# AN INVESTIGATIVE APPROACH TO CONFIGURING FORENSIC ELECTRIC NETWORK FREQUENCY DATABASES

by

Christopher William Jenkins

B.S., University of Colorado Denver, 2009

A thesis submitted to the

University of Colorado Denver

in partial fulfillment

of the requirements for the degree of

Master of Science

Media Forensics

2011

This thesis for the Master of Science degree

by

Christopher William Jenkins

has been approved by

_____

Catalin Grigoras

_____

Jeff M. Smith

_____

Jan Bialasiewicz

_____

Alan J. Cooper

_____

Date

Jenkins, Christopher William (M.S., Media Forensics)

An Investigative Approach to Configuring Forensic Electric Network Frequency Databases

Thesis directed by Associate Professor Catalin Grigoras

ABSTRACT

This thesis is an investigative approach to the configuration of Electric Network Frequency (ENF) databases that are built with the intent to provide an accurate, reliable, and reproducible source of electric network frequency variations to be used in scientific research and forensic examinations of digital multimedia. For the ENF Criterion to reach full potential in the United States, forensic best practices, database cross-validations, and widely accepted methodologies should be maintained. This thesis will help guide forensic researchers in configuring ENF databases in a manner that reinforces those goals. Through an investigative approach, various elements of an ENF database are explored. The introduction of this thesis starts with a broad overview of general forensic science, then narrows the focus to defining media forensics, and finishes with background on the ENF Criterion. Chapter two reviews the available scientific literature on the ENF Criterion. Chapter three investigates several elements of an ENF database and explains how they can be used to configure a more robust, reliable, and reproducible forensic ENF database. Chapter four proposes a system of broadcast type ENF databases where ENF is gathered in one location and received in a remote location. Chapter five draws the conclusions. Appendix A describes voltage regulated ENF sources, appendix B outlines a real case application of the proposed ENF database configuration, and appendix C explains why and how ENF works.

This abstract accurately represents the content of the candidate's thesis. I recommend the publication of this thesis.

Signed_____
Catalin Grigoras

# DEDICATION

I dedicate this thesis to my sister, Jessica, who always kept my best interests in mind, encouraged me to think things through to the end, and gave me unfaltering support in pursuing my passions. Jessica's heart was always in the right place and she continually went out of her way on my behalf, and for that this dedication is the least I can do to show my gratitude. I also dedicate this thesis to my father, William, who consistently encouraged creative thought and taught me to never let go of my dreams. I also dedicate this thesis to my loving mother, Stephanie, who motivated me when I was discouraged, gave me hope when I felt helpless, and kept me focused when I would lose sight of my goals.

I could not have realized my accomplishments without the love, support, and guidance of my family, and for that I am eternally grateful and dedicate my thesis work to them.

## ACKNOWLEDGEMENT

I would like to acknowledge and express special thanks to my thesis advisor, professor, and friend, Catalin Grigoras for his uncanny dedication to his students in ensuring we were his first priority, for his unlimited patience in helping me to understand, and his constant motivation in encouraging me to push the boundaries, think outside the box, and find creative solutions. I would like to extend a kind acknowledgment to Jeff Smith for his continued guidance throughout the program and his dedication to organizing the internship. I would also like to acknowledge Alan Cooper for his valuable participation, detailed explanations and thoughtful insights. Alan was always quick with a response and thorough with an answer. I would like to express thanks to Tom O'Brian of NIST for taking the time to answer my questions with germane explanations and invaluable perspective.

It is my pleasure to extend a very special thank you to the entire team at Target Forensic Services Lab, who provided me unbridled creative space in their laboratories and supplied me with every resource I needed to conduct my research during the internship.

Last but certainly not least, I am pleased to extend a most heartfelt thank you to my friends Tony Bernal, Allysa Jordan, Tara Petty, and Jake Montenegro. Tony always provided me a helping hand without hesitation and together with Allysa and Tara they took care of my beloved dogs, Jericho and Beretta, while I was out of state on the internship. Jake watched after my house while I was gone which kept my mind at ease and he always provided thought provoking insights into my research. I cannot express enough gratitude to my friends for ensuring that my dogs, my house, and the life I put on hold would be there waiting for me when I returned from my thesis semester/internship program.

I could not have completed this thesis without each and every one of the people mentioned here and for that I am grateful beyond words.

TABLE OF CONTENTS

FIGURES

Figure

TABLES

Table

## 1. Introduction

As a disclaimer, I do not endorse any of the products or software presented in this thesis. I do not have any financial interest or connections with the products or software presented in this thesis. I am in no way affiliated with the companies that produce the products or software presented in this thesis. The products or software presented in these slides are only mentioned as tools for forensic analysis and the intention of this thesis is solely educational.

This thesis is about Electric Network Frequency (ENF) databases and how they can be configured to provide accurate, reliable, and reproducible results for use in scientific research and forensic examinations of digital media. Before jumping straight to the complex interworking of the ENF Criterion and what a forensic database means, a general overview of forensic science is presented. Then the focus is narrowed to describe media forensics, and then further focused to audio authentication, and finally an introduction to the ENF criterion is presented to help the reader understand how ENF came about and why a forensic database is necessary. The reader will gain a broad understanding of forensics and how audio authentication is used in the field.

### 1.1 Introduction to Forensic Science

The Merriam-Webster dictionary defines "forensic" as "*relating to or dealing with the application of scientific knowledge to legal problems*". The same dictionary defines "science" as "*knowledge or a system of knowledge covering general truths or the operation of general laws especially as obtained and tested through scientific method*" [36]. Logically it would follow that "forensics" is the argumentative science of applying a system of knowledge to solve legal problems. Forensics is a combination of several scientific fields to aid in the discovery of facts for answering legal disputes. From anthropology to zoology, there is a forensic application for almost every scientific discipline today but the history of applying science to answer legal questions has a history almost as old as jurisprudence itself. Some sources place the first applications of forensics as far back as 700BC when the Chinese used thumbprints in clay sculptures and on documents to preserve the identity of one's possessions [37]. In 250BC Greek physician, Erasistratus, noticed that the heart rate of his patients would rise when they were lying [38]. Roughly around 1235AD Chinese author Song Ci published the first literature on applying medical science to solve crimes involving death [39]. One of the most recognized early applications of forensic science in a legal dispute leading to a conviction comes from France where in

1840AD Mathieu Orfila found traces of arsenic in the body of Charles Lafarge after conducting the Marsh exam, this evidence led to the conviction of Lafarge's wife for murdering her husband [40].

Throughout history, forensics has helped people understand how events took place by applying scientific reason to the scene of a crime as well as helping judges and juries to understand where the accountability of events should lie by making identification, comparison, and authentication possible through the science of DNA, fingerprints, handwriting, ballistics, and the list can be extended. Forensics has aided legal disputes for centuries in several types of legal systems from Roman law to Napoleonic Code to Religious law and eventually spawning out into what the Western world knows today as the two basic concepts of law, adversarial and inquisitorial. The adversarial system descends from common law and the inquisitorial system descends from civil law. Forensics will continue to aid the trier of fact in any legal system well beyond our lifetimes and even in legal systems not yet imagined because applying scientific knowledge to legal problems is the most logical way to discover the truth of the matter.

The adversarial system of law governs the United States, which allows for both sides of a dispute a fair chance to pose their argument in front of a judge and jury. In most circumstances the jury is the trier of fact ultimately making the decision about the outcome of the dispute. In some instances, such as most traffic violations, there is no jury and the plaintiff makes their case without representation to the judge alone. In more complex disputes such as murder trials, civil hearings, and child pornography cases; attorneys commonly utilize a wide range of outside perspective on the case in the form of expert testimony to elaborate their point. In the adversarial system experts enter the court after going through a deposition or Daubert hearing or some hybrid of a Daubert/Frye voir dire hearing depending on the state [41]. At which point the expert is allowed to testify as to their opinion of the matter based on the scientific conclusions they have deduced from analyzing the evidence in the case. Many forensic analysts find themselves on the witness stand at some point in their careers, testifying about the work that they have conducted and offering their opinions in an unbiased manner to the jury.

The expert's opinion will ultimately play a partial role in the jury's decision about the case. The jury is faced with the task of weighing the opinions from all the experts, other witness testimony, and evidence of the case into their ultimate decision. In a Daubert hearing the judge holds the role of "gatekeeper" making the decision about whether or not to allow a witness to testify in front of

the jury as an expert. In addition to measuring the relevancy of an expertise, during a Daubert hearing, the trial judge measures the reliability of an expert's testimony against this non-exclusive checklist: the expert must be able to demonstrate the theory or technique is falsifiable, refutable, and testable; the basis of their opinion has been subjected to peer review and publication; the techniques used in arriving at such conclusions have a known or potential error rate; there are existing methods and maintenance of standards and controls concerning the operation of those methods or techniques; or the theory and technique is generally accepted by a relevant scientific community [42]. Providing proof of a majority of these five Daubert standards is relatively easy and a forensic examiner can be qualified as an expert with a minimal amount of training on the subject, this however, does not mean that a minimal amount of training should be acceptable or that the Daubert standards should be taken lightly.

The Frye standard on the other hand, states that the basis for the expert's opinion must be sufficiently established to have gained acceptance in the particular scientific field [43]. The United States Supreme Court's opinion on this matter came from an expert attempting to use the systolic blood pressure deception test as a basis for his deduction. The court held that the testimony was inadmissible and the defendant was found guilty of second degree murder. Some states in the US still uphold the Frye standard but the majority of US states have adopted the Daubert standard.

There is no clear-cut generalized standard for the level of education a forensic examiner must have, thus some forensic disciplines require more training and certification than others. Latent print analysis for example, is a position that an examiner holding a certificate from a one-semester community college course and a one-year internship can find themselves sitting. Forensic psychology on the other hand, is a field where having an advanced degree such as a PhD, EdD, or PsyD, will be required to make it past the Daubert/Frye/voir dire. Recently more attention has been paid to the field of forensics and the judicial impact of an expert's testimony in general; the industry is starting to trend toward educational requirements across the board. In 2009 a congressionally mandated report was generated by the National Academy of Sciences (NAS Report) declaring that there are serious deficiencies in the nation's forensic science system [44]. The report elaborated by making a call for major reforms concerning new research, mandatory certification programs, and stricter protocols for analyzing and reporting on evidence, as well as the gradual shift of forensics out of law enforcement and into the private sector. Any changes

that come as a result of the NAS report will take several years to come to fruition but forensic agencies should be aware of the implication in the NAS report. Forensics can have a positive impact on the outcome of a case by providing concrete interpretations of the evidence leading to the conviction of a perpetrator or the release of an innocent suspect. On the other hand, forensics can have catastrophic impacts on the judicial system by providing wrong, biased, or misinterpreted results leading to the conviction of an innocent suspect or the release of guilty perpetrator. Forensics is a discipline with a high magnitude of responsibility, a discipline that should require a minimum education at the master's level, as suggested in the NAS report. To further illustrate this point a few landmark cases will be presented where forensic science failed to provide solid scientific findings and had irreversible impacts on completely innocent people.

Case 1: Scotland, United Kingdom, 1997 [45]. Murder case of Marion Ross. A fingerprint was found near the victim's body that led detectives to believe that Shirley McKie, Scotland Police Officer, had entered a restricted area of the crime scene. This event sparked a chain-reaction that would eventually lead the well-respected officer to a life of fear and isolation. David Grieve, US fingerprint expert who was called upon to cross examine the findings in the Marion Ross murder case, once commented on finger print analysis by stating that:

> "*Errors of this magnitude within a discipline singularly admired and respected for its touted absolute certainty as an identification process have produced chilling and mind-numbing realities. Thirty-four participants, an incredible 22% of those involved, substituted presumed but false certainty for truth. By any measure, this represents a profile of practice that is unacceptable and thus demands positive action by the entire community*" [46].

Shirley McKie, victim of judicial error by wrongful forensic science in the Marion Ross case, was acquitted after Mr. Grieve gave his testimony. Eventually McKie was compensated £750,000 but not until after her lively-hood, career, and personal life had been completely devastated by embarrassment, cover-up, and false accusations. To this day McKie lives a quiet life working in a friends shop and avoiding police at any cost due to the phobia she has developed from the trauma that nearly drove her to divorce, abandonment, and suicide.

Case 2: Madrid, Spain, March 11, 2004 [47]. A series of explosions targeting the mass-transit train system brought Europe to a screeching halt. Less than a month later on May 6th the United States Federal Bureau of Investigation (FBI) arrested an Oregon attorney, claiming that a fingerprint found on a backpack near the bombings belonged to Brandon Mayfield. Mayfield was held for more than two weeks as a material witness in undisclosed locations with no contact to legal counsel or his family. Even after Spanish authorities found the finger prints to belong to someone other than Mayfield, the FBI persisted in their prosecution of Mayfield. Eventually, when Spanish authorities released their position on the matter, international news spread to the US and the FBI released Mayfield. A series of lawsuits ensued from Mayfield's counsel in the Supreme Court, eventually compensating Mayfield 2 million dollars. Luckily for Mayfield his wife and family stood by him throughout this ordeal. Unfortunately, many wrongfully convicted people leave prison to find that their spouses have remarried, their children have left, and their family has abandoned them, leaving them with nothing except an extremely difficult to expunge criminal record that blocks them from decent jobs and homes.

Case 3: Dallas County, Texas, 1985 [48]. Finger print analysis is not the only forensic science that has led to judicial errors. Media forensics has been misused in several cases and has led to the wrongful convictions of completely innocent people. On February 4, 1986 David Pope was brought to trial for the aggravated sexual assault of a Texas woman. A man had broken into the woman's apartment, held a knife to her throat, and raped her. After the attack, the rapist called her several times over the phone and she worked with police to record the phone calls. The woman wrongfully identified Pope in a line up claiming that his hair color was similar to her attacker's. Larry Howe Williams, a Houston Police Officer, conducted a voice-print analysis and comparison of the phone recordings made by the woman and voice samples taken from Pope. Williams had completed a 2-week voice print identification course in Somerville, New Jersey on voice-print analysis and was a member of the International Association of Identification which was enough to satisfy the requirements to enter the court as an expert on the subject. Williams was wrong in his analysis and contributed faulty science to a case that led the jury to find Pope guilty. After serving 15 years in prison for a crime he had nothing to do with, Pope was exonerated on February 2, 2001 becoming the first person exonerated through DNA testing in Dallas County.

Case 4: Romania, March 21, 2011 [49]. An expert, George Pop, working for the Romanian Ministry of Justice submitted his forensic report to the

Romanian Supreme Court of Justice in criminal case number 10753/1/2008. EdiTracker was used in the expert's analysis of the authenticity of a digital audio recording. In the EdiTracker program, a Russian software based on non-validated methods, digital audio shall be native 44.1kHz. The evidence recording was up-sampled from 8kHz. The expert claimed that up-sampling the signal did not introduce any distortions to the evidence. However, in figure 5 of the experts report a graph shows the spectrum of the up-sampled signal with nearly 15dB FS (Full Scale) amplification between 4kHz and 6kHz. The up-sampling jeopardized the integrity of the evidence when this process introduced these kinds of signals between 4 kHz and 6 kHz, and more than that, the up-sampling from 8 kHz to 44 kHz added new samples to the signal, new frequency components, and masked potential previous traces of manipulation. The distortions introduced by up-sampling the signal were evident, it is not clear if the expert did it because he didn't know how to deal with basic signal processing or if he counterfeited the recordings for the prosecution, the Court refused to provide the defendant a clone of the evidence recordings, and no further investigation has been open against the expert.

Case 5: Romania, June, 30 2011 [50]. Another forensic report from the Romanian Ministry of Justice was submitted in the Court of Appeal Brasov criminal case number 6367/2/2010. In this report Pop was trying to answer to the argument that opposing counsel had risen about the necessity to up-sample digital audio so that it can be used in EdiTracker. The expert sent an email to the STC developers of EdiTracker, asking them to please clarify the issue. In the email response, the STC EdiTracker developers stated that: "…*you should have the file sampling rate* ***over*** *44.1 kHz*…". But when the expert translated this email from English to Romanian for his Expertiză Criminalistică he stated that: "…*you should have the file sampling rate* ***lower*** *than 44.1 kHz*…". This is a case of expert unfairness and will ultimately have unfortunate judicial implications.

Case 6: Boise, Idaho, April 21, 2011 [52]. Dennis Walsh, a former New York City detective and self-proclaimed audio examiner was rejected as an expert by US District Judge Lynn Winmill in the Edgar Steele Conspiracy case. Steele was accused of conspiring to hire a hit-man to murder his wife and mother-in-law after a pipe bomb was found attached to the underside of his wife's car and the hired hit-man confessed to the FBI. An audio recording of a conversation between Steele and the hit-man had its authenticity brought into question and Walsh conducted an analysis of the audio for the defense. Walsh used EdiTracker in his analysis and the Judge ruled that: "*I just have to conclude he does not have the background and experience*" after noting that the

qualifications on Walsh's CV had been inflated and that key-points in the report duplicated the other proposed expert's report verbatim, and that Walsh does not hold any education or certification as a forensic examiner. Dave Snyder, certified forensic examiner and electronics engineer for the FBI stated that: "…*the uncertified, Russian-made testing program (EdiTracker) that Walsh used detected several anomalies but the program is unreliable – and that's why the FBI doesn't use it*".

Case 7: Romania, November 16, 2009 [51]. Truică-Zevedeanu Alin-Nicolae is sentenced to prison after a photography/video expert, Alexandra Văsc, from the Romanian Intelligence Service (*Serviciul Român de Informaţii* in Romanian language) submitted a facial comparison between ATM video footage and suspect photos made of Alin-Nicolae. The comparison between the images was sub-par at best, having not been lined up correctly, placed on the same plane, or compared in a scientific manner. A forensic IT expertise provided no digital evidence against Alin-Nicolae and no scientific evidence to support the hypothesis that he had anything to do with the original crime, but he fell victim to faulty media forensic science, and thus he remained in prison for over seven months until a former Romanian Internal Affairs and Ministry of Justice image expert presented an accurate comparison of the evidence. After the new report was submitted Alin-Nicolae was immediately released from prison.

Case 8: Bucharest, Romania November 11, 2011 [73] [74]. Recent developments in Romania have uncovered a baffling affair in the Eastern European country. In Romania the inquisitorial system of law is used and there are no private or independent forensic experts in Romania, as there are here in the US and many other places around the world, including most of Europe. Because there are no private experts, this means that all forensic examinations are carried out by "state" forensic experts. When a panel of judges requests a forensic examination they turn to the Romanian Ministry of Justice - National Institute of Criminal Expertise (INEC) which oversees the interactions between forensic experts and judges. There have been several outcries that the recently appointed director of INEC, a state prosecutor Catalin Ceort, was placed in his position in debatable circumstances. The same Romanian expert mentioned in cases 4 and 5, Gheorghe Pop, entered the Romanian court in early November 2011 and claimed that he was required to use un-validated methods in his forensic analysis because of a "protocol" between the National Anticorruption Department (Departamentul National Anticoruptie in Romanian language) and INEC, where Pop is employed as an examiner. On November 11, 2011 Ceort released a statement that there is no such protocol between the two agencies. The

entire affair around these kinds of state expertise without any scientific background, non-credible experts, contradictory statements in the Court under oath, and further official statements by the Ministry of Justice, seems to develop like any corruption affair, affecting many branches of the state system including the Romanian public education system. Politehnica University of Bucharest created a Master's of science program in Media Forensics in Romania, launched in the fall of 2011, with faculty members that have no experience in forensic media, they have no published papers in peer-reviewed journals, no scientific research, and no expertise in the field. It is obvious that these kinds of programs look more like a business then a scientific program, and the effects are predictable: a non-credible faculty will generate a non-credible Master's program, and non-credible students, which will further infest the Romanian judicial system claiming that they have a M.S. diploma and that they can be media forensic experts, like any other respectable scientist from abroad that did scientific research, published peer-review articles, and got experience in Court cases. The connections between the Romanian Ministry of Justice, Politehnica University of Bucharest and INEC will generate results that are produced for the highest bidder and not produced for forensic science, completely disrespecting forensic science. Unless Romania opens the doors to outside experts, like the European Union has been requesting since 2006, then real forensic science may never enter a Romanian court room again. For more information about this scandal please see references [73] and [74], the web pages are in Romanian but can be translated with a search engine.

Special attention shall probably be paid by the so called "strategic partners" of Romania who, in turn, support these practices; they speak positively about certain currently empowered politicians and judicial reforms, while the facts don't support their political or diplomatic statements. It is hard to believe that a country that promotes these kinds of practices in forensic expertise and their judicial system can be a strong, credible, and respectable partner in an international coalition. Any vulnerabilities or weakness of one of the members can irreversibly affect the credibility of the entire alliance.

There are standards throughout all forensic disciplines to help keep judicial errors from occurring, these standards are not always respected however, through neglect, bias, or ignorance. Evidence is required to have a chain of custody that clearly details who had possession of the evidence and when they had it for example. Another example is that evidence should never be changed, like writing files to an evidence hard drive. The forensic examiner has no control over the circumstances in which the evidence was created, nor does the examiner

have any control over the chain of custody up until the evidence is delivered for examination. The forensic examiner does however have control over the way the evidence is analyzed; this is where using scientific methodologies is crucial. The examiner has control over how the analysis is conducted and interpreted; this is where bias can be introduced into the examination and the examiner should strive to mitigate bias. The examiner has control over the way the opinion is reported; this is where the examiner can become an advocate for the counsel instead of an advocate for the science, an examiner should never advocate for the counsel. Professional associations and societies have rules set forth to manage behavior such as ethics violations and biased opinions among the members. Disregarding such rules can end an expert's scientific career.

Throughout the history of forensic science there have been disciplines that still flourish today and others have not stood the test of time. Phrenology for instance, was the pseudoscience of determining particularities about a person's intelligence, demeanor, and personality by making measurements of the skull. For nearly 100 years phrenology stood up to scientific standards and there was even a phrenology society based out of Edinburgh, Scotland. By the mid 1800's the American Phrenological Journal was being published in New York [53]. Eventually the "science" of phrenology was debunked and is viewed today as a source for judicial error and substantially groundless assumptions without any scientific foundation. There are examples of other forensic fields that get more credit than they deserve; bite mark analysis, ear print analysis, and hand writing analysis are a few examples of forensic disciplines that have not had any great advances since the time of their creation and require a very minimal amount of training to become a court accepted expert. Even though they require a minimal amount of training these forensic sciences still play an important role in the courtroom today. Across the nation evidence is entered into the court every day that requires the attention of a forensic expert including bite-mark, ear print, or handwriting evidence and everyday new crimes are committed that require the attention of new techniques and strict methods which is even more reason to uphold the NAS report. As Edmond Locard stated, "Every contact leaves a trace" [54]. However, in the dawn of the digital age, technology allows criminals to commit crimes that require no contact and commit crimes that leave no trace.

## 1.2 Introduction to Media Forensics

In order for a fingerprint expert to conduct their analysis a finger must make contact with an object; for a handwriting expert, a pen must make contact with paper; for a ballistics expert, a bullet must make contact with the rifling of a

barrel; for a DNA expert, biological traces must be left at the crime scene. In media forensics on the other hand, there is no direct contact between the speaker and the microphone; there is no contact between the camera and the object being photographed; there is no contact between the files being downloaded and the computer user; there is no contact between a text message and the person who sent them. In media forensics there is the absence of contacts and traces because advances in technology have created a technical barrier between the perpetrator and the crime scene; simultaneously creating the need for advances in the way forensics is applied to such digital crime scenes. There are several aspects to media forensics, the main concept being that media forensics is applying digital science and a system of digital knowledge to answer legal questions concerning digital evidence. Digital knowledge is comprised of the science of digital audio recordings, digital image recordings or stills, digital files from computers, cell phones, GPS systems, and the list can be extended. After thousands of years of forensics having the advantage over criminals through scientific methods, forensics is now faced with the challenge of catching up with the advances in technology that criminals have taken advantage of. Just as murderers could use arsenic on their victims undetected until the chemist, James Marsh, developed the Marsh exam - modern criminals will continue to use technology in ways that defy the examiner until the scientific truth is exposed through advances in scientific forensic media research. One recent development in media forensics helps to authenticate audio recordings. The demand to authenticate audio recordings was pushed to new limits during the 1970's when perpetrators took advantage of the lack of knowledge surrounding what constitutes an original and continuous recording.

On June 20, 1972 in the Executive Office Building of the President of the United States, an audio recording was created on analog tape using hidden microphones [55]. This tape, among others, became the center of one of the largest scandals in American history, leading the nation to question the ethics and integrity of the government as a whole; as well as leading to the resignation of President Richard M. Nixon. This moment in history is referred to as the "Watergate Scandal" and has been the source of many books, movies, and pop culture parodies. Media forensics did not exist in 1972 but through the work of six audio experts, brought together during the Watergate investigation to identify the source of an 18-minute gap on the tape from June 20, 1972, the foundation for audio authentication was created.

Today, the standards of audio authentication closely resemble the methodologies, techniques, and analyses used by the Watergate audio

authentication panel to determine the authenticity of the tape. The six person panel consisted of four PhD's from MIT and two MS Electrical Engineers, all the members had backgrounds in electrical engineering and had contributed significant research in the fields of acoustics, psycho-acoustics, under-water acoustics, digital signal processing, speech analysis, tape recorder development and manufacturing, and more. Whether those six panelists knew it or not they followed the same principles that other forensic sciences had been following for centuries; do not change the evidence in anyway, reduce bias in the analysis and conclusions, and cross verify the findings. Looking back from today's perspective with the strict guidelines on examining audio evidence, the panel respected all of the standards that would be expected of them today, even though those standards did not exist in 1972.

