a WAV file format sent on a CD or flash drive for enhancement.

Audio Authentication is an analysis of recordings to detect insertions, deletions, alterations, over-recordings or any other acoustic anomaly that is present during the recording. Indicative of this are missing parts of speech, issues with continuity of conversation, multiple clicks or pops, stops and restarts of the recording, multiple pauses, or complete dropouts and resumption of the audio. In digital recordings, most recorders leave "digital signatures" in the waveform (a graph display that visually records time and amplitude of sound). A professional familiar with editing audio software can make insertions and deletions that may not be detected by the average person. This has necessitated the use of intricate and sophisticated software used by forensic audio experts to detect these edits.

Forensic Transcription: Once an audio enhancement has been done, sometimes certain key phrases will still be of marginal quality. Forensic transcription is a focused transcript of words spoken.

Owen Forensic Services often receives videos with poor audio quality — especially common with police interviews. Today's technology makes it possible to enhance the audio on the video track without disturbing the synchronization of the video. Audio tracks from videos can also sometimes be tampered with and synched back to the videos with no obvious alterations. Forensic audio experts have various tools at their disposal to detect these alterations and identify modifications made to the video.

Digital video surveillance systems are becoming standard for most businesses. When there is an incident that occurred and the evidence needs to be produced from the proprietary player, I strongly suggest that you hire a forensic video expert who can extract the video and ensure the integrity of the file. If there is the option to export the video from the proprietary player, then that is what should be done to ensure the highest-quality video possible.

File Verification and the steps taken to procure video evidence need to be documented and the system photographed from all angles. One of the most important documents is the manual to the system. Use the manual to avoid mistakes in extraction and production of files. Run file hashes and other file verification software to protect the integrity of the file. Also, just like audio, a video that is compressed will not be the same level of quality as an uncompressed video. If possible, always try to obtain an uncompressed file format for video.

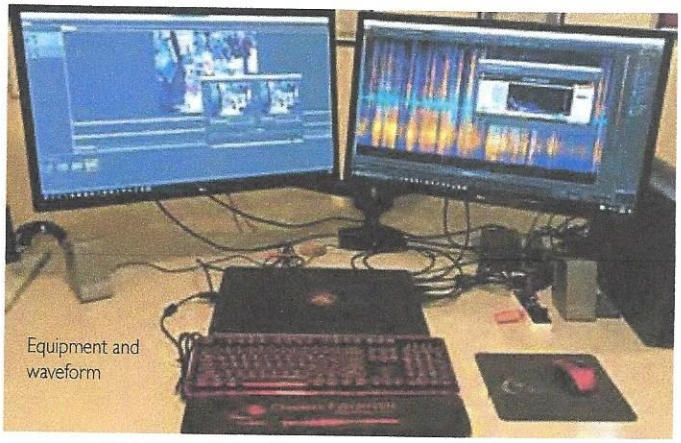
Once the video is retrieved, the next step is usually enhancement of the video. When performing **Video Enhancement,** some common issues include:

- Stabilizing video frames, correcting the "shake" of the video
- Exposing images that are too dark to see
- Enhancing and defining personal characteristics of individuals (tattoos, scars, etc.) or their belongings (make and model of car, license plate, etc.)

Once a video has been processed and enhanced (always on a working copy, never the original) the area of interest of the incident becomes the focal point of the investigation. Still images are then taken from the video and should be saved in an uncompressed format such as BMP or TIFF for optimal visual quality. **Image Clarification** of a single image or photo is sometimes crucial to the investigation. Spotlighting weapons, slip and fall accidents, and other areas of interest are all part of today's recorded evidence investigation. The presentation of these still images is an effective way to present to a jury or to submit as exhibits along with a report.

Another aspect to verifying authenticity of images is to check the integrity of the images. **Image Analysis** is invaluable. There is data that can be obtained from photos to verify if the image has been modified.

A forensic tool that works in conjunction with video and image enhancement is **Photogrammetry.** Photogrammetry is defined as "the science and technology of obtaining reliable information about physical objects and their environment through the process of capturing, measuring and interpreting photographic images." For example, a suspect's height can be determined if there are known measurable objects in the same location where the incident took place.



Equipment and waveform

Video Authenticity Analysis can also be conducted to establish if a video has been tampered with. Insertions, deletions, over records and various alterations can be detected just like in audio authentication.

A common request is **voice identification, speaker comparison or voice analysis**. This analysis is a combination of the aural spectrographic method and biometric voice identification. The aural spectrographic method has been accepted in the courts since the 1960s. The spectrographic method relies on many different factors for comparison: pitch, dialect, inflection, articulation, syllable coupling, critical listening and unique speech characteristics. The biometric voice identification analysis uses pitch statistics, spectral formant method and the Gaussian mixture models to compare voice samples. The difference is that this methodology relies more heavily on the statistical data it produces. Combined, both methodologies may give better insight and can be used as an investigative tool for identification, elimination, or to narrow the suspect pool.

Presenting audio and video evidence in a courtroom can be challenging depending on the equipment available. It is always best evidence to bring high-quality speakers for audio (not the ones on your laptop), and a high-quality monitor where the jury can see significant detail in the visuals you will show. All demonstrative evidence should not be connected to the internet (where a drop connection could potentially occur in the middle of your presentation) and make sure your computer's updates are current to avoid reminders popping up during your presentation. It's also important to make sure your desktop is orderly and does not have personal screensavers that day.

As advocates for evidence, the digital detective has a duty and responsibility to provide clients with the best possible service. All investigators should have a basic understanding of each of these services that will assist with your client's recorded media, further their objectives with fact-based evidence to support their claims, and ensure the integrity of their media has not been compromised. **PI**

Jennifer E. Owen of Owen Forensic Services, L.L.C., maintains a state of the art facility for the purposes of digital audio enhancement, digital video enhancement, digital audio and video authenticity analysis, image analysis, voice identification, speaker comparison and media/data recovery. The company provides forensic consulting, examination, expert testimony, and over 25 years of experience in analyzing, enhancing, authenticating all recorded evidence for presentation in court. Their hardware and software are the latest that technology has to offer. Their specialty is providing clients with powerful demonstrative evidence and fact-based testimony.