

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

UNITED STATES OF AMERICA,
Plaintiff,

v.

Criminal Case No. 10-CR-148-BLW

EDGAR STEELE,
Defendant.

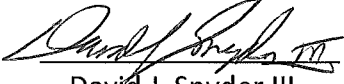
Affidavit of David J. Snyder III

I, David J. Snyder, III., being duly sworn, depose and say as follows, based on information and belief, the source of which is my training and experience with the FBI in the Forensic Audio, Video and Image Analysis Unit as a Forensic Audio Examiner for 11 years. I have been admitted as an expert in the disciplines of audio enhancement, analog and digital authenticity in Federal, State and Local courts on several occasions. I have a BS degree in Electronics Engineering Technology and an AS in Electrical Engineering Technology.

1. Duplicate copies of the recordings listed as 1D1 (6/9/10) and 1D2 (6/10/10) by the Federal Bureau of Investigation were provided to the defense in the proprietary format with a version of the proprietary player.
2. The files on 1D1 (6/9/10) and 1D2 (6/10/10) also have "hash values," which are obtained by using a mathematical algorithm to produce a 32-character string value, similar to a finger print, which uniquely identifies the original data. By comparing the original file's hash value against the hash value of any purported copies of the original file, an examiner can quickly confirm whether the copy is a true, complete and accurate copy of the original. The reliability of hash values is well-established within the computer software, computer forensic examiner, audio forensic examiner and video forensic examiner fields. The hash values of the original file matched the copies provided to the defense.
3. The audio recorder used to produce the recordings referenced above was a Flex8F audio recorder.

4. Audio recorded on the Flex8F recorder cannot be monitored or reviewed until it is transferred from the recorder to a computer workstation. A recorder can be connected to a computer workstation to view the session log, but the audio cannot be monitored or reviewed as a feature to protect against tampering. If the recordings are not transferred additional recordings can be added to the recorder.
5. Once recordings are transferred to the computer workstation, the recorder must be erased before new recordings can be produced, also as a hardware protection against tampering.
6. Files transferred from the recorder can be written directly to write-once media, such as a CD-R or DVD-R, as an additional protection against tampering.

I declare under penalty of perjury that the foregoing is correct on this 15th day of September, 2011.


David J. Snyder III