The methodologies that the panel used are still widely accepted and used to this day; there have been several advances in the field of audio authenticity since 1972 but given what they had to work with, they utilized very strong methods and techniques in their analysis. The panel developed a logical approach to determine the authenticity of the Watergate tape; they followed a seven step method that consisted of critical listening, magnetic marks, waveforms, spectra of speech and buzz, phase continuity and speed Constance, flutter spectra, and other tests and measurements including searching for splices, measuring azimuth alignment, and measuring for bias signals. They also investigated the claimed original recording equipment and made test recordings. Today, when analog tape analysis is needed, these procedures are still used as a guideline; there have been advances in analog tape analysis since 1972 such as magneto-optical tape development which makes the magnetic markings on the tape visible. Critical listening, waveform, spectrum, and phase continuity analyses still uphold to modern challenges when dealing with digital audio. Since the early 1970's there have been advances in audio authentication methods because the audio technology has morphed from analog to digital. Even though this thesis focuses on the latest method in digital audio authentication, a brief description will be provided to catch the reader up to speed on what audio authentication methods look like today in a digital world and why the distinction between "sound" and "audio" is important as a closer look is taken into media forensics.

Sound and audio surround people at almost every moment of every day, from traffic noise to background sounds and cell phone conversations to MP3 music and entertainment. This also means that sound and audio are fast becoming key elements in many crimes and consequently key elements in many civil and criminal cases. All evidence brought into the courtroom is subject to scrutiny

from the opposing side and seemingly simple definitions can be twisted to convince a jury that solid evidence is null. For this reason, it is necessary to distinguish the difference between audio and sound. Sound is the human perception of an acoustic wave as it propagates through a medium such as air, water, or steel. Pressure waves generated from a sound source such as a loud-speaker, propagate through these mediums and excite the neighboring particles until the pressure wave hits the human ear. Once in the ear canal the signal hits the ear drum which moves three small bones on the backside of the eardrum called the hammer, anvil and stirrup known collectively as ossicles [56]. The ossicles transfer sound pressure from the outer ear to the inner ear like a system of levers which activate the fluid filled cochlea. The cochlea is full of tiny hair-like follicles that are connected to nerves and this mechanical motion is transduced into a signal which the brain interprets as sound.

Audio on the other hand, is an electrical signal which travels through wires and circuits such as a signal being sent through a digital recorder, for example, once the audio-electrical signal reaches the loud-speaker on a cell phone it is then transduced from an audio signal into an acoustic signal which the brain interprets as sound. There is also scientific reasoning for this distinction between audio and sound. With audio and sound the wavelengths are calculated using the same formula where wavelength is equal to the speed of the signal divided by the frequency ($\lambda = c/f$ ) [57]. The difference is that sound signals traveling through a medium have a much lower speed than audio signals traveling through circuits. The speed of a sound signal propagating through air is roughly 1,130 feet per second at sea level and 70 degrees Fahrenheit, where an audio signal travels roughly at the speed of light or 982,080,000 feet per second in a vacuum. Clearly the wavelengths for sound and audio are going to have different measurements. Sound is transduced into audio in several ways, be it by talking into a cell phone, recording an instrument, or capturing a conversation with a recorder, but the principle is always the same: Sound propagates through a medium until it reaches a microphone, then the acoustic pressure waves are transduced into an electrical value and then sent to a microphone preamplifier to boost the signal level and then to an analog to digital (A/D) converter (see section 3.3) and finally to a digital signal processing unit or other storage media.

In forensics, when dealing with questioned recordings “audio” is the term used. A forensic examiner cannot make precise calculations or explain error rates based on what they hear, due to the fact that human perception of sound is subjective. Precise measurements and calculations can only be made on audio which has finite values which will be the same no matter who is conducting the

examination (unless it's analog audio stored on a magnetic media, which will naturally deteriorate to some degree every time the media is played back). Many times the authenticity of a questioned audio recording will be brought up during trial and there are several tools available to the forensic examiner to verify whether a recording is authentic.

Recent advances in recording technology have created a simple and sometimes undetectable process for the alteration of digital audio recordings. Forensic examiners have several tools at their disposal for authenticating digital audio recordings such as physical inspection, metadata analysis, critical listening, high-resolution waveform analysis, narrow-band spectrum analysis, spectrographic analysis, phase continuity, statistical analysis, and digital data analysis [18]. Because of the rapid developments in recording technology a complete list of authentication tools will not be covered in this thesis, the most common and widely accepted digital audio authentication tools will be discussed here. Each forensic case is unique and new audio formats will require new techniques. One recent and emerging technique has proven to be a powerful authentication tool in Europe and will continue to foster new growth and scientific research in the US. Before discussing this new technique, a brief summary of the authentication tools listed above will be presented.

According to the Audio Engineering Society an authentic audio recording is one "*made simultaneously with the acoustic events it purports to have recorded, in a manner fully and completely consistent with the methods of recording claimed by the party who produced the recording, and free from unexplained artifacts, alterations, additions, deletions, or edits*" [58]. The Scientific Working Group on Digital Evidence (SWGDE) defines an authentic audio recording as "*the first manifestation of sound in a recoverable stored format be it magnetic tape, digital device, voicemail file stored on a server, optical disk, or some other form*" [59]. Over the years there have been several techniques for authenticating audio recordings that have developed into a widely accepted protocol and are briefly described below.

Physical inspection is an examination of the evidence to determine if there are physical indications of alterations or tampering to the evidence. Some physical indications of tampering could be found in the form of tape splices for example.

Metadata analysis is the examination of the information that the computer reads in binary, hexadecimal, or ASCII form. The examiner can utilize

specialized software to view this information and extract valuable information such as creation date/time, recorder make/model/serial number, length of the recording, and signs of audio editing software used on the recording among other facts.

Critical listening is the aural examination of the evidence recording using high quality headphones on a professional playback system. Critical listening can expose areas in the recording that should be examined more closely. Some common events to listen for are pops, clicks, and sudden changes in background noise, interrupted speech, and discontinuities in foreground noise. Critical listening cannot substitute statistical observations but can pin-point areas that should be examined more closely.

High-resolution waveform analysis is a visual examination of the relationship between the time and amplitude characteristics of the recording on a graphical display where time is on the X axis and amplitude is on the Y axis. Most any audio editing software can display waveforms allowing the user to zoom in on areas of interest, even to the sample level. This analysis can reveal suspect areas where the values between two consecutive samples show a drastic change.

Narrow-band spectrum analysis is also a visual examination where the frequency content is represented on the X axis and the amplitude content is represented on the Y axis. By dissecting the audio into small windows and calculating the average for each window this analysis can reveal what the amplitude is for each frequency band in the evidence recording. This is useful for quickly determining factors such as the amplitude of a 60 Hz signal, digital aliasing, and sample frequency bandwidth among other factors. By decreasing the size of the FFT window from 512 to 4096, for example, the examiner can increase frequency resolution while decreasing time resolution. Conversely, increasing the size of the FFT window can increase time resolution while decreasing frequency resolution.

Spectrographic analysis is another visual examination where the audio signal is represented on a graph displaying time on the X axis and frequency on the Y axis, areas of high amplitude are usually light in color and areas of low amplitude are usually dark in color. This type of analysis can quickly reveal constant tones, speech formants, and certain types of edits that interfere with a broadband of frequencies among other information.

Phase continuity is the comparison between discrete tones captured in the evidence recording with reference tones generated from software. This type of analysis works better with discrete tones that span the length of the recording, have a substantial signal to noise ratio, and fall within the high frequency bandwidth.

Direct Current bias or DC bias can be caused by poor quality analog components, a problem with the A/D conversion process, or other sources. DC bias can be detected if the averaged values of a time vs. voltage waveform equal something other than zero. Sometimes DC bias can be used to help determine if an evidence recording is consistent with the recording device claimed to have created it.

Frequency bias can be caused by a recording device clock functioning improperly. When a recording device clock is sampling the signal too fast or too slow then frequencies will be shifted lower or higher. Frequency bias can be detected if the nominal frequency is subtracted from the time vs. frequency waveform and the result is something other than zero. Frequency bias can also be helpful in determining particularities of a certain recording device.

Statistical analysis involves extracting information about the numeric relationships in the recording's digital structure. This type of analysis can reveal useful information about the consistency of repeated bytes and can also be used to compare test recordings to the evidence recording.

Digital data analysis is a technique used to find information about the bits and bytes in the metadata of the recording. Digital data analysis is a lot like the statistical analysis but digital data analysis is carried out on an image file of the recording and not the actual recording file itself.

Because digital technology evolves so rapidly, and different techniques used in authentication also develop rapidly, the techniques listed above should suffice in giving the reader a general overview of the most common methods and help to explain what forensic examiners are looking for when conducting an analysis. To learn more about digital audio authentication the Bruce Koenig and Doug Lacey AES paper [18] offers an in depth exploration of the techniques listed above and more.

Another important note on audio authentication is that the claimed original recording device should be submitted with the evidence recording. If the

forensic examiner has the claimed original recording device there are several more techniques that can be used to establish authenticity. An example for analog recordings is that recording events such as stop, start, pause, and record over leave unique frequency signatures on analog tape. The physical distance between these unique signatures can be compared with the physical distance between the record, play back, and erase heads in the claimed tape recorder. Digital audio devices can be examined to ensure that the format of the evidence recording is consistent with the normal operations of the recording device. In both analog and digital authentication the claimed original recording devices should be examined and test media should be produced from them to produce as much information as it is possible about the authenticity of the evidence. With digital media it is possible for a forensic examiner to determine that the evidence is not authentic. But for a forensic examiner to find that the evidence is completely authentic is an impossibility; due to the limitations in digital media that face the forensic examiner the closest opinion that the examiner can reach to completely authentic is that the evidence is consistent with an authentic recording.

### 1.3 Introduction to Electric Network Frequency

The latest development in digital audio authentication comes from Dr. Catalin Grigoras, National Center for Media Forensics (NCMF), University of Colorado Denver. Grigoras discovered that small variations occurred over time in the frequency of electrical power. These small variations led to a huge discovery that eventually developed into what is known today as the Electric Network Frequency (ENF) Criterion. ENF analysis consists of extracting the power line hum from a digital audio recording and comparing it to a database to determine date and time of creation, areas of potential additions or deletions of audio, and the geo-location where the evidence was created.

To understand ENF one must understand two basic concepts: First, Alternating Current (AC); second, digital audio recorders. These two concepts combined make possible the authentication of digital audio by comparing the power-line hum embedded in the recording to a database of grid activity at that point in time. In a basic overview, AC electricity is produced and consumed continuously on a power grid. The differences in production and consumption create small variations in the frequency of the grid. These small variations are nearly the same at any two points on the grid at any given moment, fluctuating constantly but in unison. When a digital audio recorder is powered by the grid (plugged into an outlet) or in the proximity of an electromagnetic field (power lines, refrigerator, ect.) the recorder not only records the intended speech, music,

or other sound of interest but the recorder may also record the small variations coming from the grid frequency.

Later, when the recording becomes evidence and is given to a media forensic expert for examination, the expert can extract the recorded variations of the power-line signal from the recording and compare this signal to a reference database that will indicate exact date, time, geo-location, potential additions, potential deletions, and mixed material in the recording. To further elaborate the concept and origins of ENF, the two fundamental concepts of AC electricity and digital recorders will be presented below.

### 1.3.1 AC Electricity

AC electricity can be produced in a variety of ways, the most popular methods being hydroelectric, nuclear reactors, and coal power. Hydroelectric methods typically use a water wheel and the gravitational force of falling water to get a turbine spinning. Coal and nuclear energy produces steam and use steam-pressure to get a turbine spinning. Whatever method is used to get the turbines spinning the concept is the same after that point. AC electricity is produced by a spinning turbine connected to a generator that rotates at 60 cycles per second in the US and at 50 cycles per second on the UCTE grid. The speed of the rotation of the generators creates the transmission frequency that the voltage is transmitted from the power plants to the end user. The electricity from the power plants goes to a transmission substation where a transformer boosts the voltage to hundreds of thousands of volts in order to prepare it for its long journey to the end user. High voltages such as 500,000 volts help reduce line-loss while the power is being transmitted. Due to differences in produced and consumed electricity, the generators may rotate at slightly different speeds than exactly 60 cycles per second. There are strict thresholds that maintain rotation speeds within roughly 0.2 Hz on the US Eastern grid for example. Because the generators rotate in tandem with each other, the rotations per second are generally nearly identical throughout a given grid. A generator rotating as much as 2 Hz out of sync with the others can quickly generate enough heat to destroy itself.

When the power comes off the transmission grid it goes to a power substation where it is stepped down from the high transmission voltages to something on the order of 10,000 volts. At this point the power can be distributed in different branches to the end user. Electricity generated from power plants in the continental United States provide electricity to the Western Grid, Eastern Grid, and the Texas Grid [22], [60], [65]. The Eastern and Western grids also

extend north into Canada [12] but Quebec is on an independent grid. This electricity is transmitted from the power substations to the end user in the form of alternating current at sixty cycles per second 60 Hz US (50 Hz UCTE) just as it was at the power plant. Differences in the amount of electricity being produced and the amount of electricity being consumed cause the frequency of the grid to vary over time. This balance leaves a distinct signal that is always fluctuating, always random, highly non-predictable, and has a high-probability of never repeating roughly between 59.5 Hz and 60.5 Hz on the US grids and roughly between 49.5 Hz and 50.5 Hz on European and United Kingdom grids [22]. These small variations between established thresholds can be captured with an ENF probe plugged into a mains power source such as a wall socket. The ENF probe's output is a line-level signal that can be plugged into a computer soundcard or other audio interface and recorded. Simultaneous ENF recordings from the same grid will be nearly identical because each grid carries a consistent phase across the grid's entire span. For the United States, this was tested and confirmed by Professor Rich Sanders [12] at the National Center for Media Forensics (NCMF) as well as the physical extension of the Eastern and Western grids into Canada.

Theoretically, only four ENF databases are needed to establish 24-hour a day monitoring of ENF activity throughout the continental United States and Canada. The geographic regions that are covered by the Western grid ENF database include everything generally west of the Rocky Mountains extending from the southern borders of the United States and north through Canada. The geographic areas covered by the Eastern grid ENF database include everything generally east of the Rocky Mountains extending from the southern borders of the United States and north through Canada, minus Texas and Quebec. The geographic area of Texas has a separate electrical grid and will require its own ENF database. The geographic area of Quebec also has a separate electrical grid and will require its own ENF database. Four ENF collection sites established in strategic locations can provide useful information about digital audio recordings made within a region of roughly 7.6 million square miles. Likewise, any digital recording device that is introducing ENF into the recorded digital audio will have the nearly the same ENF trace as the rest of the electrical grid it was created on at that moment in time, which is a unique trace in time due to the differences in production and consumption. For this reason digitally recorded audio can be compared to an ENF database to establish a date/time stamp, geo-location, potential edits, deletions, additions, and mixed material. Figure 1 displays the three electric grids of the continental United States. See Appendix C for more details.

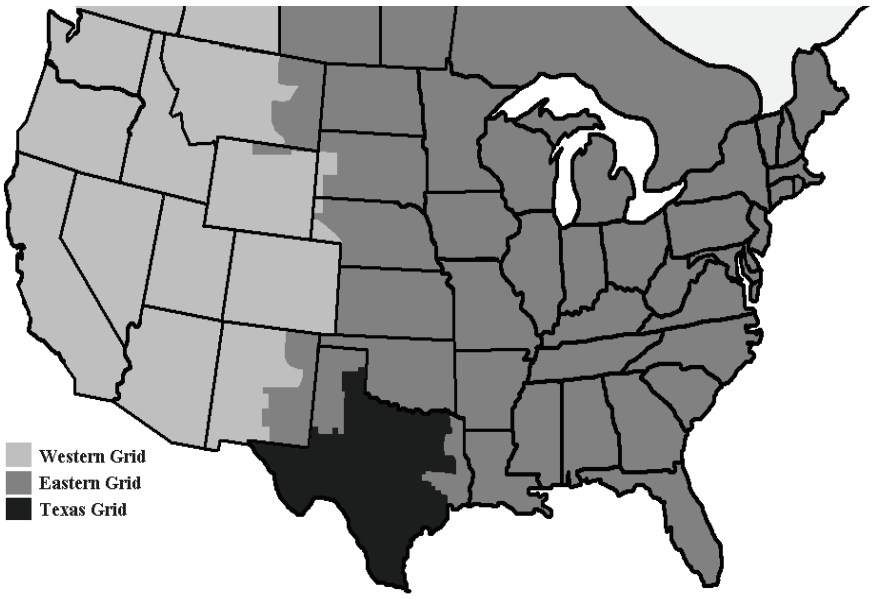


**Figure 1** United States Electrical Grids

### 1.3.2 Digital Recorders

Digital audio recorders are devices that turn continuous waveforms into a discrete stream of 1s and 0s. There are several types of digital recorders available on the market from rack-mount recorders to hand-held units. Even video cameras with the ability to record audio fall into this category. The idea is the same in almost every type of digital recorder. A pressure wave propagating through a medium is picked up by the microphone and then amplified; or a line-level signal is received, then either the microphone signal or the line-level signal is transmitted to the low-pass anti-aliasing filter to meet the requirements of the Nyquist Frequency, then passed on to the sampler or analog to digital A/D converter, which samples the analog signal at *fs* (Sampling Frequency) values per second and assigns a binary word to represent amplitude (bit depth). This process results in a digital representation of the original sound or signal with *fs* values for the time axis and "X" bit values for the amplitude axis.

This data stream is then saved to a storage format such as a Hard Disk Drive (HDD), Solid State Drive (SSD), or flash memory. This data stream can be reproduced any number of times and is more resilient to degradation than analog media. Because of this ability to reproduce binary words any number of times, making the distinction between original, first, or second generation copies

becomes nearly impossible. HASH values can even be calculated to verify that the copied material is an exact representation of the original and at that point there is almost no way to distinguish the two. Digital audio can also be edited in ways that analog audio could never be edited, defying the forensic examination.

The microphones used for picking up sound can also pick up electromagnetic variations through the air and embed this information into the recorded audio; this is because the microphones, leads, and recorder circuitry can act like capacitors and inductors picking up the presence of electromagnetic fields, similar to how certain metal objects can act as antennas when connected to a power source. Even if a digital recorder is powered by batteries alone and not mains power, ENF traces can sometimes still be extracted simply because the recorder was in the presence of electromagnetic fields coming from a variety of sources such as refrigerators, computers, or power lines. Whether the recording device is powered by the mains or powered by batteries, if ENF is embedded into the recording then a comparison can usually be made against an ENF database.

When building an ENF database for forensic purposes, ensuring that the recorded signal satisfies standards for forensic analysis is crucial. The ENF signal shall be free of clipping, lossy compression, and distortions, the signal to noise ratio (SNR) shall be as high as possible, and the acquisition system clock shall be synchronized with an atomic-radio clock or grid independent time controller. Using an ENF database to compare reference and questioned ENF involves precise measurements of amplitude, spectrum, and zero-crossings in order to accurately time-stamp, discover potential edits, and authenticate digital audio/video recordings. There are several precautions that should be respected in order to maintain the integrity of a forensic ENF database. In this thesis suggestions will be made regarding fifteen aspects of the database configuration that should be viewed as helpful guides in order to build and maintain a robust, secure, reproducible, reliable, and accurate forensic ENF database that will satisfy forensic standards and best practices.

## 2. Review of the Literature

This chapter reviews the available scientific papers that have contributed to the ENF criterion. These papers have been published from across the globe and collectively offer a broad range of perspective on the ENF criterion. Each paper is given a short summery and then a discussion about the coinciding theories and conflicting theories is presented. Next, explanations about further directions that are potentially available for the ENF criterion are discussed. Then this chapter concludes with an overview of existing ENF databases.

### 2.1 Summaries of Scientific Literature

**[1] Digital Audio Recording Analysis: The Electric Network Frequency (ENF) Criterion**
by Catalin Grigoras

This article was published by the journal of Speech, Language, and the Law in 2005 and introduced the Electric Network Frequency criterion to the forensic community as a valuable tool for the authentication of forensic digital audio recordings. Written by Dr. Catalin Grigoras during his tenure at the National Institute of Forensic Expertise in Bucharest, Romania, this article outlines his research and begins with an introduction to the process of authenticating digital audio. Grigoras then explains the fundamentals of the ENF criterion on the European 50 Hz grid and stresses the importance of compiling a database to be used in comparing evidence recordings against a reference. Graphs displaying his analysis of the ENF help guide the reader through his findings. Grigoras initiated three experiments to verify his theory by monitoring the variations around 50 Hz in different locations in his office building, elsewhere in the city of Bucharest, and three different geographic locations across the European grid. The results show that for all consumers, at any moment in time, the ENF values are the same. This discovery laid the groundwork for an entirely new tool for authenticating forensic digital audio.

Grigoras explains in a real case example how the ENF criterion was used to determine where deletions had been made in a disputed digital audio recording between two speakers. By comparing the evidence recording to the reference database, Grigoras was able to verify the claims made by speaker A that several deletions had been made, as well as, determine the length of time that had been obfuscated by each deletion, and conclude the exact date, hour, minute, and second that the recording had been produced. Grigoras explains the

spectrographic method he used to extract the ENF from the evidence recording and he shows the 2D-spectrograms used to visually identify alterations in the recording. Explanations of the software used in this case are presented with the settings of the down-sampling, band-pass filtering, and FFT size functions used to extract the ENF.

In the following section, Grigoras presents another method of ENF extraction, known as the Zero-Crossings Method (ZCR). This method is a time-domain analysis of the ENF as opposed to the frequency-domain analysis used in the Spectrographic and Long Term Average Spectrum (LTAS) methods. By analyzing the ENF in the time-domain Grigoras was able to compute the zero-crossings of the signal and measure the time differences of consecutive zero-crossings then he used these values to plot the signals traces on a graph with enough resolution to see the micro variations in the ENF. The ZCR method can reveal enough detail about the ENF to see differences in quantification levels if there are audio segments coming from different recording equipment and spliced together.

In his article, Grigoras explains his database configuration that has been continuously monitoring ENF activity on the European 50 Hz grid since May 2000. He also explains the storage requirements for such a configuration, followed by a flow chart for automatically detecting the date and time of a questioned recording. The limitation of extracting ENF from analog recordings is briefly outlined to stress that the ENF criterion is designed for digital audio recordings where the original ENF signal must not be distorted during extraction. This is a very well written paper and it lays the foundation for using the Electric Network Frequency as a tool in forensic authentication of digital audio.

**[2] Application of the Electric Network Frequency (ENF) Criterion a Case of a Digital recording**
by Mateusz Kajstura, Agata Trawinska, Jacek Hebenstreit

This article was published through the Forensic Science International 155 (2005). The authors conducted their contributing research for this article at the Institute of Forensic Research in Cracow, Poland. The aim of this article was to verify the ENF criterion and the reliability of the extraction methods. The authors employed a series of tests involving different types of recorders located in different areas around Poland recording simultaneously. Later the recordings were processed and compared to verify that equipment in different places of the same grid will capture the same grid fluctuations at that moment in time. The

authors also acquired some information from the power company, which samples the ENF once every second, and made a comparison of the power company's values against the values that the authors were seeing in their tests. This confirmed that the ENF criterion could be used to establish the authenticity of a digital audio recording in Poland. The authors also tested and verified the ability to detect edits, particularly deletions, using the ENF criterion.

A real case example is given in this article where the authors were asked to authenticate a 55 minute recording between two business men. The date claimed by the business men was different then the date in the metadata of the recorder by about 196 days. Using the ENF criterion, the authors were able to verify that the recording was consistent with the ENF fluctuations on the date that witnesses of the conversation claimed. It was later determined that the person operating the recorder neglected to appropriately set the time and date of the recording device. The authors conclude that the ENF criterion is a valid forensic tool for authenticating questioned digital audio recordings in Poland. Poland, like most European countries, is part of the Union for the Coordination of Transmission of Energy (UCTE).

**[3] Dating of Digital Audio Recordings by Matching of Electrical Network Frequency Patterns**
by Francisco Javier Simon del Monte, Jos Bouten, Catalin Grigoras, Joaquin Gonzalez-Rodriguez

This is a technical presentation from 2006 given to the European Academy of Forensic Sciences in Helsinki, Finland. This presentation explains the complex mathematics behind the long term average spectrum, zero-crossing extraction methods and automatic pattern matching methods employed to search databases automatically. There are several helpful charts and equations in this presentation.

**[4] Applications of ENF criterion in Forensic Audio, Video, Computer and Telecommunication Analysis**
by Catalin Grigoras

This article was published by the Forensic Science International in June 2006. This article investigates the application of the ENF criterion to determine the integrity of forensic audio/video, computer, and telecommunication systems. The article starts with an in depth explanation of the ENF criterion and the extraction methods. An early version of a forensic ENF database is presented

here as well as an outline of several experiments carried out by the author to establish the validity of the ENF criterion over the European electrical network. Three case work examples are discussed involving: 1) a digital audio recording between two speakers of a three hour length, 2) a video with audio, and 3) a video with audio that was broadcast on television. In all three cases the author successfully employed the ENF criterion to determine the authenticity of the audio/video recordings establishing dates, times, and mixed material. Using the ENF criterion it was the author's opinion in case three that three ENF signals could be found. ENF1 coming from the video camera, ENF2 coming from the broadcasting company, and ENF3 coming from the questioned tape containing the video transmitted recording. This article further solidifies the validity of the ENF criterion and expands the applications of the criterion to video with audio, computer, and telecommunications.

**[5] An Investigation into the Electrical Network Frequency (ENF) Technique for Forensic authentication of Audio Files**
by Nisha Morjaria

This is the thesis work of Nisha Morjaria and constitutes an investigation into the applicability of the ENF criterion on analog tapes. The author explains the experiments that were undertaken to arrive at the conclusions. The author verified that simultaneous recordings in three areas around the United Kingdom captured the same ENF variations at that moment in time. The experiments show that visual correlations could be seen between the three recordings that were made to analog tape at three separate geographic locations in the United Kingdom. Conducting more complex examinations such as zero-crossing and automated database search are highly unlikely to occur with analog evidence due to the inherent wow and flutter from the mechanical motions inside the tape machines. This article is the first step in verifying that the ENF criterion can be employed on the United Kingdom electric grid.

**[6] Further Investigation into the ENF Criterion for Forensic Authentication**
by Eddy B. Brixen

This article was presented at the 123rd Audio Engineering Society (AES) conference in 2007. The author investigates ways to establish reference data, spectral contents of the electromagnetic fields, the effect that low bit rate codecs have on low frequency hum, and tracing ENF harmonic components. This article suggests that multiple databases should be connected to the same grid to help protect from losing data in the event of localized power outages. The author

approaches the above investigations in a statistical manner and provides several helpful graphs to help elaborate the point. The author also stresses the point that there are standards and best practices for authenticating analog audio but that there needs to be the same protocols for digital audio. This article further verifies that the ENF criterion can be extended to apply to Denmark, which shares the same UCTE grid as Romania.

**[7] Techniques for the Authentication of Digital Audio recordings**
by Eddy B. Brixen

This article was presented at the 122nd AES convention in 2007. This article further explains the need for a solid methodology that can span international boarders when authenticating digital audio. This article starts with a brief introduction to challenges facing experts when they present digital audio analysis into court and then explains several other digital audio authentication tools. The author also discusses digital recorders and explains how the microphones can pick up ENF signatures from being in the proximity of electromagnetic fields with no physical connection to the grid. In closing the author mentions ways to detect edits and ways in which the ENF criterion can be cheated.

**[8] Applications of ENF Analysis Method in Forensic Authentication of Digital Audio and Video Recordings**
by Catalin Grigoras

This article was presented at the 123rd AES conference in 2007. This article reports on different ENF types, phenomenon that determine ENF variations, analysis methods, stability over geographic areas in Europe, internal laboratory validation, uncertainty measurements, real case examples, effects of different compression algorithms, and potential problems that the forensic examiner can encounter when employing the ENF criterion. The author also discusses quality control measures for establishing a forensic ENF database.

**[9] Frequency Disturbance Recorder Design and Developments**
by Lei Wang, Jon Burgett, Jian Zuo, Chun Chun Xu, Bruce J. Billian, Richard W. Conners, Yilu Liu

This article was published in 2007 by the Institute of Electrical and Electronics Engineers (IEEE). This article discusses the complex network that monitors electric grid disturbances across the continental United States and parts

of Canada called the Frequency Monitoring Network (FNET). FNET is comprised of several Frequency Disturbance Recorders (FDR) strategically placed around the United States and Canada. These recorders generate statistical data that is used to monitor and control the frequency variation on the electrical grid interconnects. Virginia Tech has been involved with this project for several years and has been instrumental in establishing this network. FNET is a database of ENF variations; FNET is not a high resolution database of ENF variations however. FNET can supply statistical data that is averaged in 1 minute windows or 10 minute windows, this information can be useful for monitoring overall network performance but for a forensic application of the ENF signal a high resolution database is necessary to be able to detect the differences down to the second and to employ automated searches. The techniques and methods in this article imply that the ENF criterion should be as valid in the United States as it is in Europe.

**[10] ENF; Quantification of the Magnetic Field**
by Eddy B. Brixen

This article was published by AES at the 33rd International Conference in 2008. This article takes a statistical approach to quantifying the magnetic field and the effects it can have on recording equipment. The author conducted several experiments to quantify this phenomenon including the use of calibrated magnetic field strength detector, a device made to generate magnetic fields, and several types of digital recorders. This article has several helpful charts and graphs that help give a visual aid to explain the experiments and the results.

**[11] The Electric Network Frequency (ENF) as an Aid to authenticating forensic digital audio recordings – an Automated Approach**
by Alan J. Cooper

This article was published in 2008 at the AES 33rd International Conference. The author employs a statistical approach to establishing an ENF database of nominal values instead of audio recordings. The advantage to this type of database configuration is that storage requirements are small, automated database searches are made easy, and the database is a relatively simple but powerful and an accurate means to acquire ENF. The author employs a Short Time Fourier Transform that calculates the peak magnitude in short windows, then the windows are overlapped and calculated again and again for the length of the recording. This results in a very accurate representation of the ENF signal

suitable for automatic processes. This article establishes the validity of employing the ENF criterion on the United Kingdom electrical grid.

**[12] Digital Audio Authenticity Using the Electric Network Frequency**
by Richard W. Sanders

This article was written by the founder of the National Center for Media Forensics in 2008, published at the AES 33rd international conference. This article explains the first nationwide ENF experiment in the United States. The results explained in this article solidified the ENF criterion validity and potential for application in the United States. The author also proposes a schematic for an ENF probe based on a 3-resistor voltage divisor. The experiment involved synchronized recordings of ENF fluctuations in different locations on the Western Grid, synchronized recordings of ENF fluctuations in different locations on the Eastern Grid including the physical extension of this grid into parts of Canada, and synchronized recordings of ENF fluctuations in different locations on the Texas Grid. The results verify that the ENF criterion has potential for use on the United States interconnects and the article contains several helpful charts and graphs to help illustrate this point.

**[13] An Automated Approach to the Electric Network Frequency (ENF) Criterion: Theory and Practice**
by Alan J. Cooper

This article was published by the International Journal of Speech Language and the Law in 2009. In this article the author expands on his previous paper and further explains the automated approach used to configure the ENF database at the Metropolitan Police Forensic Laboratory in the United Kingdom. The author explains how the ENF time-domain signal is split into overlapping frames and how each frame has the peak value calculated and how this is averaged over time to create the ENF signature. This is a very logical and robust approach to establishing an ENF database.

**[14] Forensic Speech and Audio Analysis Working Group (FSAAWG) Best Practice Guidelines for ENF Analysis in Forensic Authentication of Digital Evidence**
by Catalin Grigoras, Alan J. Cooper, Marcin Micha£ek

This is a forensic best practice guideline that was published by FSAAWG in 2009. This best practice guideline walks through the step-by-step procedures

for extracting ENF and gives some suggestions as to how the forensic ENF database should be configured.

**[15] Using the ENF Criterion for Determining the Time of Recording of Short Digital Audio Recordings**
by Maarten Huijbregtse, Zeno Geradts

This is a paper written by a student at the Netherlands Forensic Institute. This paper explains that using maximum correlation coefficient is a more robust method to match ENF patterns because frequency offsets will affect the Mean Square Error and zero-crossing methods. In addition, the author proposes that the correlation coefficient (CC) is a more robust approach over Mean Quadratic Difference (MQD). In essence the author empirically shows how CC is more accurate when applying automatic search algorithms to digital audio evidence that has word-clock errors from the recorders sampling clock.

**[16] Applications of ENF Analysis in Forensic Authentication of Digital Audio and Video Recordings**
by Catalin Grigoras

This article was published by the AES in September 2009. This article expands on the author's 2007 AES article. This article covers the majority of the content presented in his former article with the addition of a section on ENF influences which covers the phenomenon of digital recorders capturing the ENF trace while in the presence of electro-magnetic fields. The format of the article is basically the same but additional information is presented in almost every section.

**[17] The Application of Power-line Hum in Digital Recording Authenticity Analysis**
by Marcin Micha£ek

This article was published by the Institute of Forensic Research (Krakow, Poland) in 2009. This article explores the algorithms for automated ENF database searches against evidence digital audio recordings. The author also speaks of the tests that were undertaken in writing this article to see the results of an automated discontinuity check. This article is a purely statistical approach to automated searching and follows much of the same logic presented in Cooper's previous articles. There are several graphs and charts that help illustrate the explanations.

**[18] Audio Authenticity: Detecting ENF Discontinuity With High-Precision Phase Analysis**
by Daniel Patricio Nicolalde Rodriguez, Jose Antonio Apolinario, Luiz Wagner Pereira Biscainho

This article was published by IEEE in September 2010 and offers a very interesting approach to the ENF criterion. This article proposes a method for detecting phase discontinuities in an ENF signal which can help reveal areas of edits that have been added or deleted. The main idea is that even without a database, the continuity of the ENF signal can be determined to be either continuous or altered by examining the phase of the captured evidence ENF signal. In the introduction, a brief overview of the ENF method is explained and then that ties into section two which gives the fundamental origins of the ENF signal. Section three covers how complex algorithms can estimate the phase of a sinusoidal signal. Section four covers the method for employing this phase estimation during audio authenticity, including a visual approach and an automatic approach. Section five evaluates these methods using real examples. Section six covers practical issues such as investigating the practicality of this method when applied to a 60 Hz network from Rio de Janeiro, where a slight increase in error rate was encountered. Section seven concludes that the idea of finding abrupt phase changes in the power grid signal is a favorable method for finding edits in audio recordings when the ENF database is unavailable. The main lesson to take from this article is that the authors propose a fourth type of ENF sub-database that samples the ENF at 12 kHz.

**[19] Building a Database of Electric Network Frequency Variations for use in Digital Media Authenticity**
by Jeff M. Smith

This paper was written by Smith, who worked closely with Rich Sanders, while Interim Director of the NCMF, and presented at the 2010 scientific meeting of the American Academy of Forensic Sciences. It explains the ENF database that was originally installed at the NCMF as well as a brief explanation of the ENF database that Grigoras maintains in Romania and the ENF database that Cooper maintains in the United Kingdom. The author explains how there needs to be certain standards in place in order for the ENF criterion to reach its full potential in the United States. The author also briefly explains the FNET system described in the Wang et al IEEE article.

**[20] Advances in ENF database configuration for Forensic Authentication of Digital Media**
by Catalin Grigoras, Jeff M. Smith, Christopher W. Jenkins

This article was published by AES at the 131st convention in 2011. This article explains the advances in forensic ENF database configuration and is an instrumental step in establishing forensic best practices that can transcend international borders. This article gives a brief background on the ENF criterion and then explains the methods used at the National Center for Media Forensics to develop the modern ENF probe. The authors then explain how a secure, redundant, and reliable ENF database should be configured.

**[21] Forensic Authentication of Digital Audio Recordings**
by Bruce Koenig and Douglas Lacey

This article was published by the AES in 2009 and is the closest manuscript there is to a standard methodology in the field of digital audio forensics. This article walks the reader through several digital audio authentication techniques in a methodical manner that can almost be followed like a check list. Not every single method for authenticating digital audio can be covered since the advances in digital audio are developing every day. This article does give a solid foundation to the science of authenticating digital audio.

**[22] Statistical Tools for Multimedia Forensics**
by Catalin Grigoras

This article was published by the AES at the 39$^{th}$ international Conference in 2010. This article extends the list of digital audio authentication tools to include compression level analysis. When a digital recording is edited the user must save the file with the edits, which introduces a second layer of compression. The levels of compression can be detected and used to verify if a recording has undergone multiple generations of compression. There are several graphs to illustrate the point and this article takes a purely statistical approach to analyzing digital audio evidence.

## 2.2 Coinciding Theories about the ENF Criterion

The ENF criterion has been tested in Romania, the United Kingdom, Denmark, the Netherlands, Poland, Denver, Canada, at various other points across Europe as well as all three grids in the United States and has consistently shown three important concepts. First, fluctuations in an electric grid leave unique signatures over time. Second, these fluctuations are the same when measured simultaneously from any two points on the same electric grid. Third, digital audio recording equipment can capture these variations and the recordings can be analyzed to determine date, time, hour, minute, second, potential additions/deletions, mixed material, and broad geographic location.

The methods for extracting ENF are widely accepted [1-23]. The spectrographic analysis is the simplest approach and usually is enough to satisfy the needs of the matter. The spectrographic method is a visual comparison of an evidence recording to the ENF database. Both the database and the evidence are down-sampled to twice the nominal frequency of interest plus 20%, and then both files are band-pass filtered with a width of about 1 Hz around the nominal frequency of interest. Utilizing a high FFT order it is possible to see small variations around the nominal value very closely and determine similarities and differences, areas of missing or added material, or multiple ENF traces.

If more complex analysis is required the next step is the Fast Fourier Transform (FFT) approach which samples the audio in short windows, computes the maximum magnitude frequency in each window based on the power spectrum of that window. Then the windows overlap each other by a determined amount, usually one sample offsets, and then the process is repeated. In this method it is also necessary to down-sample and band-pass filter the signal accordingly. Cooper developed a similar method using Short Time Fourier Transforms (STFT) on the $100^{th}$ harmonic of the ENF signal and zero-padding the time values to alleviate the time versus frequency tradeoffs inherent with FFT. These methods are computational approaches that can produce statistical and robust results.

Another computational approach is the time-domain zero-crossings method. This method calculates consecutive zero-crossings and the length of the semi-period and builds a comparative graph from those values.

## 2.3 Conflicting Theories about the ENF Criterion

From the available literature on the ENF Criterion, one conflicting theory was found. The conflicting theory does not concern the phenomenon that makes ENF work nor does it concern the way that ENF databases are configured, but it is a crucial point that needs to be clarified because if automatic search algorithms are implemented incorrectly during a forensic examination then judicial errors may soon follow. The conflicting theory has to do with the way in which automatic search algorithms are applied to the ENF Criterion. Automatic search algorithms are a powerful tool that can add a statistical quantification, known error rates, and unbiased results to the forensic analysis; these are important attributes for using the ENF Criterion in US courts. In addition, automatic search algorithms save the examiner from the daunting task of visually comparing unknown evidence ENF to reference ENF. Simon del Monte et al. [3], Cooper [11], and Huijbregtse et al [15] presented both Mean Square Difference (MSD) and Correlation Coefficient (CC) algorithms. The goal of both algorithms is to automatically find a date and time in an ENF database that is most consistent with unknown evidence ENF recordings. Even though both algorithms are inherently different mathematically, the appropriate steps for both methods involves pre-processing such as down-sampling, band-pass filtering, and ensuring frequency bias sample rate offsets are accounted for. Once the pre-processing has been correctly and uniformly conducted across all the examination material (evidence and reference) an accurate comparison can be made between different automatic search algorithms.

Huijbregtse et al states that "*It is seen that the ENF criterion failed in correctly estimating the time of recording for 44 out of the 70 recordings*" [15]. Huijbregtse et al demonstrated that using the MSD algorithm on ENF recordings that had been pre-processed inappropriately *without* mean subtraction, caused the automatic search method to return 44 out of 70 wrong results. On the other hand, Huijbregtse et al demonstrated that computing the CC *with* mean subtraction for automatic database search resulted in only 3 out of 70 wrong matches. In essence, Huijbregtse et al compared one method without first subtracting the mean values (correcting frequency bias) with a method that had the mean values subtracted. The reason that this type of mistake can be easily overlooked is that CC naturally resolves any issues pertaining to frequency bias sample rate offsets that are caused by the word clock in the evidence recording device performing poorly. In other words, the CC used in Huijbregtse et al experiment subtracts the mean values as part of the algorithms product, which is how frequency bias

sample rate offsets are corrected. MSD on the other hand, requires an additional step before applying the algorithm to correct frequency bias.

This conflict of opinions is a good example of how the scientific community can learn about the scientific process in question. Cooper explains these differences clearly and makes a convincing case for MSD in his 2011 International Journal of Speech, Language, and the Law article [23]. Cooper explains how the CC works "under the hood" as well as the MSD. Cooper then conducts an experiment on 50 mock-evidence recordings each 22.5 seconds in length (not too short to return all wrong matches and not too long to return all correct matches). What Cooper proves is that MSD returned 13 out of 50 correct matches and CC returned only 4 out of 50 correct matches. The 4 matches identified by the CC were also identified by the MSD. In addition, Cooper calculated the next best 30 matches and found that the MSD had 23 lowest order correct best matches where CC had zero. By using statistical analysis, Cooper demonstrates the superiority of MSD over CC when the pre-processing has been correctly and uniformly conducted across all the examination material. Cooper's findings [23] are fully supported by the NCMF tests conducted during 2010 – 2011, by the students coordinated by Grigoras and Smith, showing that MSD is more robust than CC for automatic ENF matching.

### 2.4 Existing ENF Databases

An advantage of the ENF Criterion is that one database per electric grid is enough to establish most of the network variations for that entire grid. The disadvantage is that a localized power outage can knock the database off-line and cause valuable ENF information to be lost. For this reason, more ENF databases should be configured on each grid in strategic locations. The more forensic ENF databases that are configured appropriately around the globe will increase the possibility to use the ENF Criterion when examining digital media. All of continental Europe shares one electric network called the UCTE grid and this grid is monitored by the ENF database that Grigoras configured. The United Kingdom has an independent grid from continental Europe and the UK grid is monitored by the ENF database that Cooper configured. The continental United States has three grids; the Western grid is monitored by a primary database at the NCMF in Denver, Colorado configured by Grigoras and Jenkins, and a secondary database at the Target Forensic Services Lab (TFSL) in Las Vegas, Nevada configured by Jenkins. The Eastern grid is monitored by the TFSL database in Minneapolis, Minnesota configured by Jenkins and Steinhour. As of the end of 2011 there is not a known database of Texas grid ENF. Digital media from the UK, continental Europe, and the continental US (minus Texas) has the

potential to be compared against an ENF database. According to Rodríguez [19], if the evidence digital media contains ENF the Criterion can still be applied to detect edits even if no reference database is available.

Grigoras configured the first European forensic ENF database in Bucharest, Romania in the late 1990's [1], [4], [8], [16]. Since that time Grigoras has made some changes to the database configuration. Initially, Grigoras used a three resistor voltage divisor in the ENF probe circuitry. Eventually, the ENF probe circuitry was updated to include the series of anti-parallel diodes to protect the computer soundcard from network spikes and higher voltages. During the tests performed at the NCMF the best component values were determined and this became the modern ENF probe [22].

Grigoras sampled the ENF signal at 120 Hz initially, but as he developed the zero-crossings extraction method, higher sampling rates were required. This is the reason that high-resolution ENF databases should sample audio at 6 kHz – 8kHz. The model that is used in Grigoras' database influenced the model that the NCMF uses in Denver, Colorado. The Bucharest database utilizes an ENF probe to step the 240 VAC 50 Hz signal down to a 6 VAC 50 Hz signal. The signal passes through a three resistor voltage divisor and then a series of anti-parallel diodes limits the amount of voltage that can pass to the output. The output of the ENF probe is connected to a computer soundcard and then the system captures the ENF signal at 8 kHz. The files are backed-up continuously and then processed as needed. The acquisition computer is connected to an Uninterruptable Power Supply to protect against short-term electric network interruptions.

Alan Cooper of the Metropolitan Police in England also maintains a Forensic ENF database. The United Kingdom electric grid is independent of continental Europe but is also a 50 Hz grid. Using bespoke software based on STFFT and quadratic interpolation, designed from the ground up in MATLAB, Cooper digitizes the ENF signal by first utilizing a step-down transformer that reduces network voltage to a safe level for a high-quality 16-bit computer soundcard. Then, after the appropriate software interface processing, the ENF signal is estimated using STFFT and quadratic interpolation procedures that can be found in Cooper's 2009 International Journal of Speech Language and the Law article [13]. The incoming signal values are saved to a .MAT file along with the time and date of creation. Atomic radio clocks are used to synchronize the acquisition systems clock to BIPM time. Cooper's current ENF database superseded his original database configuration in 2008. In the original

Metropolitan Police ENF database, Cooper developed a clever method to overcome the time and frequency resolution tradeoffs that were inherent with the "off the shelf" FFT analyzers. By using the non-linear ENF signal and the even-order harmonics, the $100^{th}$ harmonic of the ENF fundamental was used to monitor the electric network variations. The nominal ENF in the UK is between 49.5 Hz – 50.5 Hz, the $100^{th}$ harmonic is 5 kHz and was expected to fluctuate between 4950 Hz – 5050 Hz because 49.5x100 and 50.5x100 create that range. Thus a higher order FFT could be applied to a frequency range of 100 Hz instead of a 1 Hz range, and this in addition to zero padding the time domain values created accurate peak frequency estimations. After each FFT, the peak values were selected from a 1.5 second window, creating a vector of peak frequency estimates. The estimated values were then interpolated back down to 50 Hz and the database archive was created with 100 times as many frequency estimates for a given time period [11].

The NCMF maintains the primary US Western grid forensic ENF database. The NCMF database is comprised of two independent acquisition computers that run in parallel. Each computer is fed the ENF variations from separate ENF probes plugged into the sound cards. Each computer is plugged into a UPS and the recording software is offset by 12-hours so that PC1 changes files at 23:59 and PC2 changes files at 11:59. Each computer has its own atomic-radio clock that synchronizes the system's time with the NIST WWVB radio station in Fort Collins, Colorado [22].

The TFSL in Las Vegas, Nevada maintains the secondary US Western grid forensic ENF database. This database also utilizes a dual acquisition system offset by 12-hours. Each acquisition computer has its own ENF probe that is feeding the computers sound card. The files are written to a Solid State Drive and the OS is contained on a separate Hard Disk Drive. The TFSL has their own internal network which is protected by firewalls inside the larger Target network that is also protected. TFSL utilizes NIST NTP to synchronize the acquisition system clocks. UPS units are in place to prevent loss of power and to provide continued recording during a power outage.

The TFSL in Minneapolis, Minnesota maintains the primary US Eastern grid forensic ENF database. This database also utilizes a dual acquisition system offset by 12-hours. Each acquisition computer has its own ENF probe that is feeding the computers sound card. The files are written to a SSD and the OS is contained on a separate HDD. The TFSL has their own internal network which is protected by firewalls inside the larger Target network that is also protected.

TFSL utilizes NIST NTP to synchronize the acquisition system clocks. In section 3.2 the recommendation is made to use atomic-radio clocks or GPS time receivers but because of the unique scenario that the TFSL internal network is configured a decision was made that security risks were negligible. This decision was based off of a rigorous penetration test by Target Information Security Services. UPS units are in place to prevent loss of power and to provide continued recording during a power outage. Appendix B outlines this database configuration in detail.

## 2.5 Further Directions for the ENF Criterion

The fundamental foundations for the ENF criterion have been tested, verified, and confirmed in Europe, the United Kingdom, the United States, and Canada. The ENF criterion has been accepted into court rooms in the United Kingdom, Romania, Poland, Cyprus, Denmark, and the International Centre for Settlement of Investment Disputes (Washington D.C., USA) [72]. The ENF criterion has stood up against peer review in the Audio Engineering Society, Institute of Electrical and Electronics Engineers, International Journal of Speech Language and the Law, Institute of Forensic Research, and the Forensic Science International. The ENF criterion has been adopted by the Forensic Speech and Audio Analysis Working Group and incorporated into a forensic best practice in Europe. In academia, a thesis from Nottingham Trent University focuses solely on ENF and ENF research is carried out at the NCMF. The ENF Criterion has been widely accepted across the forensics community. The forensics community spans across international borders; national laws on the other hand, do not span international borders.

In order for the ENF criterion to reach its full potential in the United States it must have best practice guidelines in place from US scientific working groups such as the Scientific Working Group on Digital Evidence (SWGDE). In addition, the ENF Criterion must be accepted into US courts by satisfying Daubert or Frye standards by demonstrating that the theory or technique is falsifiable, refutable, and testable; the basis of the expert's opinion has been subjected to peer review and publication; the techniques used in arriving at such conclusions have a known or potential error rate; there are existing methods and maintenance of standards and controls concerning the operation of those methods or techniques; or the theory and technique is generally accepted by a relevant scientific community. The ENF Criterion meets the Daubert and Frye requirements. The ENF criterion has been used by law enforcement and forensic experts outside of the laboratory, which demonstrates that the ENF Criterion is

falsifiable, refutable, and testable. The ENF Criterion has been published in several peer reviewed scientific journals, which demonstrates that the ENF Criterion has been subject to peer review. The ENF Criterion has known error rates for automatic search algorithms and the spectrographic extraction method has a negligible error rate for low noise evidence recordings, which demonstrates that there is known and published error rates for the ENF Criterion. The ENFSI working group maintains a best practice manual for the ENF Criterion in Europe and it is logical to assume that soon SWGDE will maintain a best practice manual for the US, which demonstrates that there are maintained standards for the ENF Criterion. There have been several scientists in the forensics community from around the world that have researched, used, and verified the ENF Criterion, which demonstrates wide acceptance of the ENF Criterion among a relevant scientific community. Since the implementation of the secondary US Western grid ENF database the Criterion can now go through cross validation tests for databases sharing the same grid, which will assist in the maintenance and control of standards and methods surrounding the ENF Criterion.

Further research into ENF probe circuitry is being conducted that will advance the capabilities of the ENF probe to include hardware low-pass filters, radio technology for broadcast purposes, and internal data storage. Examination techniques are continually being updated and clarified, such as automatic database search algorithms. Statistical research is being carried out to help develop a better understanding of electric grid variations, probability of repetitiveness, and the effect lossy compression algorithms have on ENF signals. ENF research is fostering further development and potential; ENF will continue to be on the cutting edge of forensic research and forensic examination on media evidence.

## 3. Investigating the Forensic ENF Database Configuration for use in Digital Media Authentication

In this chapter, fifteen areas will be investigated to discover the methods in which an advanced and robust high-resolution ENF database can be configured to satisfy forensic standards such as accuracy, reliability, and reproducibility. These areas have been researched through tests conducted at the NCMF and Target Forensic Services Lab (TFSL) and have been determined to be of importance for anyone wishing to build an ENF database for forensic purposes. For anyone wishing to use an ENF database for authentication of digital media, the first step to ensuring that their database meets forensic best practices is to respect the guidelines that are explained in a variety of literature on ENF research. Many of the available research articles focus on the methods of applying the science behind ENF but briefly discuss configuring the entire ENF database system. This chapter will take an investigative approach into the configuration of an ENF database and expand on the advantages and disadvantages of different configurations. Disrespecting recommended configurations could diminish database security, integrity, and reliability; eventually leading to erroneous findings, faulty science, and judicial error. To maintain accuracy, reliability, and reproducibility the areas outlined below have been identified as important and necessary guides for a forensic ENF database from functionality, security, redundancy, and administrative points of view; which combined, take into account the precautions for ultimately examining the evidence, interpreting the results, and preparing a report for use in the court room as well as advancing scientific research for peer-review.

The areas outlined below are not listed in order of priority and each one should be considered just as important as the others. Each area has an impact on the integrity of the database. Each area can affect database security, database functionality, database reliability, or a combination of these foundations. The fifteen areas explained below are: The NCMF ENF probe; atomic-radio clock/source clock synchronization; sampling frequency, advantages of high resolution ENF databases and resolution/FFT settings; sound card, input level, and signal to noise ratio; type of storage (HDD vs. SSD); Direct Current (DC) bias and Frequency bias; distortions; network failure/Uninterrupted Power Supply (UPS) and safe guards; advances in ENF database configuration; and other areas to pay attention to.

### 3.1 The NCMF ENF Probe

At the core of most ENF databases there will be an ENF probe. The ENF probe is a small and simple device that receives the US 120 VAC 60 Hz (UCTE 240 VAC) signal and outputs a signal that is safe to plug into a computer sound card for recording ENF variations and compiling ENF database files. Due to the inherent differences in electronic components, building multiple ENF probes to create multiple databases with matching waveforms can be challenging. This challenge was addressed and solutions were offered [22]. By using MATLAB it was possible to determine the proper combination of ENF probe components for the NCMF and TFSL database configurations. Time, effort, and money were saved by using software to determine the proper combination of components to build a high-quality ENF probe that accurately records the ENF variations from the grid to the database. In Figure 2, the darkest line represents the calculated waveform that was obtained from using the proper components for the ENF probe circuitry utilized in the NCMF and TFSL forensic ENF databases.

One schematic has been proposed by Rich Sanders of the NCMF [12]. Sanders' schematic was based on a voltage divisor with three resistors. Since that time, tests have been performed using various schematics at the NCMF and conclusions were made that a newer and more robust schematic was necessary in order to protect the computer soundcard from network voltage spikes and to capture ENF without clipping the waveform. Several variations of the ENF probe circuitry were simulated and experimented with to determine the components that will output a waveform free of clipping and distortions. The main concept of the ENF probe is to take an electric grid signal from any wall socket and step the signal down to a line-level signal that is safe to plug into a soundcard. This is accomplished by using a transformer that converts the mains US 120 VAC (UCTE 240 VAC) to 6 VAC. Next, the signal is divided through a three resistor voltage divisor. Then, to protect the computer soundcard against possible network spikes or higher voltage levels a series of anti-parallel diodes are used at the probe's output (see Figure 3).

When executed on the US 120 VAC Western grid, the output voltage of the NCMF ENF probe was ~550 mV with an impedance ~280 ohms relative to the sound card used. This was accomplished by using the following component values: R1 & R2 = 1.5 kΩ, R3 = 200 Ω, D1, D2, D3, & D4 = 1N5863. When building an ENF probe it is recommended to first simulate the ENF probe schematic and determine the components that will best suit the needs of the system that the ENF probe is intended to be used in.

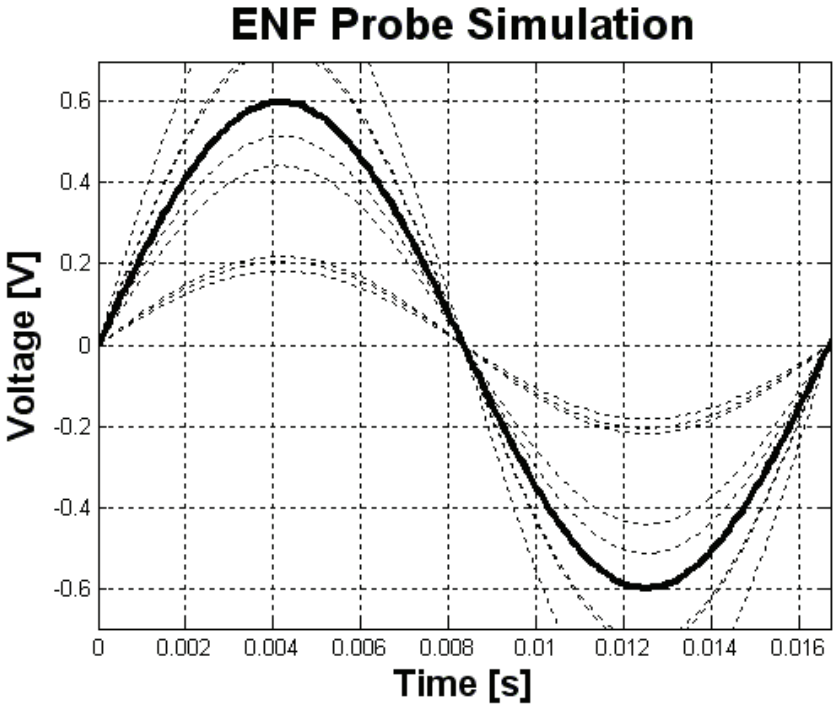


**Figure 2** Probe Output Waveform

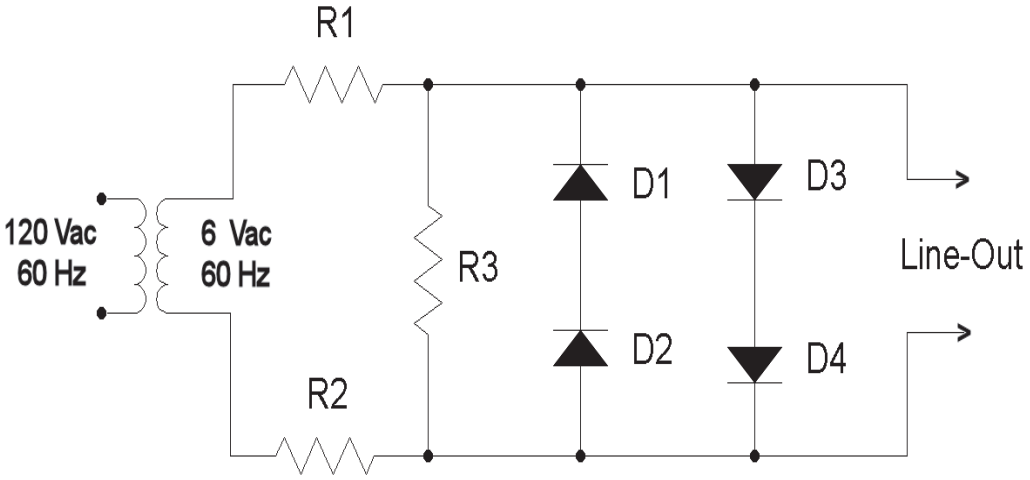


**Figure 3** Proposed Schematic for ENF Probe

Another solution is to replace R3 with a variable potentiometer which will allow the user to calibrate the ENF probe to best suit their configuration. An ENF probe with variable amplitude was constructed at the NCMF by Jenkins and Scott Anderson and tested to confirm the findings of the software simulation. Through this experiment it was decided that the variable potentiometer can be used to calibrate the ENF probe to function optimally with a wide variety of sound cards or other components. An optimal calibration shall be one that results in a waveform that is not too low in amplitude nor too high in amplitude and also free of clipping and distortions. High/low amplitude, clipping, and distortions are factors that can cause challenges when attempting reproducibility, automatic database searches, and zero-crossings extraction.

The implementation of the ENF probe shall be carried out by connecting the ENF probe directly to the wall socket and not the UPS, power strip, or surge protector. By connecting the probe directly to the wall socket, one will eliminate the possibility of the US 120 VAC (UCTE 240 VAC) signal being processed through any power conditioning or voltage regulation circuit before reaching the probe. Such circuits can commonly be found in UPS units, power strips, and surge protectors. Another reason to connect the probe directly to a wall socket is that in the event of network interruptions there will be no ENF signal but the probe will unnecessarily draw power from the UPS, causing the database to record the battery variations of the UPS. If the probe is directly connected to a wall socket when the network returns to normal operation, the probe will automatically be initiated and continue sending signal to the soundcard. As long as the UPS is able to power the PC during the network interruption the entire system should remain record enabled and continue recording when the network returns to normal operation. Figure 4 shows a completed NCMF ENF probe with variable amplitude.

There is still room for advances in the ENF probe, such as, on-board Low Pass Filters (LPF), on-board Analog to Digital (A/D) Converters, wireless transmission (see chapter 4), and on-board storage. For example, Figure 5 displays a graphical tool that can be used to help determine the optimal components for an on-board Low Pass Filter (LPF). Using an on-board LPF can help mitigate aliasing distortions in case the sound card LPF is not functioning properly. In Figure 5 the top graph displays 0.2 seconds of a 60Hz sine wave resulting from the component values in Figure 3. The amplitude of the waveform from the schematic with the added resistor and capacitor has been attenuated slightly but this can be adjusted at R3. This way, the amplitude can be checked to ensure that it is not too low in amplitude nor being clipped by the diodes.

Additionally, a variable resistor can be used in place of R3, or different component values can be experimented with to optimize the waveform amplitude. In the middle graph of Figure 5, the Long Term Average Spectrum (LTAS) of an ENF database file is displayed. The first spike indicates the 60Hz fundamental and the other spikes are harmonics of that. The X-axis spans from 0 Hz to 4000 Hz because this file was sampled at 8 kHz meaning that there are no values above *fs*/2 or 4000 Hz. The bottom graph in Figure 5 displays the same ENF database file after the LPF has been applied. In this instance, the LPF was created by adding a 12.25Ω resistor and a 6.49 uF capacitor to the ENF probe schematic presented in Figure 3, resulting in a cut-off frequency at roughly 2000 Hz, for demonstration purposes. This tool can be used to determine which components will result in a cut off frequency at 4000 Hz or slightly below 4000 Hz. This information can be used to build a hardware version of the schematic and be tested to verify that an ENF probe with on-board LPF will eliminate or attenuate aliasing distortions when the sound card or software LPF is not functioning properly.

**Figure 4** NCMF ENF Probe

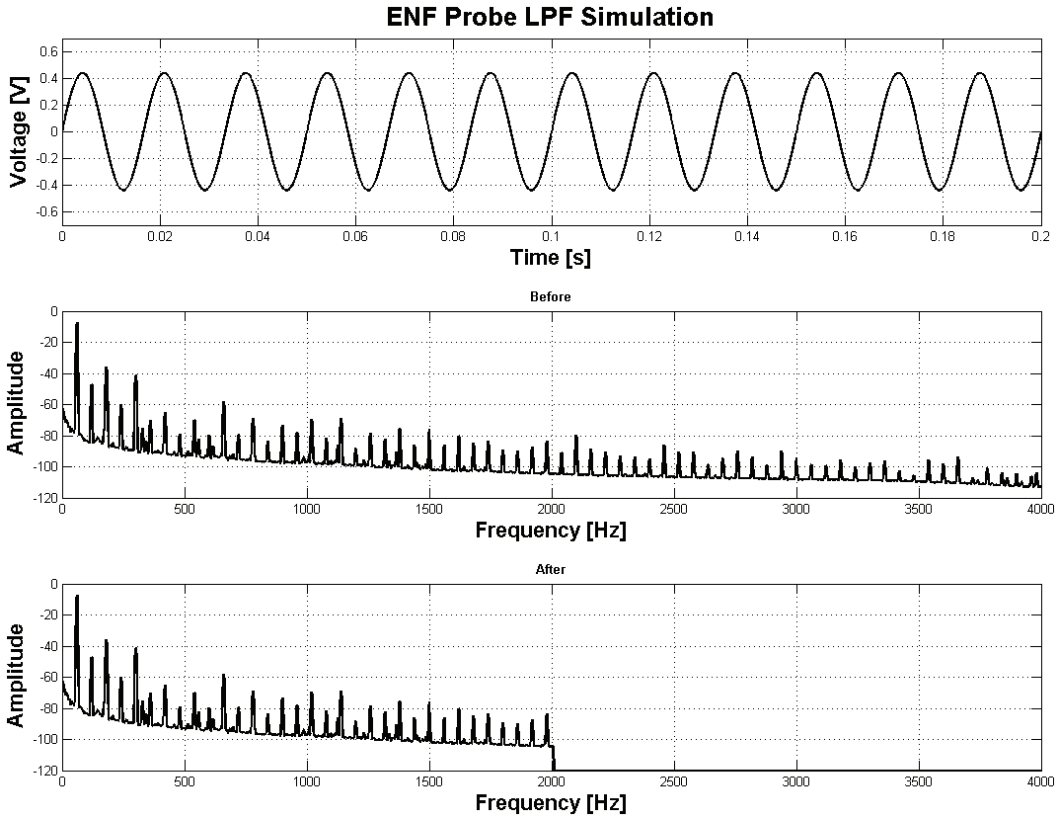


**Figure 5** ENF Probe LPF

### 3.2 Atomic Radio Clock/Source Clock Synchronization

An atomic clock/source clock is a time controller independent of the electric grid, capable of keeping the database system clock synchronized with an accurate time reference that is also unaffected by electric grid activity. For a forensic ENF database it is crucial that the time controller of the database is synchronized with a reference source that is as accurate as possible. Any deviation of this standard will cause the database time to fluctuate due to quartz oscillators found in computers being unreliable when not synchronized periodically [24] [25] and over time could result in the database providing erroneous results and irreversible judicial errors. For these reasons it is suggested that an ENF database be synchronized with the National Institute of Standards and Technology (NIST) atomic time standard, known in the United States as NIST Universal Coordinated Time (UTC NIST). There are three different ways

that an ENF database can be synchronized with the NIST time standard and these different approaches will be discussed below as well as a brief explanation about how the entire atomic clock system operates and how the calculated time standard is transmitted across the United States.

UTC is a 24-hour time keeping system based on the International Atomic Time Scale, which serves as the foundation for timekeeping around the world [26]. There are approximately 200 atomic clocks such as the NIST-F1 around the globe in about 60 laboratories used to maintain the UTC time. The Earth's Prime Meridian (0 degrees longitude), located near Greenwich, England is where the hours, minutes, and seconds expressed by UTC represent the time of day. All other times around the globe are based from this starting point, moving East of the Prime Meridian adds one hour for each consecutive time zone, likewise, moving West of the Prime Meridian subtracts one hour for each consecutive time zone. The Bureau International des Poids et Measures (BIPM) is responsible for calculating the time reference for UTC. BIPM accomplishes this task by averaging data from the 200+ atomic clocks housed in ~60 laboratories around the globe. There are a few different types of atomic clocks used around the globe but for the purposes of this thesis the most accurate atomic clock will be focused on, which is located in Boulder, Colorado at the NIST laboratories.

The NIST-F1 atomic clock is known as a fountain clock because of the way it calculates time, by filling a vacuum chamber with a gas of cesium atoms, gently influencing these atoms to take the shape of a sphere using lasers that simultaneously cool the atoms to near absolute zero, and directing this sphere of atoms through a microwave cavity [27]. The lasers gently force the sphere of atoms to rise about 1 meter, then due to the Earth's gravity, this sphere of atoms falls back through the microwave cavity and passes another laser that shines a light onto the atoms. Any of the cesium atoms that had their atomic state altered by the microwaves emit photons when the light hits them and a detector senses this light and auto-calibrates the frequency of the microwave cavity until the resonance frequency of the cesium atom is obtained around 9,192,631,770 Hz. The standard for the duration of a second is thus defined as the amount of time it takes a cesium atom to cycle 9,192,631,770 times. Atomic clocks are not standard "time of day" clocks but rather they provide a ticking rate for time of day clocks. When asked about the way NIST configured the NIST-F1, Chief of the Time & Frequency Division at NIST, Dr. Tom O'Brian was kind enough to provide the following information:

*The ultimate source of all time and frequency information distributed by NIST is the NIST time scale at the NIST facilities in Boulder, Colorado. The time scale comprises a system of about a dozen commercial atomic clocks, which are regularly calibrated by the NIST-F1 primary frequency standard. NIST-F1 is not a "time of day clock," but is a frequency standard that is used to provide the "ticking rate" for the time scale. The commercial atomic clocks in the time scale are fairly stable, but not accurate – that is, each clock's "ticking rate" stays fairly constant for weeks to months, but each of the dozen clocks may "tick" at a different rate. NIST-F1 is used to provide a common "ticking rate" (frequency) for all the clocks. A complex measurement system produces a real-time average of all the clocks, based on their recent stability, and produces the continually changing value of NIST time.*

*This rather complex system is needed because the world's most accurate frequency standards, such as NIST-F1, are too complex to operate continuously. A clock measuring time of day cannot be "off" for even an instant, or the time of day is lost. The time scale provides the continual realization of the time of day, and continues to operate well even if one or several of the approximately dozen clocks have failed. NIST-F1 is used to provide the best possible frequency ("ticking rate") so that the time scale time of day is as accurate as possible.*

*The NIST time scale is compared several times per day with similar time scales across the world in about 60 timing laboratories. The International Bureau of Weights and Measures in France (French acronym BIPM) uses time from NIST and these other approximately 60 labs to produce the official international time, Coordinated Universal Time, UTC. NIST and the other labs produce their own version of UTC, for example UTC(NIST). UTC(NIST) is official US time, and the time that is distributed by all NIST time and frequency services.*

NIST sends this information from Boulder Colorado, where the NIST-F1 resides, to Fort Collins Colorado where the WWVB NIST radio antenna array resides [28]. The time reference information is sent from the Boulder lab to the Fort Collins antenna array via Global Positioning System (GPS) Common-View (see Figure 6). The GPS Common-View is a measurement technique used to compare two clocks at remote distances from each other. Using a single reference, the Common-View method directly compares two clocks to each other. Errors from the two paths that are common to the reference cancel each

other out and the uncertainty caused by path delay is nearly eliminated [29]. NIST also maintains a number of servers around the United States that can communicate with just about any computer that has access to the internet. These servers also provide synchronized time from the atomic clock. The time signal being sent from the NIST server to a remote computer via internet connection is typically compensated with a 50ms lead time so that when the signal arrives at the computer the marker reference is closer to the actual time instead of being delayed by the amount of time the signal took to travel from the server to the end user. NIST also utilizes GPS to transmit the atomic time reference to the end user. This is accomplished through satellite communications. Radio is not the only way that NIST transmits the time information from the atomic clock to the end user. An ENF database can potentially be synchronized to NIST time in three ways; by radio clock, internet connection, or GPS signal. There are advantages and disadvantages of each system. In order to understand which method is best suited for a forensic ENF database, these three systems will be discussed and the considerations for each of them from a reliability and security point of view.

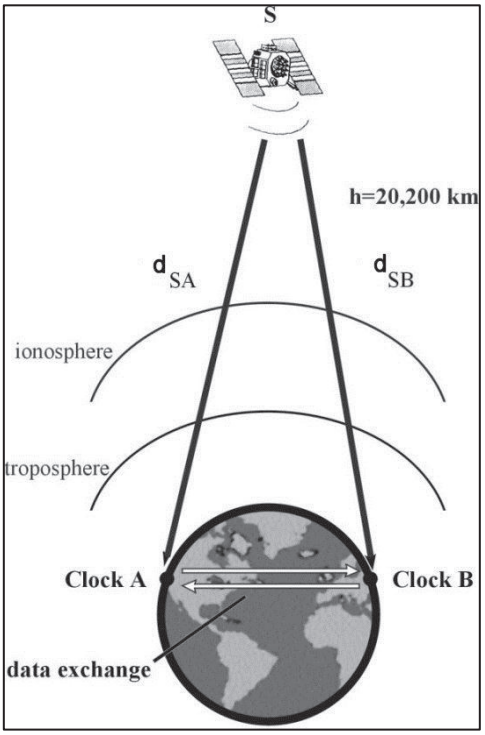


**Figure 6** NIST GPS Common-View Satellite Communications

### 3.2.1 NIST Radio Synchronization

The WWVB NIST radio station in Fort Collins, Colorado broadcasts time information for millions of radio clocks in the continental United States on a 60 kHz carrier signal using pulse width modulation where the carrier power is reduced by 17 dB at the start of every second then full power is restored 0.2 seconds later to signify a binary "0" or 0.5 seconds later to signify a binary "1" [25], [27], [30]. Other information is contained in the broadcast such as year, day of the year, hour, minute, second, day light savings time or standard time, leap years, and leap seconds by utilizing binary coded decimal to convey this information into what is observed when reading a radio wrist-watch or clock. Even though it is a common misconception to call radio clocks "atomic clocks", due to the fact that there is nothing atomic about the radio clock, radio clocks still keep their time based off of the ticking rate coming from atomic clocks such as NIST-F1 and so they are commonly referred to as atomic clocks. Perhaps the greatest advantage in using a radio clock to synchronize the forensic ENF database time controller is that the grid variations and the radio broadcasts are two completely separate and independent systems. Any malfunctions in one system will not affect the other. For example, if there is a catastrophic grid failure the radio station will continue broadcasting as normal because of the redundant and sophisticated system of UPS units, back-up diesel generators, and power switching mechanisms all housed on site in Fort Collins, Colorado. A similar fail-safe system has been implemented in the NIST Boulder, Colorado lab where the laboratory can operate at full capacity for days between fueling the back-up generators. This means that the time keeping system will continue to operate smoothly even while the grid is down. When the electric network returns to normal operation the database time controller will re-synchronize to the radio clock and the database time will still be accurate. Another advantage to the radio synchronization method is that it does not introduce any type of security risk to the database, where internet connectivity has the potential to.

Perhaps the biggest disadvantages of synchronizing the ENF database time controller to a radio clock is that the radio transmissions are susceptible to an increasing amount of electromagnetic interference especially in densely populated areas, the radio clock must be situated in a place that the signal can be received such as a window or a place with a clear view of the sky, and there is only one broadcast site in the lower 48 states resulting in varying signal strength. The path delay in the radio broadcast system is measurable but negligible. The radio station clock is synchronized with the NIST-F1 via the GPS Common-View described above, once the radio station clock signal is sent through the

transmitters, antenna feed lines, and the antennas themselves there is a resulting delay of approximately 0.000,017 seconds which means that over the course of 170,000 years this system would introduce a 1 second off set from the source clock. In addition to this delay there is a certain amount of delay introduced by distance of the receiving clock from the radio station antenna. In ideal conditions the delay of the electromagnetic 60 kHz wave traveling through free air would equate to about 10ms delay for every ~1,864 miles. Because these delays are so minuscule NIST does not compensate for any transmission delays.

### 3.2.2 NIST Internet Synchronization

NIST maintains +/- 26 servers across the United States from California to New York that can be connected to from almost any computer with internet access in order to synchronize a computer's clock to UTC (NIST) time [31]. Updated Server information and IP addresses can be found at (http://tf.nist.gov/tf-cgi/servers.cgi). Many Operating Systems (OS) such as Windows, Mac OSX, and Linux allow the system clock to be synchronized automatically at periodic intervals with an external source via the Network Time Protocol (RFC-1305), Daytime Protocol (RFC-867), or Time Protocol (RFC-868).

RFC-1305 is the most popular protocol because this is the most robust and accurate of the three. RFC-1305 runs continuously in the background of most OS and periodically gets updates from a number of servers. This protocol takes an average from the servers, disregarding those that appear to be wrong, and updates the computers system clock to the averaged value. The computer's OS receives the time stamp in UTC seconds since January 1, 1900. Some home computers use a variation of RFC-1305 called Simple Network Time Protocol (SNTP), which makes a single request to a single server. Likewise, the RFC-867 and RFC-868 do not do any type of averaging; these protocols make a single request to a single server and set the computer's clock to the received time.

RFC-867 includes additional information with the time stamp such as Julian Date (an integral number of days since noon January 1, 4713BC. For example, September 11, 2011 is 2,455,815.5). Daylight savings time or Standard time, server health, the number of milliseconds being compensated for transmission delay, an indication that the OS is receiving UTC(NIST), and an on the mark indicator that tells the system what the time is when the mark is received are also included in the transmitted information. According to the NIST

website, the RFC-868 is only used by 1% of consumers and will eventually be phased out [31].

Out of the three ways a computer can be synchronized with NIST time via internet RFC-1305 is the most widely used and most robust. Another advantage of using NTP synchronization is that RFC-1305 is not susceptible to electromagnetic interference or varying signal strength the way that radio clocks are. In common with each other, the radio broadcast systems, GPS broadcast systems, and the internet broadcast systems are completely independent of and separate from any electric network failures and safe guarded with several back-up generators and redundant equipment. There are disadvantages to connecting a forensic ENF database to the internet however; occasional lapses in internet communications such as problems with trunk lines or Internet Service Provider (ISP) servers can cause the synchronization to cease. Another disadvantage is the overall security risk of having a forensic ENF database open to the outside world. Having a forensic ENF database exposed to outside threats seriously diminishes the integrity of the database. Imagine that someone with enough skill could access the database and change the names of the files to represent a different day or delete files all together. Internet synchronization is a two way communication where radio and GPS synchronizations are one way communications. The third method for synchronizing an ENF database to UTC(NIST) time is the GPS system.

### 3.2.3 NIST Global Positioning System Synchronization

NIST provides a GPS service for synchronizing computer time controllers that is compiled from approximately 24 satellites orbiting the Earth; each satellite has an onboard clock and keeps the onboard time synchronized with an average from the atomic clocks located around the world [32], [33], [34]. The advantages of using a GPS system to synchronize a forensic ENF database are: Most GPS time receivers on the market can track 8 – 12 satellites simultaneously, can provide an average of date and time information from all satellites in view, can provide time and date information in a computer readable format, and most units produce a 1 pulse per second (pps) electrical output that can be synchronized to within 100ns of UTC. Even though there can be some transmission path delays due to ionosphere and tropospheric conditions, angle of the satellite to the receiver, and hardware instabilities or inconstancies, the overall reliability of the GPS system is impressive and statistically has shown 24-hour averaged accuracy to within 10 ns. The graph in Figure 7 shows the 24-hour nanosecond uncertainty for September 10, 2011. The highest uncertainty was almost 15ns but overall the

change's intra-variability was within less than 10ns. This graph was obtained from (http://www.nist.gov/pml/div688/grp40/gpsarchive.cfm). The GPS system shares a common theme with radio and internet broadcast, all these systems are independent of the electric network.

The best way to implement a forensic ENF database time controller shall be to create a fail-safe dual source clocking system. The primary time controller should be the radio clock receiver and the secondary time controller should be the GPS time receiver. In this manner the radio clock will automatically be synchronized at set intervals and the system can be configured so that if a time period longer than X-hours passes without a synchronization-update then the GPS clock will automatically take over. A sophisticated system will use both time controllers and average the time between both to synchronize the database time. A system configured in this manner will ensure that an accurate radio signal controls the system clock and in the event that radio signal is lost the GPS source will ensure that continued accurate time synchronization is maintained. The reason that it is best practice to use the radio source and GPS source is that these two systems are one-way communications and do not introduce a security risk like the internet transmission does.

In certain facilities, the database is surrounded by concrete walls and does not have exposure to any windows, making it very challenging to obtain a clear transmission signal for radio or GPS. One solution is that antenna receivers can be connected to both the radio and GPS time receivers via long cable runs. The antennas can be attached to the outside of the building or in a place with a clear view of the sky and send the information to the time controller via the cable run. Using the accurate time source from NIST or BIPM will ensure that the acquisitions system clock is accurate with a consistent ticking rate and will help mitigate sampling frequency offsets or frequency bias (see section 3.6).

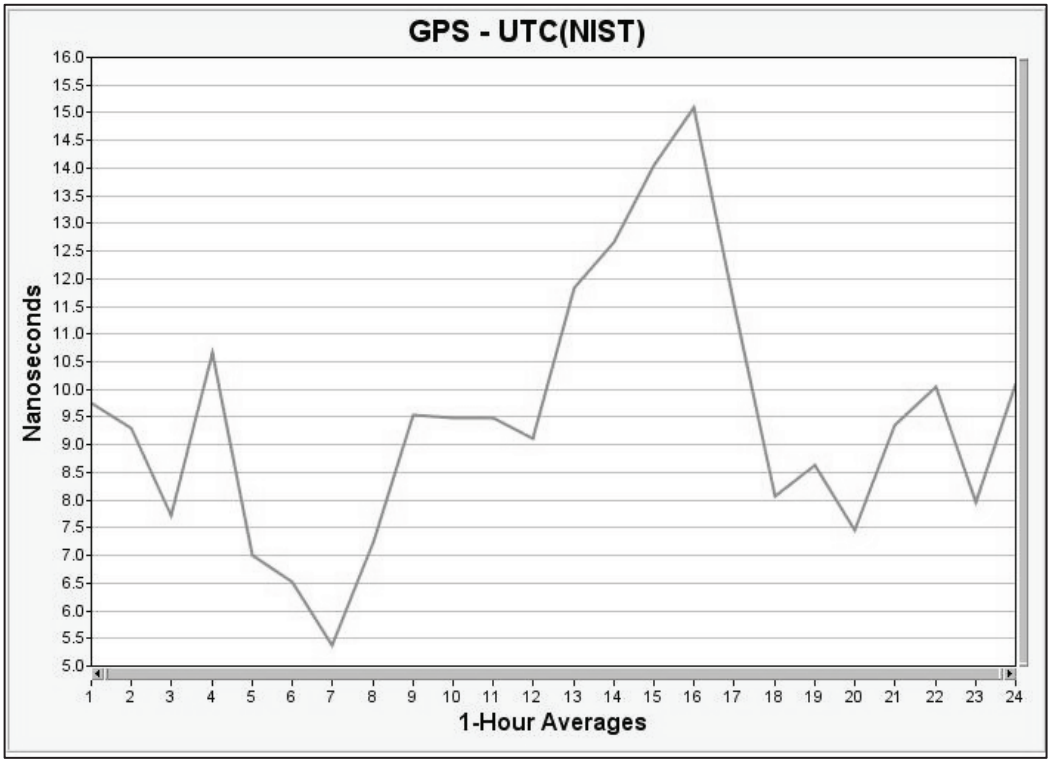


**Figure 7** NIST GPS Time Accuracy Over 24-Hours (09/10/2011)

### 3.3 Sampling Frequency

Sampling frequency (*fs*) or "sampling rate" is the rate at which discrete values are assigned in the digital domain to represent a continuous waveform. Digital audio is a binary representation of a sound waveform. In order for a sound waveform to be stored in a digital format the waveform must somehow be converted from its natural state as a pressure wave propagating through a medium to a series of discrete values. The most popular method for this conversion is called Discrete Time Sampling (DTS) where a two dimensional matrix is used to represent sound waveforms as digital audio waveforms. Traditionally, a waveform graph displays the X-axis as time and the Y-axis as amplitude. In most audio editing software, the resolution of the waveform X-axis is determined by the sampling frequency and the resolution of the Y-axis is determined by the bit depth (time vs. amplitude). A 44.1 kHz 16 bit .WAV PCM file for example, will be an audio waveform represented with 44,100 samples per second on the X-axis for time and 65,536 (2^16) data points on the Y-axis for amplitude. This popular sampling rate is a standard resolution because it

accurately reproduces the original waveform to a degree that the human brain can interpret all audible frequencies as continuous. There are of course several factors that come into play when the term "accurately reproduces" is used, such as: quality and/or frequency response of the microphone(s), preamp noise, aliasing error, and the list can be extended. The best way to mitigate errors in the recording process is to use high quality components, well designed circuits, and proper gain stages as will be discussed later in sections 3.4 and 3.7. There is also a technical reason that 44.1 kHz has been adopted as an industry standard; the Nyquist theorem states that the sampling frequency should be at least twice as high as the highest frequency in the signal. Since most humans are limited from 20 Hz – 20 kHz in the frequency range that they can perceive; a sampling frequency of 44.1 kHz allows for all the audible frequencies to be reproduced without aliasing (refer to section 3.7).

For safe measure, most sampling frequencies are decided by doubling the highest frequency to be reproduced and adding 10% - 20%. For a forensic ENF database it is recommended in the June 2, 2009 Forensic Speech and Audio Analysis Working Group (FSAAWG) document [14] that "*the desired signal shall be sampled at twice the highest frequency plus 20%*". The desired ENF signal is around 60 Hz (50 Hz UCTE) and thus the minimum sampling frequency shall be 144Hz (120 Hz UCTE). The recommended sampling frequency for ENF databases however, is 6 kHz – 8 kHz which will leave room for further types of analysis without taking up an unmanageable amount of storage space. Figure 8 illustrates how a sound's waveform is turned into a series of discrete values. Each data point falls at a certain interval along the X-axis determined by the sampling frequency; simultaneously each data point is assigned a position on the Y-axis determined by bit depth representing amplitude.

Implementing a proper sampling frequency for a forensic ENF database is crucial and 6 kHz – 8 kHz is the recommended sampling frequency for a forensic ENF database. 6 kHz .WAV files will be approximately 1GB per 24-hours and 8 kHz .WAV files will be approximately 1.3GB for every 24-hours and will help to manage storage requirements. Even though the target signal is 60 Hz (50 Hz UCTE), sampling at 6 kHz – 8 kHz allows for various types of ENF extractions and scientific research such as zero-crossings.

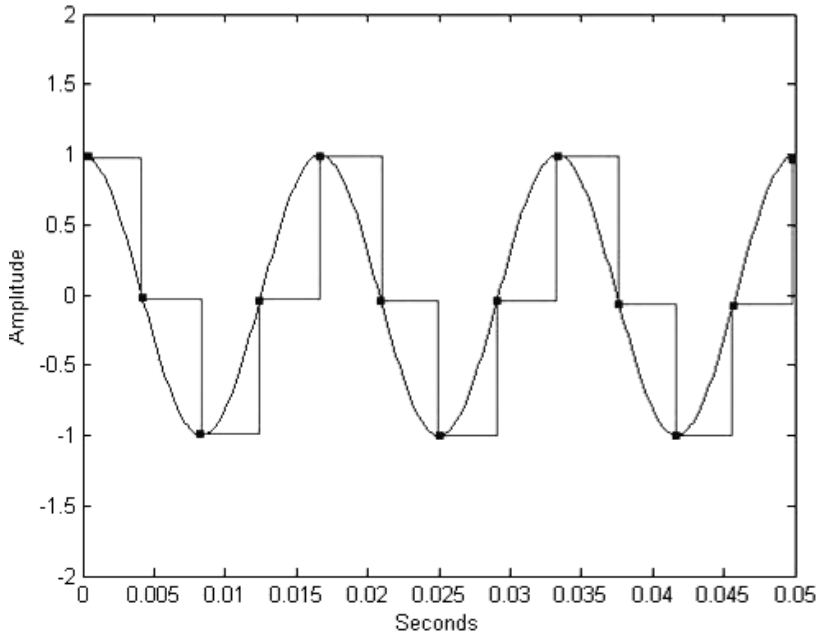


**Figure 8** Continuous Waveform to Discrete Waveform

### 3.3.1 Advantages of High-Resolution ENF Databases

There are several advantages to configuring a forensic ENF database to sample audio at a high sampling frequency. Having a forensic ENF database configured to record the ENF signal at 6 kHz – 8 kHz allows for various types of ENF extraction methods and further scientific research. When the 60 Hz (50 Hz UCTE) signal is captured at 6 kHz – 8 kHz the harmonics of that signal are captured up to 3 kHz – 4 kHz. The harmonics can be useful when employing different types of forensic analysis and scientific research. The zero-crossing extraction methods in particular benefit from a high sampling rate because a high resolution waveform will more precisely place the zero-crossing in the correct, or as close to correct, place as possible.

### 3.3.2 Resolution/Fast Fourier Transform Settings

Resolution and Fast Fourier Transform (FFT) settings are critical parameters for ENF extraction methods and can be affected by the sampling frequency that the audio was captured at. The resolution and FFT settings can drastically affect the results of the spectrographic, time-domain, and frequency-domain extraction methods. Time and frequency are inversely related when

applying FFT. The more frequency resolution one obtains by increasing the FFT order to 16,384 for example, the less time resolution will be available. The more time resolution one obtains by decreasing the FFT order to 512 for example, the less frequency resolution will be available. This is because resolution can be defined as: Resolution (R) = Sampling Frequency (*fs*) / Fast Fourier Transform (FFT) order or [16]:

$$R = \frac{fs}{FFT} \quad [1]$$

For example, if the sampling frequency is 144 Hz and the FFT order is 16,384 then the resolution will equal 0.008 Hz. If the sampling frequency is 8 kHz and the FFT order is 512 then the resolution will equal 15.6 Hz. This means that when the ENF signal is down-sampled to 144 Hz and the FFT order is 16,384 it is possible to analyze variations as small as 0.008 Hz. When the ENF signal is left at 8 kHz analyzing frequency variations less than 15.6 Hz can be, to put it mildly, challenging. On a technical note, analyzing the UCTE 50 Hz signal is superior to analyzing US 60 Hz because the 50 Hz signal can be decimated more than the 60 Hz signal due to Nyquist limitations, thus the *fs* becomes smaller allowing for smaller observable variations of the frequency content.

The implementation of correct resolution/FFT settings is crucial for proper ENF extraction methods. These areas should be tested and analyzed on a case by case basis. Different cases or research will require different resolution/FFT settings; but whenever ENF comparisons are being made, the evidence and database files shall have the same time and frequency resolution.

### 3.4 Sound Card

The sound card is the interface that translates the analog signal coming from the ENF probe into a digitized representation of that waveform. There are a wide variety of sound cards available on the market such as PCI cards, PCI express cards, external USB cards, rack-mount units, and the list can be extended. The sound card is typically responsible for converting the analog signal to the digital signal, commonly referred to as an A/D converter. Sound cards can have a wide range of connection types from 1/8$^{th}$ inch, ¼ inch, XLR, RCA, and the list can be extended here as well. The type of sound card or the

connections for the sound card are not of great importance so long as the sound card is capable of performing its duty as an interface in a forensic ENF database.

The sound card used in a forensic ENF database shall have the capability to record at the desired sampling rate. The NCMF and TFSL sampling rates are 6 kHz – 8 kHz for ENF database .WAV files. A wide variety of soundcards on the market advertise the capability to "record up to XX kHz", the problem is that the soundcards may record at high sample rates but the soundcards may lack the ability to record down to 6 kHz – 8 kHz. As discussed in section 3.3, a 6 kHz – 8 kHz sampling rate captures the ENF signal enough times per second to fulfill the freedom to conduct various ENF extraction methods and scientific research without occupying an unmanageable amount of storage space.

Whichever sound card is decided upon, it should be tested and verified to be performing optimally, in other words, a Signal to Noise Ratio (SNR) of at least -94 dB as well as a Total Harmonic Distortion (THD) of at least 0.003% [16] to ensure the linearity of the original signal is not being compromised. Testing for aliasing, jitter, and other distortions should be conducted before the ENF database is operational. Software can be used to sample the signal instead of a hardware A/D converter but the software should be verified to be producing valid results through testing for aliasing, jitter, and other distortions. The software should also be able to sample at the desired sampling frequency of 6 kHz – 8 kHz. In section 3.7 distortions such as aliasing are discussed that can result if the soundcard/software is not low-pass filtering the signal correctly.

### 3.4.1 Input Level

Input level is the amplitude at which the ENF probes output is received when entering the acquisition system. The input level of the signal can also affect the integrity of the database by being too high or too low. The Input levels of recorded ENF signals at the NCMF are ~ -12 dB Full Scale (FS). This allows for a strong signal without clipping. Noise can also have an effect on zero-crossings and the input line should not be introducing noise. All electronic and electric systems are going to inherently introduce some level of noise. Depending on the type of noise being introduced it could add unwanted frequency components or could change the original signals linearity; such as Total Harmonic Distortion (THD). By using high-quality sound cards and high quality circuits it is possible to obtain low THD interference and avoid altering the relationship between voltage and current of the original signal. 0.003% THD is acceptable [16]. Unwanted frequency components can be added to the original signal in many

ways including poor circuit design, low-quality components, and improperly designed cables. The more leads, coils, and inductors that are introduced along the signal path the more potential there is for introducing unwanted noise into the database. In Windows 7 OS the configuration of input source and level can be modified through the Control Panel. RecAll Pro also has a tab under Preferences that allows the user to modify which driver RecAll Pro uses. Proper gain stages should be utilized to optimize the acquisitions system probe output, sound card/interface, and

### 3.4.2 Signal to Noise Ratio (SNR)

The signal to noise ratio can be defined as the difference between desired signal and unwanted noise, also referred to as noise floor. If the desired signal is -12 dBFS and the noise floor is -108 dBFS the signal to noise ratio would be 96 dBFS. In a forensic ENF database the signal to noise ratio is crucial for correctly implementing the extraction methods. The signal to noise ratio shall be as high as it is possible because low signal to noise ratios will decrease the ability to properly estimate peak frequency values potentially effecting automatic search algorithms and decreasing important identifying characteristic detail when applying the spectrographic method. The error rate chart in Figure 9 is coming from Grigoras 2009 [16]. This chart shows that the lower the signal to noise ratio of evidence recordings the higher the false alarm probability will be when applying automatic algorithms for ENF extraction. When visual matches are made, such as the spectrographic method, there are no reported error rates, however the identifying particularities of the signal are diminished.

Figure 9 is a chart used for evidence digital audio recordings; by measuring the SNR of the nominal ENF frequency against the recording's noise floor, the chart in Figure 9 can be used to determine the false alarm probability when applying automatic search algorithms to evidence. Basically, the closer the signal of interest is to the noise floor the more likely one will be to obtain a false result. Even though the forensic examiner has no control over the conditions in which the evidence was created, the chart in Figure 9 can be helpful in assessing the best approach to conducting an ENF analysis.

The SNR of the forensic ENF database however, can be maximized by using high quality components and circuits that introduce less noise and less THD as well as using a variable resistor in place of the ENF probe schematic R3, this way the optimal signal can be calibrated for the system it is being used in.

Higher sampling rates such as 8 kHz can help in creating better resolution and be beneficial when applying filters in post-processing.

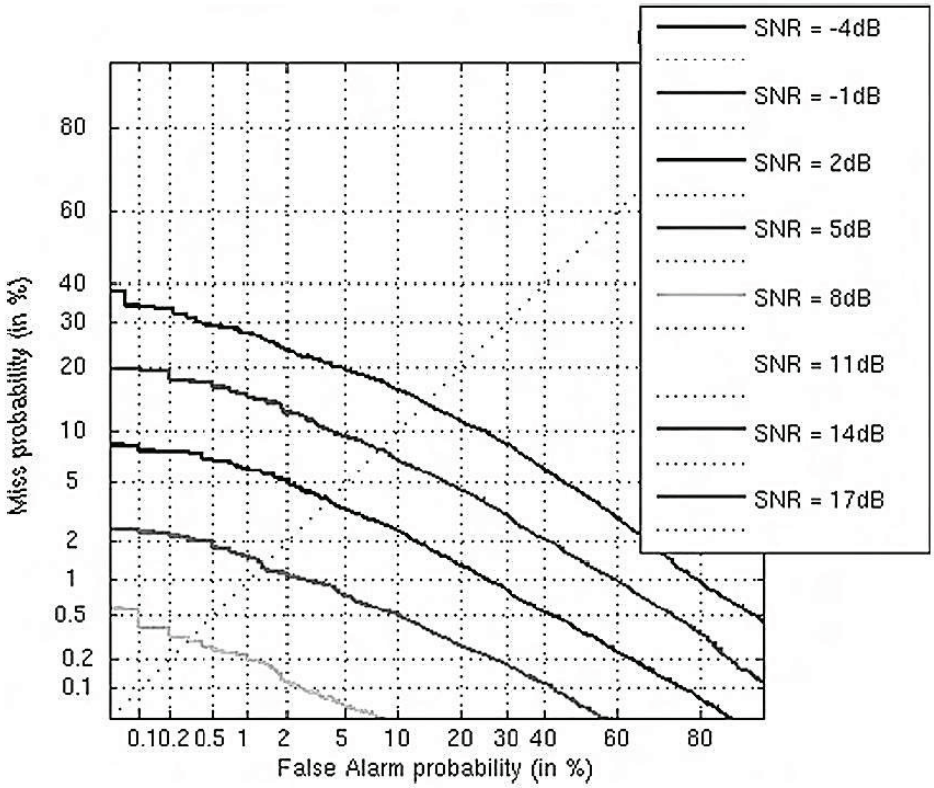


**Figure 9** Evidence Signal to Noise False Alarm Probability

### 3.5 Type of storage (HDD vs. SSD)

The information gathered for the forensic ENF database must be stored for later reference. Storage media such as Hard Disk Drives (HDD) or Solid State Drives (SSD) are examples of popular storage media. When building a forensic ENF database the decision to use HDD or SSD will need to be made. The drives can be configured in a variety of ways for example, a Redundant Array of Independent Disks (RAID) can be utilized to stripe ENF data files across two disks, the Operating System (OS) can be installed on one drive while another drive is reserved for reading and writing only, or SSD can be used and the combination of possibilities is almost endless. There are advantages and disadvantages to any type of storage configuration. To investigate some of these configurations a series of tests was conducted using different storage configurations.

A forensic ENF database will continually write files to drives 24-hours a day, 7-days a week 365-days a year and when it comes time to move files to an external back-up drive, the system is tasked with reading and writing simultaneously. If the HDD RPM is too slow then errors can occur in the database files that look similar to files that have been edited. This problem has the potential to cause serious doubts in the integrity of the database, especially when being presented to a judge or jury. HDD's spinning at 7,200 RPM have been tested and determined to spin too slow for a forensic ENF database. An experiment was conducted by simultaneously reading and writing ENF database files to a HDD spinning at 7,200 RPM. Next, the file was processed in the same manner database files are processed for the spectrographic extraction method (down-sample to 144 Hz & band-pass filter around 60 Hz). Write-errors were found that had been introduced into the file that looked similar to a file that deletions had been made on.

Figure 10 illustrates an ENF database file that has been processed for the spectrographic extraction method (down-sample 144 Hz & BPF around 60 Hz). While this ENF database file was being written, other database files were copied from the same HDD to an external HDD. The two broadband spikes correspond to the times when the files copied, thus interrupting the write process and introducing error into this file. These broadband spikes can also be found in audio files that have had sections deleted from them.

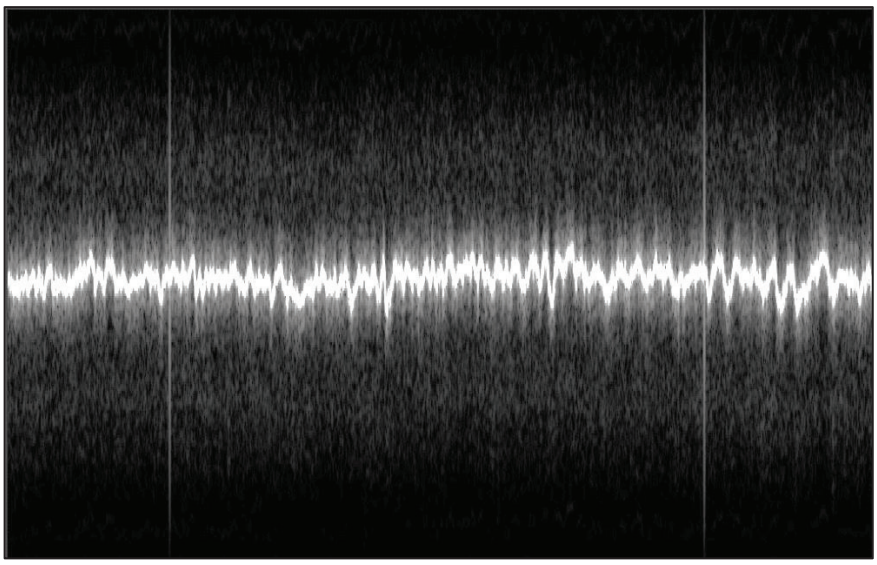

**Figure 10** ENF Database HDD Write-Error (7,200 RPM)

Figure 11 displays the spectrographic extraction of an ENF database file (down-sample 144 Hz & BPF around 60 Hz). Four deletions were made in this file which can be seen as broadband spikes throughout the recording. These deletions look similar to the errors introduced by slow disk speed write errors. The examiner would have a difficult time explaining to the jury why indications of a deletion were found in an evidence file when the database used for comparison exhibits the same particularities.

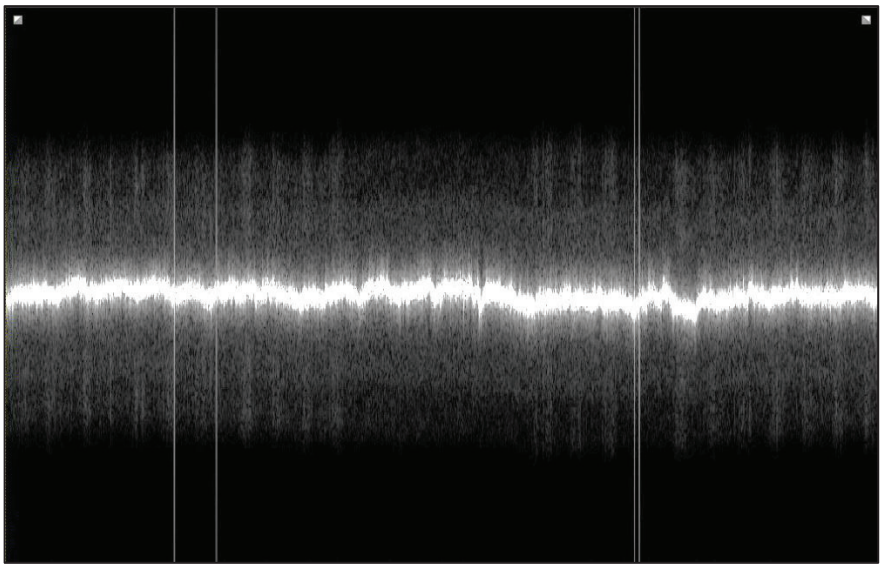

**Figure 11** ENF Evidence Deletions

These types of write errors do not occur every time files are moved from the disk that is reading and writing simultaneously. An experiment conducted at TFSL has revealed that write errors can be generated from a variety of sources such as Windows updates, machine maintenance processes, and random generation. The experiment carried out at TFSL involved the use of two independent acquisition computers. PC1 was configured with a Western Digital 7,200 RPM HDD that contained the OS as well as the storage space for the ENF files. PC2 was configured with a Western Digital 7,200 RPM HDD that contained the OS as well as storage space for ENF database files, in addition, PC2 was configured with a second Western Digital HDD that rotated at 10,000 RPM. The 10k RPM HDD in PC2 was used for ENF database file storage only and there was no OS on the 10k HDD. Next, one instance of RecAll Pro was configured on PC1 to record .WAV PCM 8 kHz files and save them to the only local drive in the computer.

On PC2 two instances of RecAll Pro were configured to record .WAV PCM 8 kHz files and save the output of the first instance to the 7.2k RPM HDD and save the output of the second instance to the 10k RPM drive. The systems were allowed to run over night. The next morning, while the files were still being written on both PC1 and PC2, files were moved back and forth from the 10k RPM HDD in PC2 to the 7.2k RPM HDD in PC2 every 15 minutes for 1 hour and 15 minutes for a total of 5 file transfers. When the file transfers were finished the systems were allowed to record for an additional 15 minutes. The recordings were stopped and then analyzed to see if 10k RPM HDD rotates fast enough to avoid write errors. The results of this experiment were not exactly the anticipated results. PC1 7.2k RPM HDD encountered zero write errors for the 19 hour duration that it recorded. PC2 10k RPM HDD encountered four write errors. PC2 7.2k RPM HDD encountered four write errors. Every write error on PC2 7.2k RPM HDD occurred at precisely the same moment as the write errors on PC2 10k RPM HDD. None of these write errors occurred during the file transfer time.

These results indicate that 10k RPM HDD's are susceptible to write errors, write errors do not always occur when files are being transferred, and the electric network was not the cause of these simultaneous errors. The files being transferred back and forth between PC2 HDD's were roughly 800MB in size. All of the log files were inspected on PC2 in order to determine if there was an update or some automatic system maintenance that caused the simultaneous write errors, no events were logged within less than 5 minutes from a write error. (see Figure 13). One would expect that a single ENF probe providing a single sound-card the signal would produce the same waveform on two drives being written to simultaneously because the A/D converter only has one output. If the waveform in Figure 13 is examined closely it can be seen that the waveforms are not identical, even though the input of the PC2 HDD's should have been receiving the same bit words from the A/D converter. Figure 13 is a close up view of one of the write errors that occurred simultaneously on two separate HDD's.

One advantage of the HDD is that they yield a lot of storage capacity for a small price. One disadvantage of the HDD is that they have several moving parts and the disks rotate at various speeds such as 7,200 RPM or 10,000 RPM. If a HDD is used in the database then it is highly likely that errors such as the write errors will be introduced. This is the reason that SSD are recommended over HDD. In another experiment a SSD was used to simultaneously write an ENF file and copy other ENF files from the same SDD three times during the recording. After processing the file that was written to the SDD, no traces of

write errors were found. Other storage media configurations were experimented with during the configuration of the TFSL ENF database, please refer to appendix B.

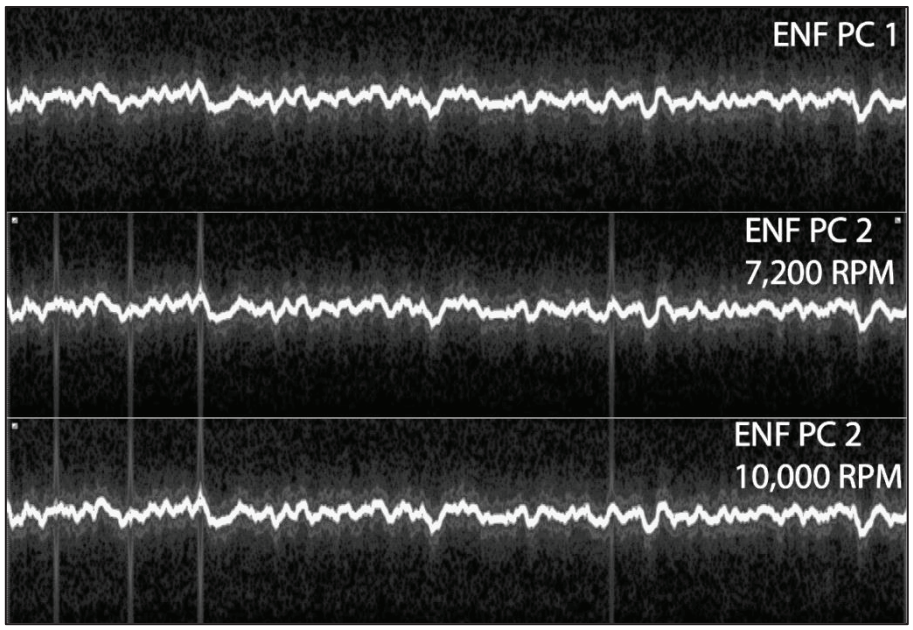


**Figure 12** Comparisons of Three ENF Files

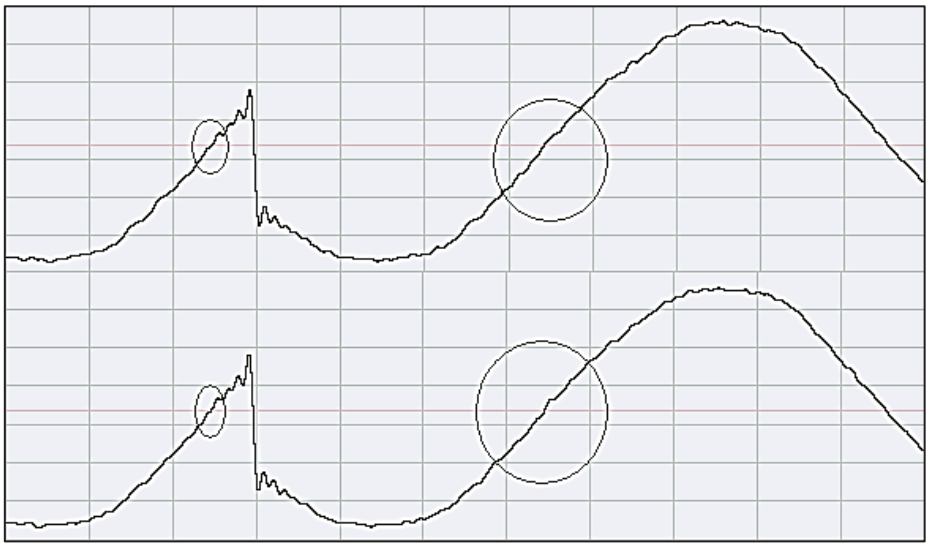

**Figure 13** Differences in two files from the same A/D output

### 3.6 Direct Current (DC) Bias and Frequency Bias

DC bias can be a product of the original analog signal, imperfections in the A/D conversion process, or a number of other sources. In a digital system DC bias can be the result of poor quality/design of components in the A/D converter and if DC bias is introduced, the waveform (X-axis = time, Y-axis = amplitude/voltage) average value will not be zero. DC bias is seen in the frequency domain as a finite value at zero Hz. For example, if there is a DC bias present in the signal, the amplitude of the waveform will not be centered on zero, when the signal is averaged the result will be something other than zero. ENF processing involves non-real time processing thus the simplest way to compensate for DC bias is to compute the average of all the samples then subtract this average from each sample [1], [4], [8], [16], [61]. Detecting DC bias can be simple because the peak values of the waveform should be as equally distant from the center line as the valley values.

Frequency bias on the other hand, can be a product of an offset or bias in the frequency of the recording device clock. If there is an error in the recording device clock and frequency bias is introduced, the nominal ENF frequency will appear at some other frequency. For example, if a recording device clock is incorrectly counting seconds then the sampling frequency will not be sampling at the apparent setting; if the $fs$ = 8 kHz but the recording device clock is taking 1.1 seconds to sample 8,000 times then a 60 Hz signal will have additional cycles per second causing the 60 Hz signal to appear higher than it actually is. If frequency bias is present in a signal then subtracting the nominal value from the waveform (X-axis = time, Y-axis = frequency) will result in a value other than 0 Hz.

DC bias and frequency bias are particularities of the recording device and the examiner has no control over the method used to create the evidence. The examiner does, however, have control over the methods and precautions used in the laboratory. Being aware of DC bias and frequency bias and the affects they can have on ENF is an important consideration when implementing the ENF criterion as well as when maintaining a forensic ENF database. DC bias is an offset of an amplitude/voltage vs. time waveform average from zero. Frequency bias is an offset of a frequency vs. time waveform away from its nominal value.

DC bias and frequency bias can both affect the zero-crossings of a signal. If the DC bias is not mitigated properly the zero-crossings of the signal will be too close to the bottom or top of the wave form depending on weather the DC bias is positive or negative. This will become a difficult challenge when

attempting to apply automatic database searches based on zero-crossings because the length of semi-periods will be too short, then too long, then too short, and so on every time the signal crosses zero. The frequency bias can affect zero-crossings because the signal will have lower or higher frequency than the nominal ENF, causing the cycles to be elongated or shortened. DC bias should be removed from evidence recordings by computing the mean of all the samples and then subtracting this average from each sample. Frequency bias should be removed from evidence recordings by computing the mean of the time and frequency vectors and then subtracting the means from them. DC bias should be removed from database recordings, and typically will be removed through the post-processing. If frequency bias is not dealt with properly then the results of an ENF analysis can be incorrect. For an example please refer to section 2.3 Conflicting Theories about the ENF Criterion.

### 3.7 Distortions

In digital audio, a distortion is any change in the content of a signal or a change in the shape of the signal waveform during its transmission. Distortions can come from a variety of sources and have a variety of effects on the recording. Some distortions come from hardware such as write errors in a HDD, a malfunctioning low-pass filter, or a bad word-clock. Other distortions come from signals for example, poorly planned gain stages, low quality ENF probe circuits, or low signal to noise ratio. A complete and exhaustive list of distortions will not be covered here but only the most common and easily overlooked distortions. Any of the distortions mentioned here are simple to test for and simple to correct. When establishing a forensic ENF database, attention should be paid to these types of distortions and steps should be taken to mitigate these errors before they occur.

Digital aliasing occurs when the system tries to reproduce frequencies that are above half the Nyquist frequency (*fs*/2). There are simply not enough samples per second to reproduce the number of cycles per second in frequencies above *fs*/2 since each cycle needs at least two samples per period to be reproduced. Aliasing is a type of distortion and an important consideration when determining sampling frequency for an ENF database. In an ENF database there are two ways that audio can be sampled; hardware or software. Both methods follow the same logic: Signal is received, signal is low-pass filtered to respect the Nyquist Frequency, signal is sampled. If there is a problem with the initial low-pass filter then frequencies above *fs*/2 will enter the sampler and start to introduce a variety of errors. Figure 14 illustrates a 60 Hz sine wave sampled at 8

kHz. Figure 15 illustrates what aliasing can do to a signal, in this case a 60 Hz sine wave sampled at 110 Hz, showing how the distortions can affect a signal. Another consideration about aliasing is the effect of "fold-over" where frequencies beyond the Nyquist frequency begin to fold-over into the audio bandwidth. This fold-over effect is caused by improper sampling rates, dysfunctional LPF's, or other sources and has detrimental effects on the quality of the recorded audio. The problem with fold- over is that the aliasing distortions being introduced are indistinguishable from real frequencies by the recording system. For example, if the sampling rate is 8 kHz and a signal of 6 kHz is introduced then there will be a fold-over of 2 kHz where 8 kHz = *fs* (Sampling Frequency), 6 kHz = F (Frequency > *fs*/2), and 2 kHz = F*f* (Aliasing Distortions).

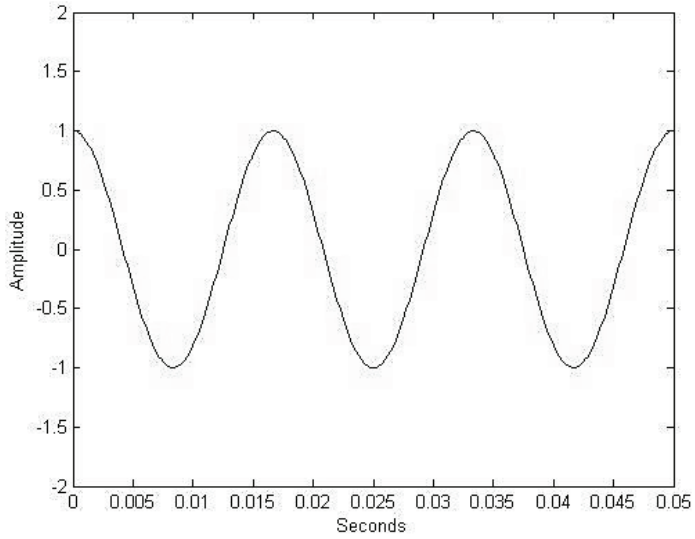


**Figure 14** 60 Hz Signal Sampled at 8 kHz

To demonstrate what can happen to the signal if the low-pass filter is not working correctly an experiment was conducted using a hand-held digital recorder, a laptop sound card, and the Sage Brush RecAll Pro recording software and illustrated aliasing errors and their effect on the audio spectrum when the Nyquist Frequency is not respected. To Begin, a sine-wave sweep was generated from 20 Hz – 20 kHz that repeated every 10 seconds from a laptop. Next, a Sony PCM D-50 was configured to sample at 22 kHz and the recorder was connected to the laptop. The anticipated results were that any signal above 11 kHz would start to show signs of fold over. To check the outcome a spectrogram was used

with 1024 - 256 FFT resolution (respectively) and the results were observed in both linear and logarithmic scales.

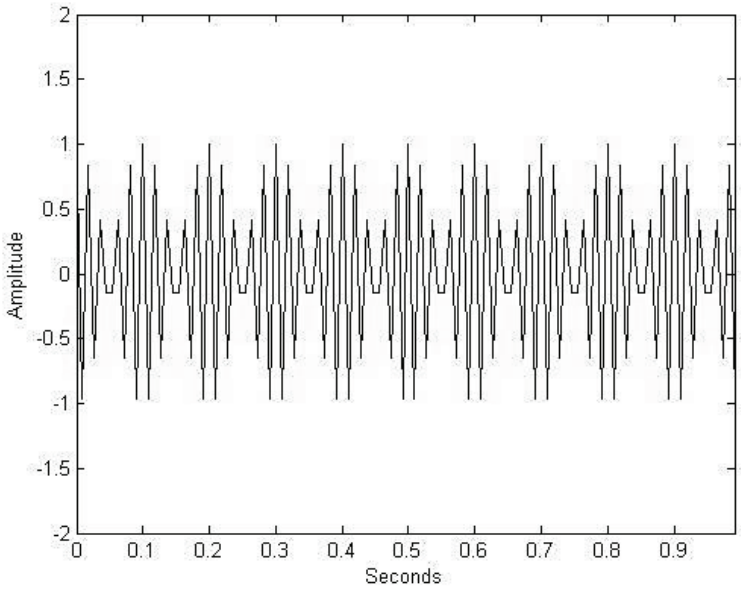


**Figure 15** 60 Hz Signal Sampled at 110 Hz

$$fs - \mathrm{F} = \mathrm{F}f$$

[2]

The linear spectrogram in Figure 16 is the result of a sine-wave sweep from 20 Hz – 20 kHz that is not cyclical but repeating, rising from 20 Hz to 20 kHz and then starting over at 20 Hz. This is a magnified view of one sweep over the course of 10 seconds. The X-axis is about 10 seconds long, the Y-axis is about 11 kHz high, and light areas indicate high amplitude. The sine wave sweep was recorded at 22 kHz 16 bit .WAV PCM. In this linear view of the spectrogram (1024 FFT) it can be seen that the low-pass filter of the Sony PCM D50 is not functioning properly. If the low-pass filter were working correctly then there would not be any fold-over. The system is taking the frequencies above *fs*/2 and interpreting them as frequencies that are within the *fs*/2 bandwidth by applying the 22 kHz sampling frequency to frequencies that are cycling faster than 11 kHz per second. For each frequency above *fs*/2 the system interprets that as a frequency proportional to the difference between cycles per second and *fs*/2. For example, 12 kHz in this instance is 1 kHz above *fs*/2 and is interpreted as a

frequency 1 kHz below *fs*/2 and is introduced back into the bandwidth becoming indistinguishable from the original 10 kHz frequency. The light areas to the left of the strong signal are the harmonics and rise at steeper angles because there are more frequencies between higher tones than there are between lower tones. For example, there are 1,000 Hz between 1 kHz and 2 kHz and there are 100 Hz between 100 Hz and 200 Hz; even though 1 kHz – 2 kHz and 100 Hz – 200 Hz are both octave ranges.

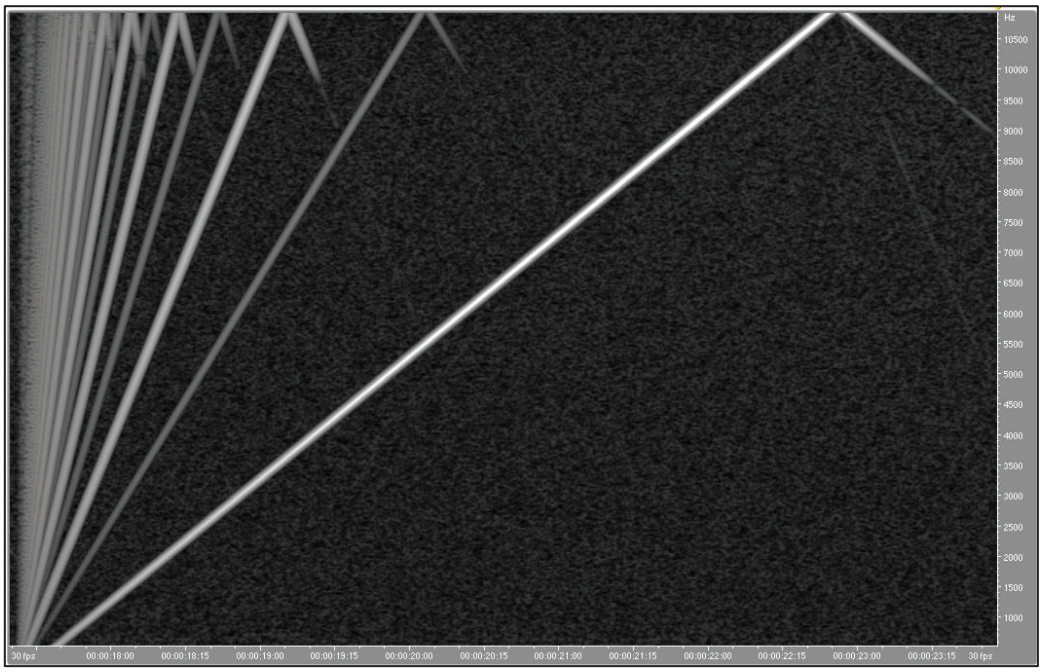


**Figure 16** Sony PCM-D50 Sampled at 22 kHz

In Figure 17 the same 20 Hz – 20 kHz sine wave sweep was used, the difference is that the sweep was sent through a laptop sound card and recorded with RecAll Pro. The sampling frequency and length of time are the same as Figure 16. The FFT resolution is the same as Figure 16 (1024) and this is also a linear scale.

However, in Figure 17 the aliasing frequencies being folded over back into the audio bandwidth are more apparent, having higher amplitudes, thus causing further distortions of the original signal. There is also more background noise in this recording, seen here as a light haze at the bottom of the spectrogram. This background noise could be introduced by a noisy soundcard, transmission

noise picked up along the signal path, or other sources. Even with the background noise taken into account, the increase in aliasing distortions is being caused by an inferior quality soundcard that is not applying a good low-pass filter to the signal entering the sampler. The same effect of the harmonics to the left of the strong signal can be seen in this example, as well as new generations of aliasing distortions. Because of the increase in amplitude of these distortions it can be said that an un-quantified amount of error will be introduced into the ENF database inversely proportional to the quality of the low-pass filter. In other words, the lower the quality of the low-pass filter, the higher the amount of distortions and error being introduced to the database. Likewise, the higher the quality of the low-pass filter the lower the amount of distortions and error are introduced to the database.

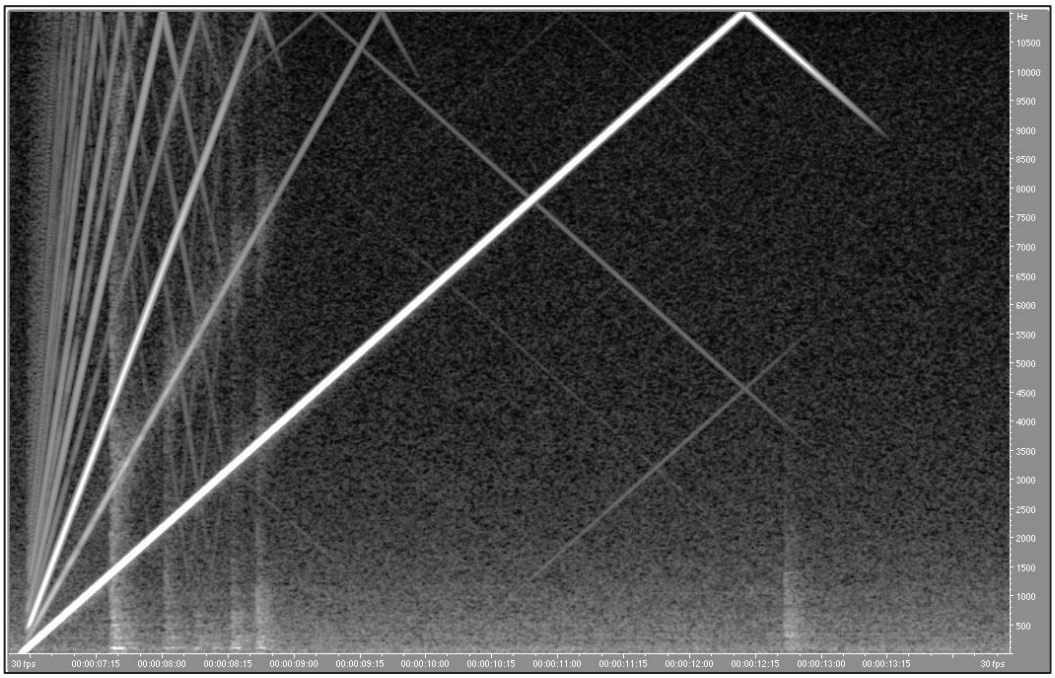


**Figure 17** RecAll Pro Sampled at 22 kHz

In Figure 18, the same 20 Hz – 20 kHz signal sweep was sent through the laptop sound card and recorded using RecAll Pro. The sampling frequency has been changed to 8 kHz and the FFT resolution has been changed to 256 to compensate for the lower sampling rate. The scale in this spectrogram is also linear and the X-axis runs for about 10 seconds and the Y-axis is about 4 kHz high. The biggest consideration to take into account with Figure 19 is that the

signal being sent into the sampler contains much higher frequency content than the sampling frequency, in fact the sine-wave sweep signal produces frequencies 2.5 times higher than the sampling rate which means that the effects of aliasing will be four-fold, literally. The fold over of frequencies ranging from 4 kHz – 8 kHz is seen in the aliasing distortions that range from 4 kHz – 0 Hz in the audio bandwidth. For the frequencies that range from 8 kHz – 12 kHz, the aliasing distortions fold over again and range from 0 Hz – 4 kHz. For the range of frequencies between 12 kHz – 16 kHz, the aliasing distortions fold over a third time and range from 4 kHz-0 Hz. Lastly, the frequencies ranging from 16 kHz – 20 kHz are folded over a fourth time and range from 0 Hz – 4 kHz. This is the reason that the "zigzag" pattern starts to appear in this spectrogram with a linear scale. To make things even worse, there are all the harmonics to the left of the strong signal that further compound this error and add an increasing amount of distortion to the database. This is a specific reason not to rely on the recording software to low-pass filter signals unless the software is tested and known to resolve this issue.

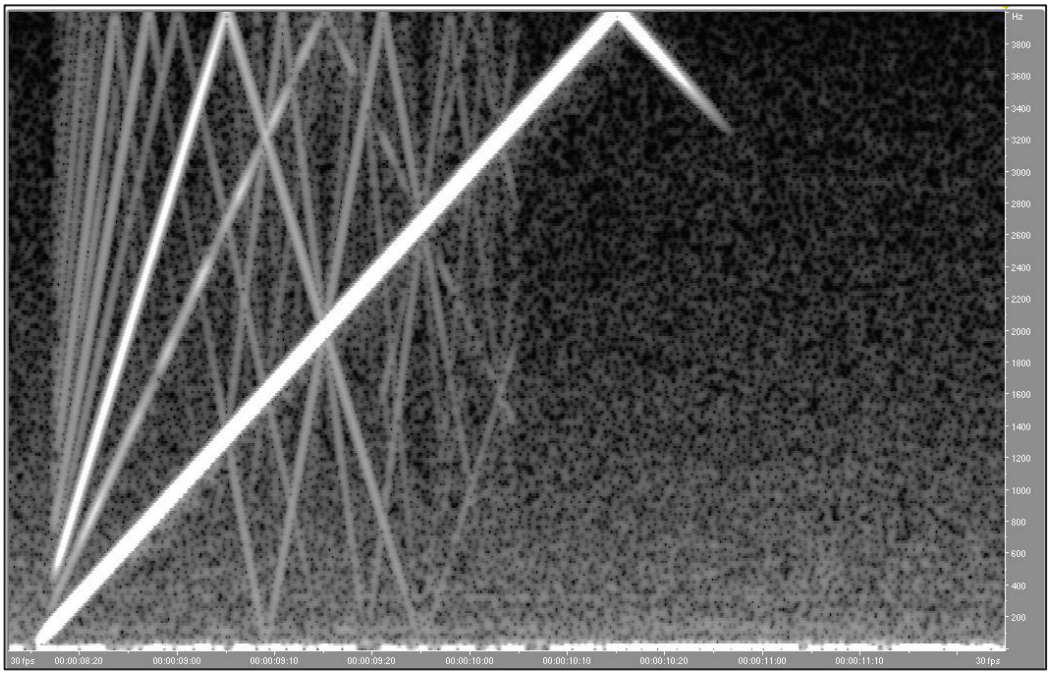


**Figure 18** RecAll Pro Sampled at 8 kHz

For implementing an aliasing free database it is recommended to verify that the sound card and/or software are applying a suitable low-pass filter. If

aliasing occurs, the distortions will introduce an un-quantified amount of error into the results. The aliasing distortions will introduce frequencies that are indistinguishable from the original signal making it impossible to determine the correct 60 Hz (UCTE 50 Hz). For forensic best practices aliasing distortions should be avoided.

There are other types of distortions to be mindful of, such as distortions introduced by the components of the ENF probe. The ENF probe components in section 3.1 were selected after conducting a series of tests at the NCMF of different component values and looking at the graphical results to determine which components caused the signal to be too low in amplitude, in a good range of amplitude, and too high in amplitude. The components that caused the signal to be too high in amplitude were avoided because signals that are too high in amplitude can cause the signal to be clipped. Another solution is to use a variable resistor in place of R3, this way the probe can be calibrated to best suit the system it is being used in. Changing the values of the diodes can allow more or less voltage to pass, but for the configuration at the NCMF the best components for the NCMF system were presented in section 3.1 and in the AES 131st Convention Paper [22].

Clipping occurs when components are overdriven by voltage and the resulting waveform is flattened at the peaks and valleys. This type of distortion for an ENF database is unacceptable and should be avoided by using a well-designed ENF probe built with high quality components. The anti-parallel diodes in the modern ENF probe allow 1.4V to pass, +.7V and -.7V. Any voltage beyond that will result in a clipped waveform, in respect to section 3.1. In Figure 19, the resulting waveforms of various component combinations are illustrated. The Darkest line represents a clipped waveform coming from components that were over-driven and had content clipped by the anti-parallel diodes. The information that is clipped cannot be readily recovered. This is a problem for a forensic ENF database because this type of distortion affects several parameters in the ENF extraction process such as harmonics, spectrographic analysis, and automatic searching. Most importantly the zero-crossings cannot be estimated if the peaks and valleys are clipped. To help determine the most suitable circuit for a clean waveform Table 1 was created with different valued component combinations. The values in Table 1 correspond to the graph in Figure 2 and Figure 19. Referencing the schematic presented in Figure 3, the values for R3 and the sound card impedance were changed. Combination number 9 had the highest clipping and is represented in the Figure 19 as the dark sine-wave. A distortion free output waveform with strong amplitude is represented as the dark

sine-wave in Figure 2. For implementing a forensic ENF database that is free from clipping distortions the NCMF configured the ENF probe circuit in the following way: The transformer steps the US 120 VAC (UCTE 240 VAC) down to 6 VAC and R1 & R2 = 1.5 kΩ, R3 = 200 Ω, D1, D2, D3, & D4 = 1N5863. An LED was also placed in the circuit so that when the ENF probe is functioning properly the LED will be lit.

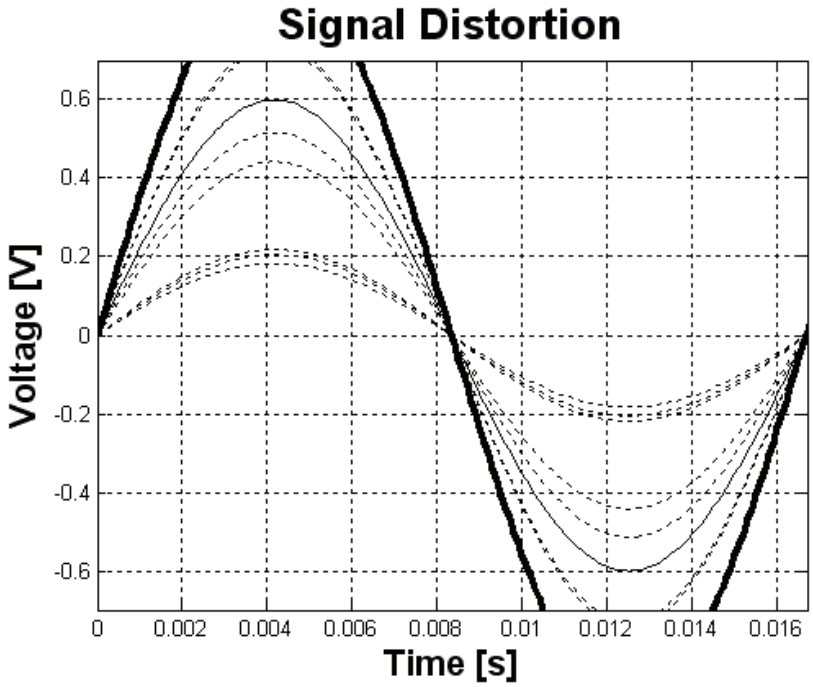


**Figure 19** Distorted Signal

Another type of distortion to be mindful of is called jitter. Jitter occurs when the system word-clock is not synchronized properly, resulting in erroneous zero-crossings. The system determines the bit value based on signal and if noise is being introduced that is close in amplitude to the signal then the system may assign a "0" for a bit when it actually should have been a "1" or vice versa. This sort of error will cause the signal to have zero-crossings that do not actually align with the original voltage. There are two common ways to check the word-clock: Peak to Peak and RMS. In the peak to peak method the distance between consecutive peaks of a sinusoid are measured against a pure sinusoid to determine if the word-clock is accurate. In the upper waveform of Figure 20 is the 60 Hz signal coming from an ENF database file. In the lower waveform is a 60 Hz sine wave generated from a tone generator. By measuring the peak to peak

in the pure-tone, jitter can be determined. The peaks of the pure tone should be spaced equally; if the peaks are not spaced equally then the word-clock is either advancing or delaying the signal, which in turn will start to affect the zero-crossings. In the ENF database file, it should be expected that the peaks will not be spaced evenly even if jitter is absent because ENF is a variation around 60 Hz (UCTE 50 Hz) and is not a pure-tone. However, if the word-clock accuracy and performance can be determined to be satisfactory with a pure-tone then the ENF signal will also be represented accurately. To verify that the pure tone is being accurately captured: 1 second can be divided by 60 Hz (1/60 = 0.016). By measuring the distance from peak to peak in the pure-tone and comparing that distance to the time line, the distance from one peak to the next or one cycle is 0.016 seconds. This process is repeated thousands of times on several seconds or minutes of audio.

For a forensic ENF database to be implemented properly, jitter should be taken into consideration and measured. Tolerances for jitter can vary, but 10 Hz in 1 second or a standard deviation of 1,000 waveform cycles is considered low jitter by the International Telecommunication Union series G document: *Transmission Systems and Media* ITU-T G.810 classifications from August 1996 [62], which might be good enough to keep from dropping packets of data but forensic ENF databases may require tighter controls.

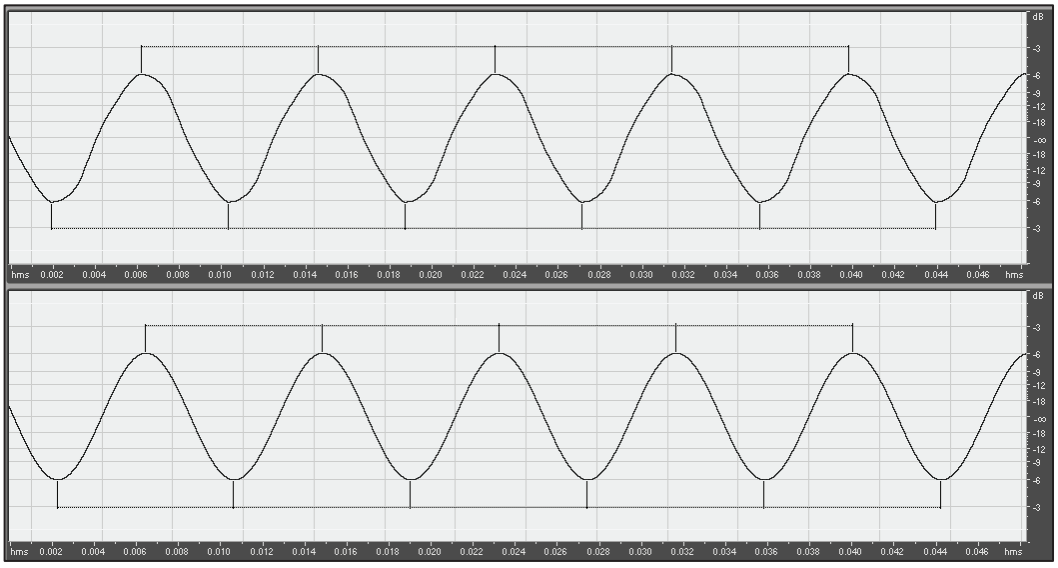

**Figure 20** Peak to Peak Jitter Measurements

In the Root Mean Square (RMS) method the jitter can be obtained by calculating the square root of the mean of the squares of the magnitude values of a signal. With a sinusoidal signal the square of the magnitude at a given resolution can be calculated, the mean of the resulting values can be calculated, and then the square root of that mean can be obtained, resulting in the RMS of a signal. In plain English, the RMS is calculated by adding all the squares of the discrete values and then dividing that number by the number of samples and then taking the square root of that. A simple example would be:

$$RMS = \sqrt{\frac{(x_1)^2 + (x_2)^2 + (x_3)^2 + \cdots + (x_N)^2}{N}}$$

[3]

The RMS obtained from the system can be compared with the RMS of an ideal clock to see the jitter difference. When making a jitter assessment of the system having an oscilloscope, an ideal clock, and other specialized tools can be helpful, but expensive. To implement a forensic ENF database that has a tolerable amount of jitter, the system clock should be checked periodically to ensure that zero-crossings are not being affected to a degree that will return erroneous results.

**Table 1** Tested ENF Probe Component Values

| # | R3 | SC impedance | Vo (mV) |
|---|---|---|---|
| 1 black line | 200 Ohms | 100 Ohms | 130 |
| 2 black dash | 300 Ohms | 100 Ohms | 146 |
| 3 black dot | 400 Ohms | 100 Ohms | 155 |
| 4 black line | 200 Ohms | 1 kOhms | 315 |
| 5 black dash | 300 Ohms | 1 kOhms | 428 |
| 6 black dot | 400 Ohms | 1 kOhms | 520 |
| 7 black line | 200 Ohms | 10 kOhms | 368 |
| 8 black dash | 300 Ohms | 10 kOhms | 530 |
| 9 black dot | 400 Ohms | 10 kOhms | 681 |

### 3.8 Network failure/Uninterrupted Power Supply (UPS) and safe guards

Network failure is commonly known as a power outage, where an interruption has occurred between the produced power and the consumed power. Network failure can be caused by many factors such as a bad transformer, disproportional consumption versus production, or a problem at the production source. Network failures can affect small localized areas like a few city blocks or network failures can affect much larger areas like a large portion of the entire grid. On September 9, 2011 two nuclear reactors lost electricity affecting the entire South Western portion of the US Western grid, leaving 5 million people without power until the system could be restored to normal operation [63]. On March 11, 1999 the largest network failure in history occurred in São Paulo, Brazil and surrounding areas [64]. A lightning strike initiated the Brazilian network failure that eventually left an estimated 75 to 97 million people without power until the system could be restored to normal operation. The span and duration of network failure can vary widely based on a number of factors and the way the network is configured. There is some protection against small, localized power outages for a forensic ENF database as will be discussed here.

An Uninterruptable Power Supply (UPS) is a device that will keep equipment powered during short network failures. The UPS is basically a battery that holds a charge capable of powering computers or other devices for short periods of time typically between 15 minutes and an hour. The UPS will keep a forensic ENF database recording during the outage and when power is restored the database should start recording the signal automatically. If the network failure lasts longer than the UPS can maintain the equipment then the ENF database will need to be restarted manually.

Certain facilities may use back-up generators to supply the building with power until the network returns to normal operation. In this circumstance, if the network fails, the UPS would keep the database computer active until the generators took control. Once the generators take control of the power to the building the ENF database would start recording the signal from the generator which will serve little forensic use. The database will continue to record the signal from the generators until the network returns to normal operation and the generators give control back to the network. Depending on the backup generators configuration, the generators may keep control of the building's power for a duration of time after the grid is functional. Valuable ENF data would be lost at this point.

This is a situation where localized power outages can be detrimental to the database. Some simple solutions would be: have multiple redundant databases at strategic locations on the same grid so that localized network failures would not decimate the entire database information for that grid, like the Denver and Las Vegas ENF databases used to monitor the US Western grid ENF. As far as recording generator signal after the grid is back online, a simple solution would be to connect the ENF probe to a socket that is powered only from the grid and has no connection to the generator breakers.

To implement the UPS in a forensic ENF database, the primary and secondary database computers should have their own UPS and only the primary and secondary database computers should be connected to a UPS. The computer monitors, ENF probes, and any other peripheral equipment should not be connected to the UPS because unnecessary power will be drawn from the UPS, essentially shortening the life span of the battery power supply during electric network interruptions. The ENF probe should be connected directly to the wall socket and not connected to a power strip as some power strips may introduce power conditioning or power regulation to the signal. The ENF probe will automatically shut off when the network fails but the computer and the recording software will continue to record. When the network is restored to normal operation the ENF probe will automatically start sending the signal to the computer again and the database recording will continue. See appendix A for more information about ENF probes connected to voltage regulated circuits.

### 3.9 Advances in ENF database configuration

Since the time Dr. Grigoras established the first ENF database there have been advances in the configuration of the database to meet forensic best practices [11], [12], [13], [17], [20], [22], [23]. The advances used in the NCMF and TFSL forensic ENF databases are discussed here to establish a more robust forensic ENF database from the software used to the minimum requirements to fulfill the extraction needs. Using audio recording software (Sagebrush Record All) automated recording of the ENF probe output can be set up. Different options can be set such as timing for automated file saving, file type, and sampling frequency. Automated file saving can be useful for keeping the maintenance requirements of the database at a minimum and also to keep the file structure consistent, as it is presented in Figure 21 (the proposed Sagebrush Record All settings). Uncompressed .WAV PCM files are the format of choice to avoid compression in the ENF database files, as shown in Figure 22.

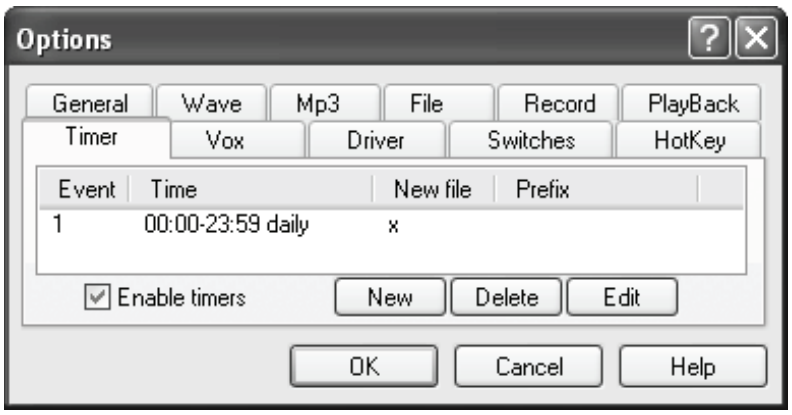


**Figure 21** RecAll Pro Timer Settings

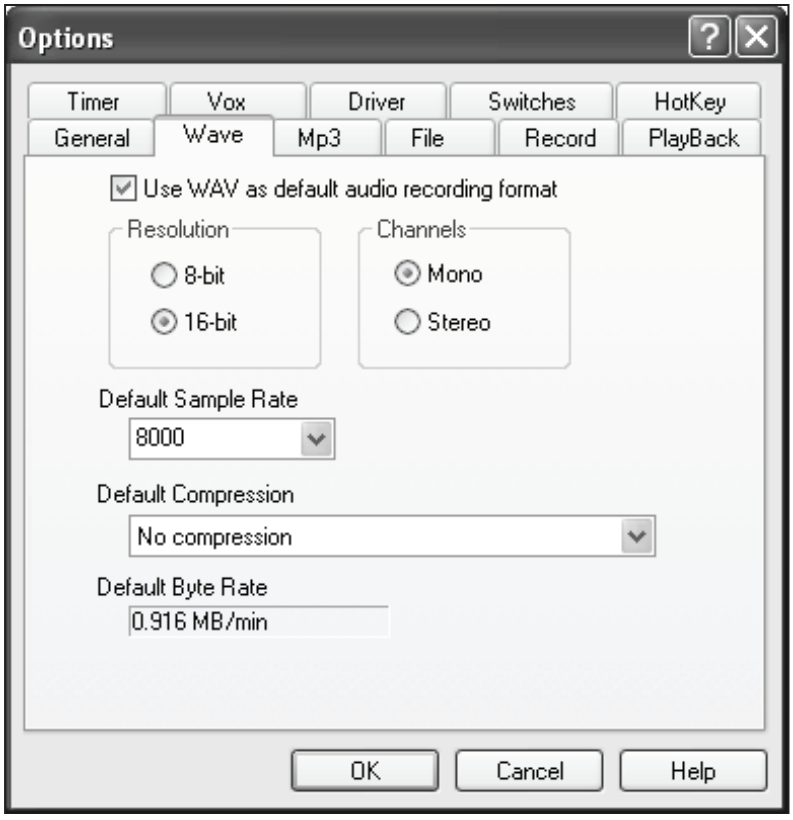


**Figure 22** RecAll Pro Audio File Settings

While various ENF database configurations and methods to extract ENF are presented by Grigoras [1], [4], [8], [16], [22]; Sanders [12]; Cooper [11], [13], [23]; and Micha£ek [17], using a high sampling frequency generates much more information per second about the recorded audio and creates a higher resolution database than sampling at twice the nominal frequency plus 20%, which will be helpful later when employing different methods of ENF comparison. Most importantly, it is necessary to acquire ENF signals at a higher sampling frequency for applying the zero-crossings method of frequency estimation where high resolution is critical [1], [4], [8], [16]. Sampling the ENF signal at 6 kHz – 8 kHz will require 1GB – 1.3GB storage per 24 hours which is a manageable amount of data, in addition, the stored file can always be down-sampled to any desired sampling frequency.

The minimum ENF database settings used at the NCMF and TFSL are: .WAV PCM uncompressed files, 6 kHz - 8 kHz sampling frequency, 16 bit, mono. Recording one 24-hour file per day with these settings results in ~1GB – 1.3GB of data per file. In order to extend the scientific research possibilities on ENF, including a cross verification of different methods to check evidence against an ENF database, a complex acquisition and analysis system is suggested and illustrated in Figure 23 and Figure 24 and described below.

It is recommended to employ two independent ENF acquisition systems and multiple levels of data backup. This redundancy is necessary for validating data and to accommodate for system updates, maintenance, and reconfiguration. As an additional precaution acquisition computers are powered by a UPS (see section 3.8). This will ensure that during a power outage the computers will continue recording. Even though the recorded signal during the power outage will be zero, when power returns, the computers will still be recording. The ENF probes are not connected to the UPS in order to collect unconditioned and unfiltered power. The recorded .WAV PCM audio files are saved to an external HDD for further digital signal processing including down-sampling of data and the calculation of zero-crossings and short-term FFT values. Processed ENF data such as down-sampled audio and frequency values from both ZCR and FFT calculations are considered sub ENF databases and should be stored remotely either through a network hard drive or at a separate physical location. This is detailed in FIGURE 25.

The primary and secondary database computers should have their time synchronized with both a radio clock and a GPS time receiver for each acquisition computer (see section 3.2.3). The radio clocks receive information on

the 60 kHz radio band in the United States and the GPS time receiver utilizes GPS common-view. Radio clocks and GPS time receivers will ensure that the time source is accurate to the NIST time reference. The ENF database computers should be behind a firewall if NIST NTP-1305 is used to synchronize the database time source, however, it is not recommended to connect the database to the outside world through internet connections because of the security risk. Since the ENF database computers are only used for acquiring ENF information they should not have unnecessary software installed on them for activities such as analysis. ENF analysis should be carried out on separate workstations from the databases.

The offset between the primary and secondary databases should be 12 hours; one database starts to record ENF at midnight, the second one at noon for example. This ensures that there will be no gap in data between recorded files and to protect against loss of data if it is necessary to shut either system down. Access to the database should be limited and only authorized personnel should be allowed to operate the database. In addition, the database should be kept behind a locked door to prevent any unauthorized tampering. All access to ENF acquisition systems shall be documented and when files are copied for analysis, SHA-1, SHA-256, SHA-512 or MD5 HASH values shall be computed for all ENF .WAV PCM files, which is stream-lined with ENF Database Manager software, see section 3.10.3.

When ENF databases are implemented as proposed, it is possible to further the research of ENF applications in forensics, compare and cross verify different ENF extraction algorithms as shown in Figure 25, and to combine them in forensic cases by using multiple methods to analyze evidence.

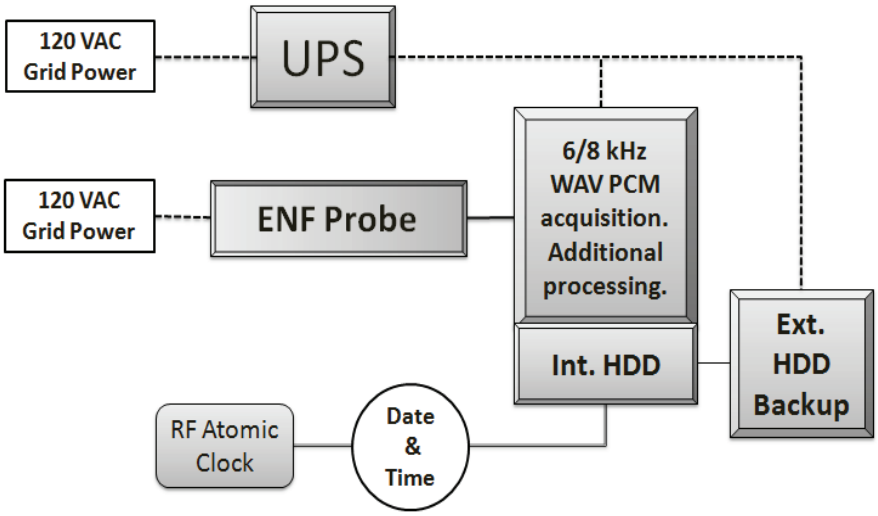


**Figure 23** ENF Database Acquisition System

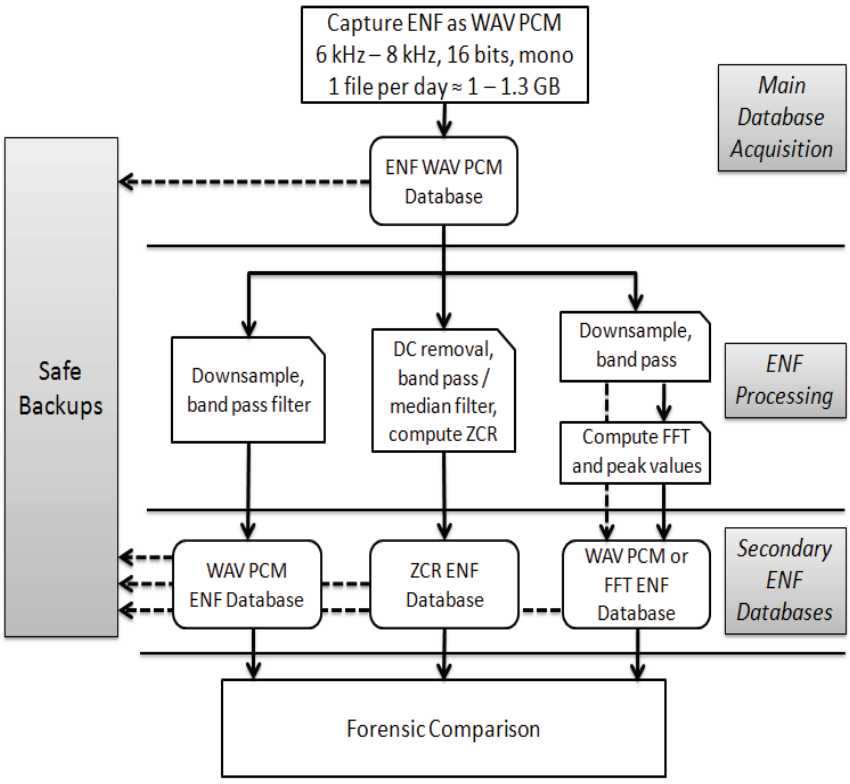


**Figure 24** Suggested ENF Database Structure

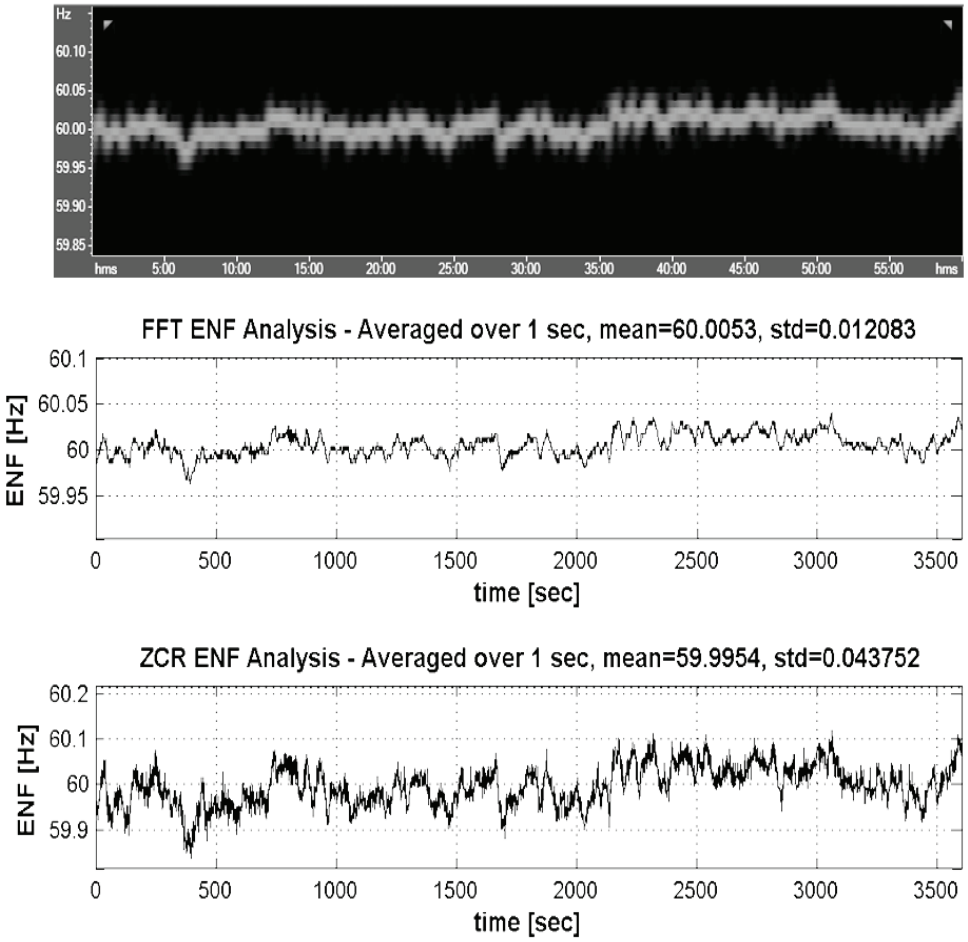


**Figure 25** Three ENF Extraction Methods

### 3.10 Other Areas to Pay Attention to

Given the number of variables in a forensic ENF database, the potential number of configurations is far greater than one thesis can outline. In addition, the advances in technology are so rapid that a proposal for a single ideal forensic ENF database configuration that will be immune to all sources of error is not feasible. The sections above have been detailed in a manner that will give general background of the subject and give general recommendations for configuring a forensic ENF database in a way that will help minimize the amount of error while simultaneously strengthening the forensic validity of the database. There are three other considerations that should be briefly mentioned so that the examiner can be aware of what the future might hold for ENF.

### 3.10.1 Proposed Changes to ENF Thresholds

In a June 25, 2011 article found at (http://www.dailymail.co.uk) details about proposed changes to the frequency thresholds of the United States electrical grid imply that clocks could lose time. The North American Electric Reliability Corporation (NERC) oversees the United States electrical grid and has proposed that the frequency thresholds be expanded to help make the grid more reliable [65]. The expansion of the thresholds would mean that plug-in clocks, like those on microwaves, alarm-clocks, or ovens, could run up to 20-minutes fast over the course of the next year in the US Eastern Grid. The grid-based clocks keep their time by counting cycles. If the thresholds are expanded then the number of cycles per second will increase and/or decrease causing the plug-in clocks to count more or less cycles per second and in turn cause the clocks to run fast or slow. For example, if the network frequency runs 5 mHz high (60.005 Hz) for 10 hours, a clock will speed up by 3 seconds [(60.005 – 60.000) / 60 * 10 * 3600 s/hr = 3s].

The implications of the proposed changes mean that the methods to monitor and extract ENF will need to be followed closely while these changes go into effect. The expansion of grid frequency thresholds means that the thresholds used in ENF extraction will also need to be expanded. Depending on what the thresholds are changed to and how far the signal is allowed to vary from 60 Hz, these changes could affect the way automated searches, spectrographic extraction, and zero-crossing methods are applied. See reference [16], [65], or the NERC website www.nerc.com for more information.

### 3.10.2 Neutral Interference at the Signal Source

Another important consideration to pay attention to is the stability of the power source used to power the ENF probe. As a colleague at the NCMF, Jack LeRoi, pointed out the neutral side of the socket should, in theory, be carrying zero volts. The positive side should be carrying the 120 volts (US grids). This ideal situation is not always the case however, if the neutral side is carrying some voltage it can cause unwanted affects in the signal, potentially altering important characteristics such as zero-crossings. Some of the sockets at the NCMF were measured and found to be carrying as much as 6 volts on the neutral side of the socket. By comparing the socket output on an oscilloscope, the severity of these distortions could be seen. There is a considerable amount of research going into this phenomenon and the impact it has on ENF, but for now the amount of error that is introduced to the signal has not been quantified.

### 3.10.3 ENF Database Manager

To help manage the files in a forensic ENF database the author developed a file management program using MathWorks MATLAB. This program is designed to help stream line the initial processing of ENF database files so that they can be easily organized into the sub databases (see Figure 25). The program is called "ENF Database Manager" and is designed so that the ENF file origination path can be selected and the ENF file destination path can be selected. There is also a section where text can be entered if the files should be appended. Next, MD5, SHA-256, and/or SHA-512 HASH values can be calculated for the original 6 kHz – 8 kHz file. Down-sampling can also be managed by selecting "keep original, 144 Hz, 360 Hz, or custom". Band pass filtering can also be managed by selecting "keep original, 60 Hz, 120 Hz, or custom". With this program the user can easily process ENF database files and organize them efficiently, presented in Figure 26.

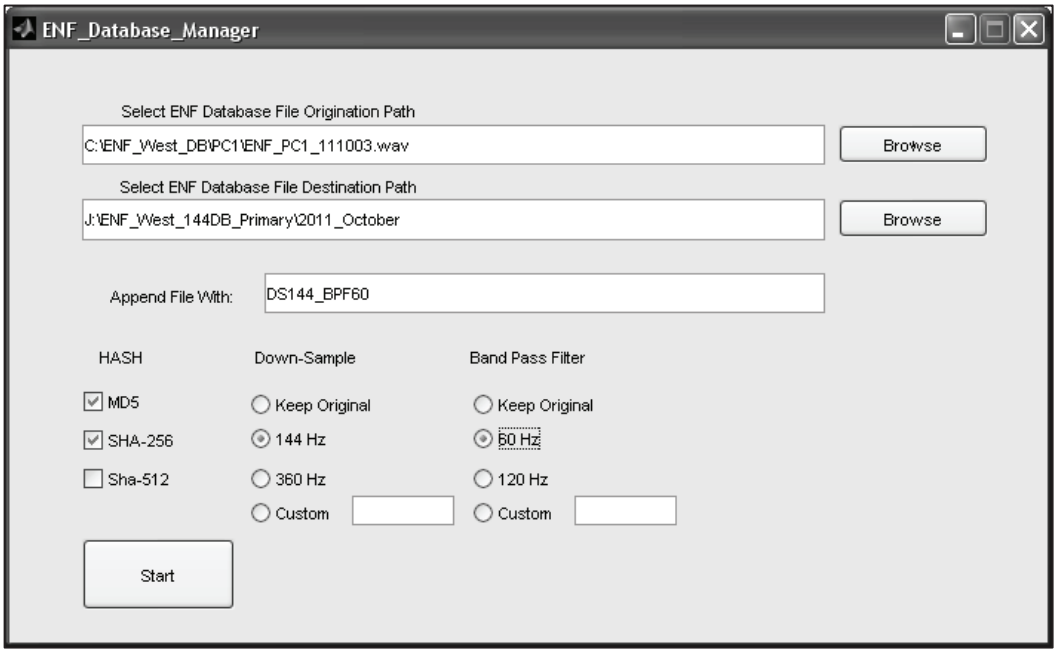


**Figure 26** ENF Database Manager

## 4. Proposal for Broadcast-Type Forensic ENF Databases

This chapter focuses on the possibility of broadcast ENF databases that can be used to capture ENF variations in one location and broadcast them to a remote location. The forensic need to design such a database configuration has developed over the course of the last decade with the increase in foreign conflict. Recently there has been an increase in the number of audio/video recordings being used to depict graphic scenes, communicate threats or other messages, and pass along sensitive information. Often times, such audio/video recordings will be made in places such as a cave or bunker and the recording equipment will be powered by generator. The recordings are often then brought to broadcast stations and possibly used to gain public attention or raise awareness of coming events. The ENF Criterion can produce valuable information from such recordings such as date and time of creation, areas of potential edits, mixed material, and geo-location. Armed with information such as this, law enforcement and military can proactively deploy valuable resources in a more efficient manner.

In a recent case, presented by Grigoras [16], a video tape broadcast was submitted to have the authenticity determined. Using the ENF Criterion it was possible to determine that there were three ENF traces in the recording. ENF1 was introduced during the digitization process, ENF2 was introduced by the broadcast company when the recording was broadcast, and ENF3 was introduced onto the original tape by a 220 V 50 Hz generator. Information such as this can be instrumental in narrowing down possibilities.

### 4.1 Scope of Broadcast-Type ENF Databases

Certain areas around the world that may be of interest for acquiring ENF information can have complex electric grid networks. Each network will have a unique ENF signature and such networks can cover small or large geographic areas. Some of these geographic areas can be places of violent opposition from local inhabitants or intense battle. Sending a forensic examiner with no combat training into these areas can be disastrous for innocent bystanders, soldiers, and the forensic examiners. On the other hand, sending a soldier with no forensic technical background into these areas can be disastrous for configuring a complex ENF database. This section offers a simple maintenance-free solution that will allow for electric network monitoring of any grid from a safe distance. This solution can provide the necessary ENF information with a one-time installation of a radio, Bluetooth, or Wi-Fi ENF probe into the grid of interest.

The installation of a broadcast ENF probe only requires that the device is plugged into any wall socket on the grid of interest. Once installed the broadcast ENF probe will transmit the ENF variations of that grid back to a safe base-station such as a military base where, once received, will be recorded onto a local acquisition computer the same way that the traditional database would.

### 4.2 Frequency-Modulation Databases

Radio has a long history dating back to the late 1800's and a collective group of contributors to its invention. There is debate about who the premier inventor of the radio is, some sources claim Guglielmo Macroni as the "father of radio" but there is evidence that he used several of Nikola Tesla's patents to broadcast the first transatlantic transmission. Today, commercial radio broadcasts can fall into several categories: Amplitude Modulation (AM radio), Frequency Modulation (FM radio), Digital Broadcast, Satellite Radio, and the list can be extended. AM radio utilizes changes in amplitude at a given frequency to drive the output signal, in other words when the source signal is in compression the amplitude increases and when the source signal is in rarefaction the amplitude decreases. FM radio utilizes a high carrier frequency that changes phase slightly over time to relay the differences in source signal, in other words when the source signal is in compression the carrier frequency is slightly faster and when the source signal is in rarefaction the carrier frequency is slightly slower. AM and FM radio are forms of analog modulation, satellite radio and digital broadcast are forms of digital modulation. Digital modulation is similar to the way NIST broadcasts from the WWVB radio station in Fort Collins, Colorado where signal strength is reduced by a certain amount at the beginning of every second to represent a certain binary value and then depending on the amount of time it takes for the signal strength to reach another threshold will signify another bit value (see section 3.2). There are several methods for digital broadcast encoding, the focus of this section is on analog type broadcasts and more specifically on FM radio because of the superior dynamic range and resilience to interference when compared to AM radio.

An experiment was conducted during the course of this thesis as a proof of concept to prove that an ENF database could be recorded remotely with no physical connection to the source providing the ENF. In configuration-1 of this experiment, a FM transmitter was built from the Ramsey Radio Kit (FM10) available at http://www.ramseyelectronics.com. This FM radio kit was equipped with RCA left and right inputs and a 9 volt power supply. To tune the radio a simple adjustment of the coil mechanism was done by connecting an mp3 player

to the FM transmitter and then listening to an open frequency on a car stereo, the coil mechanism was rotated until the signal from the mp3 player could be heard clearly. Next, an ENF probe was plugged into a wall socket and the ENF probe RCA outputs were connected to the FM transmitter RCA inputs. The FM transmitter was plugged into a wall socket to power the device. Using an Olympus WS-760M hand held digital recorder capable of receiving FM radio broadcast the signal from the transmitter was received and recorded on the other side of the building (about 30 feet). The duration of the first recording was about 1 hour and then the file was processed to investigate the applicability of using the spectrographic extraction method. The result was a strong ENF signal around 60 Hz that clearly showed the small unique variations that could be used in a forensic comparison. There was a substantial amount of background noise in the transmitted file, however, the concept proves to be possible if high quality components and a real transmitter are used. After doing some minor adjustments of the transmitter and changing the broadcast frequency, nine hours of ENF were broadcast and recorded onto the Olympus; this resulted in a SNR of 61 dB on the received transmission. The database recording had a SNR of 81 dB. In Figure 27 the lower spectrogram is roughly three hours of the broadcast signal received on the Olympus recorder down-sampled to 144 Hz and band-pass filtered around 60 Hz. The upper spectrogram is a database file from an ENF acquisition database (TFSL, Minneapolis), processed the same.

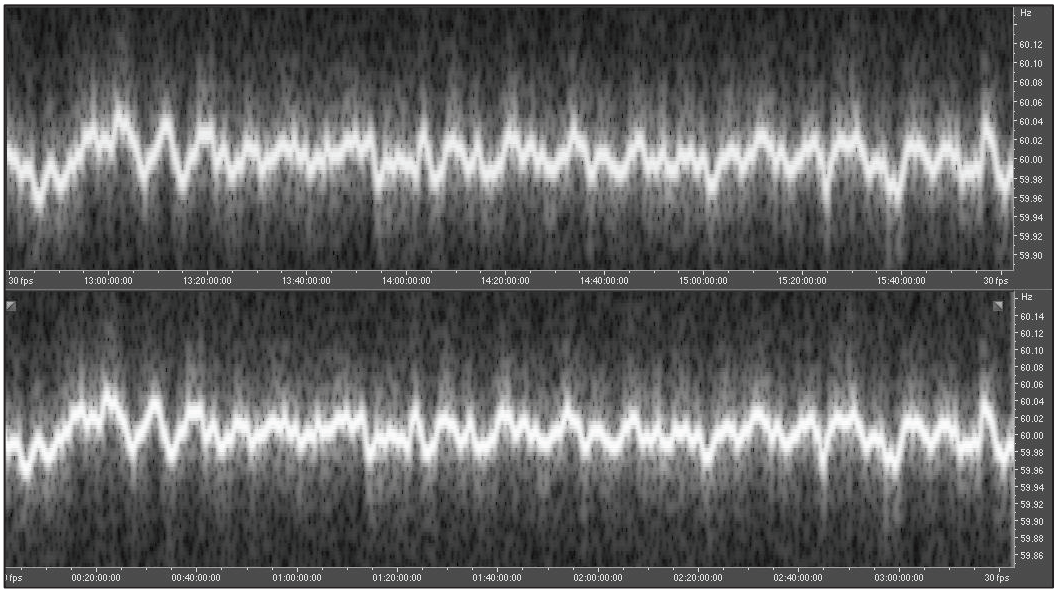


**Figure 27** FM Radio Broadcast

To ensure that the power supply was not introducing ENF into the transmission signal and that the received signal was in fact an ENF broadcast, other configurations were tested. By connecting the output of an mp3 player to the transmitter and broadcasting music that was then received by the Olympus recorder the test showed that the processed file contained no ENF. To further test the possibility of introducing ENF from the transmission, receiving, and recording equipment other tests were carried out at the NCMF that involved two more configurations of an FM receiver, a recording device, a car battery, a laptop, and a power inverter.

Configuration-2: Charge the car battery, connect the power inverter to the battery posts, and power the FM receiver, a Sony PCM D-50, and the laptop from the inverter. In this configuration none of the equipment was connected to the electric grid. The output from the FM receiver was sent to the input of the Sony and the output of the Sony was sent to the input of the laptop and then the signal was recorded using RecAll Pro. The FM receiver was tuned to the National Weather Service channel which broadcast 24-hours a day on 162.558 MHz. Only 5 days of ENF was recorded because the equipment would shut off when the battery charge was drained and then the battery would need to be charged and the system turned on again. However, the results indicated that the equipment was not in a strong electromagnetic field because there were no usable ENF traces in the recordings. From configuration-2 it could be said that the specific transmission and recording equipment, in that specific location, was not introducing ENF into the recordings.

Configuration-3: Connect the FM receiver to a wall socket, send the output to the input of a Sony PCM D-50 that was mains powered, send the output of the Sony to a laptop that was mains powered and record the signal using RecAll Pro. The FM receiver was tuned to the National Weather Service channel which broadcast 24-hours a day on 162.558 MHz. With this configuration, 7 days and 22 hours of ENF material was recorded. After examining these recordings it was determined that there were no usable ENF traces. This illustrates the point that the equipment used in this test was not in the presence of a strong electromagnetic field or susceptible to mains induced ENF bleed.

To determine if the Sony PCM D-50 was capable of capturing ENF, tests were made with the device in various areas such as next to a computer or other strong electromagnetic sources and then the recordings were examined and revealed that the Sony can capture ENF even when the device is battery powered only. From the various configurations above it can be said that ENF from

Configuration-1 was introduced by the broadcast probe and not by other means and that there is validity to a FM broadcast ENF database. With some minor adjustments and decent equipment a strong and clean broadcast signal can be obtained and the SNR can be increased beyond 61 dB. These devices can be small in dimension and have an ENF probe circuit installed. The electric network voltage can come from a wall socket and upon entering the device be split off into two branches, the first branch going to the transformer to power the transmitter itself and the second branch going to the transformer to step the voltage down to 6VAC for the ENF probe circuit. The output of the ENF probe circuit can be hard-wired to the input of the transmitter and when the transmitter is plugged in it will continuously transmit ENF.

There are some disadvantages to establishing an FM broadcast ENF database such as: transmission interruptions, loss of signal, radio jamming from sophisticated attacks, and the list can be extended. FM signals can be intercepted relatively easily, although if an ENF signal were to be intercepted the recipient would probably dismiss it as a communication channel with severe "ground noise". From a security perspective analog transmission cannot be encrypted but there are other precautions that can be used such as continuous frequency modulation techniques that constantly change the carrier frequency at variable speeds, making the signal difficult to follow for any extended period of time. But the potential for an ENF database to exist separately from its source, receiving information wirelessly, does exist and the concept has been proven using FM radio broadcast.

### 4.3 Blue-Tooth Databases

Blue-Tooth is a wireless communication technology that is mostly used in phones, cars, and medical devices to transfer information like audio, sensor data, and health statistics. Blue-Tooth is designed to operate on the 2.4 GHz radio band and consume a small amount of power which makes it useful for mobile and localized applications. Blue-Tooth can be implemented, with distance limitations, in an ENF probe and used to transfer information about the electric grid variations wirelessly to a remote location that is within roughly 10 meters, or in a scatter-net configuration, within roughly 10 meters of a "hop" point [35]. The simple explanation for Blue-Tooth is that information coming from the device is converted into 1's and 0's and this data stream is modulated to the 2.4 GHz radio signal and then broadcast. On the receiving end of the communication, the 2.4 GHz radio signal is de-modulated and the 1's and 0's are revealed in a remote location.

The world record for longest Blue-Tooth file transfer is about 1 kilometer, obtained by using sophisticated high-gain antennas [66]. With that being said, there are obvious distance limitations to the implementation of a Blue-Tooth ENF database. The remote location receiving the Blue-Tooth broadcast is typically required to be within 10 meters of the source which can be a disadvantage that perhaps FM or Wi-Fi could alleviate. The advantage to Blue-Tooth is that the technology is relatively more secure than FM or Wi-Fi. Blue-Tooth ENF probes could be useful for close range wireless ENF monitoring, but if the demands are long range, then FM is superior. If the application of a Blue-Tooth ENF probe is intended to be covert then this type of configuration could work well in not raising suspicion with wires running from a "black box" into a computer.

The reason that Blue-Tooth is more secure than FM or Wi-Fi is that Blue-Tooth is a frequency-hopping spread-spectrum (FHSS) technology. FHSS, as it is used with Blue-Tooth means that Blue-Tooth communications are constantly hopping frequency channels, making it difficult to follow a single communication stream and/or gain much information from one channel. Blue-Tooth is a radio technology that operates on the 2.4 GHz radio spectrum and is subject to FCC regulations. The FCC dictates that Blue-Tooth is allowed to operate on 79 channels in the 2.4 GHz range; in addition, Blue-Tooth communications have to be used in a pseudo-random manner across at least 75 of the 79 channels. A Blue-Tooth device must not occupy the same channel for more than 0.4 seconds in a 30 second window. The nominal bandwidth for each channel is 1 MHz and the maximum peak power output allowed is 1 Watt, hence the low power consumption but also the restricted transmission distance. Most Blue-Tooth devices hop pseudo-randomly across all 79 channels 1,600 times per second [35]. Encryption can also be applied to Blue-Tooth communications adding an extra security precaution that will randomize the data so that if it is intercepted it cannot be read. Encryption is a security precaution that FM transmission lacks because they are analog broadcasts.

If the demands for an ENF database are to supply information on a secure wireless transmission at short distances then Blue-Tooth provides a practical solution. An ENF probe can be configured with a Blue-Tooth transmitter in a small and inconspicuous device that requires only to be plugged into an outlet and then the device will need no maintenance.

### 4.4 Wi-Fi Databases

Wi-Fi (IEEE 802.11) wireless communications are also a possible solution for transmitting electric grid variations from one location to a remote ENF database. The average signal distance of traditional Wi-Fi is about double Blue-Tooth (~65 feet). Wi-Fi works in a similar manner to Blue-Tooth with regards to the fact that information is modulated so that it can be broadcast and then the radio signal is received and de-modulated, thus revealing the data stream in a remote location without the use of wires. Because Wi-Fi is a powerful wireless tool there is a lot of demand for the technology. But Wi-Fi has broadcast limitations just like any radio communication. For this reason there have been technological advances to increase the distance Wi-Fi can broadcast, with one potential use being to serve free Wi-Fi service to a geographic area the size of a city.

Wi-Fi broadcast distance can be increased by modifying the transmission power, the antenna, and line-of-sight locations. The increase in transmission power for example, will result in larger and more cumbersome devices. As technology advances there may be practical solutions in the near future that balance the need for small real-estate and long distance broadcast.

A Wi-Fi ENF probe could be configured to receive the electric grid variations from any wall socket and convert the values to binary 1's and 0's and then the data stream could be modulated and broadcast via Wi-Fi to a remote location. One work-around to the distance problem would be to broadcast the ENF from the probe to a near-by computer with internet connectivity. Once the signal is received into the near-by computer the ENF files can be sent via internet to any place in the world. Once received or downloaded from the internet the ENF data can be compiled in the database. Another solution would be to create an ENF probe that simply outputs the data stream via Ethernet cable to the internet.

Virginia Tech has completed some testing with wireless ENF [70] but Virginia Tech is interested in ENF for reasons other than forensics. Virginia Tech has developed devices called Frequency Disturbance Recorders (FDR) for monitoring electric grid frequency variations throughout North America. The information gathered from these FDR's is transmitted through the internet and then compiled in a database for later reference. The FDR units are like the NCMF ENF probe on steroids, FDR's have a built in Low Pass Filter (LPF), Analog to Digital (A/D) converter, GPS time receiver, micro-processor, and

network communication modules. The FDR units are strategically placed throughout North America and the data collected from the approximately 60 FDR units is used to study ENF variations 24-hours a day 365-days a year, paying particular attention to times when there are wide-scale frequency disturbances such as power outages or other social influences on the ENF variations such as Super Bowls [71]. The FDR units have the capability to sample ENF variations at 1,440 Hz locally; this provides enough information to create accurate graphical displays. Some lessons that can be taken from the FDR units is the utilization of the LPF built into an ENF probe potentially could reduce aliasing effects on the acquisition system. The built-in A/D converter could help with Wi-Fi broadcasting so that the probe will not have to depend on the Wi-Fi modulator, which may have inferior performance when compared to a dedicated A/D converter.

The Virginia Tech wireless experiment [70] involved lab tests and field tests. The engineers built a coil that would be sensitive to Electro Magnetic Fields (EMF) and recorded frequency variations near a high-voltage power-line. The engineers noted that the variations picked up by the coil in the field test were nearly identical to the variations recorded by another FDR at the same time in a different state. If anything, the engineers have further confirmed the ENF Criterion. Essentially what the engineers have done during this wireless experiment was to simulate what forensic researchers have done using hand-held digital recorders. The microphones in hand-held digital recorders act as capacitors in the presence of EMF variations. These variations are embedded into the digital audio recording and saved as part of the audio file. The difference between the Virginia Tech wireless experiment and this proposal for broadcast type ENF databases is that a wireless forensic ENF database will gather ENF variations in one location and broadcast them to a remote acquisition location; whereas the engineers were confirming that power grid frequencies could be captured wirelessly through the EMF in close proximity of high-voltage power-lines. The ability to broadcast ENF variation for forensic examination and scientific research could easily be offset if proper security precautions are not implemented as well as out fitting an ENF probe with advanced processing boards and network communication modules.

The security of Wi-Fi connections needs improvement; there are several free-ware programs that make unauthorized Wi-Fi access simple [67]. Even with Wi-Fi encryption, the free-ware programs simplify unauthorized Wi-Fi access; FBI agents were able to demonstrate at an Information Systems Security Association (ISSA) meeting how to crack a 128 bit WEP encryption in three

minutes [67]. In addition to the security risk involved with Wi-Fi, once the ENF files are transferred via internet there is an added security risk. Maintaining the integrity of ENF database files that are transmitted and transferred in such methods can be challenging. HASH algorithms can be employed at the file creation stage before transmission and this can help to verify the integrity of the files but this is not an "end-all" solution.

There is a potential to broadcast ENF information via FM radio, Blue-Tooth, Wi-Fi, and others. Each of these wireless systems is subject to security risks, plus the added risk of transferring files over the internet. There is much needed research in the area of ENF broadcasts because if the challenges can be solved and produce information that is suitable for forensic purposes then broadcast ENF databases can solve a plethora of problems. ENF broadcast databases could help to produce information about electric grid variations in places where physical presence is not desired. ENF broadcast databases can produce valuable information about grid variations in remote areas of interest.

## 5 Conclusions

Forensics is the argumentative science of applying a system of knowledge to solve legal problems. Forensics is a combination of several scientific fields to aid in the discovery of facts for answering legal disputes. Media forensics is applying digital science and a system of digital knowledge to answer legal questions concerning digital evidence. Digital knowledge is comprised of the science of digital audio recordings, digital image recordings or stills, digital files from computers, cell phones, GPS systems, and the list can be extended. Digital signal processing, statistics, photography, recording technology, electrical engineering, computer science, telecommunications, and more are all contributing fields to media forensics. No matter what background the examiner has, proper evidence handling comes first and foremost in a forensic examination. All forensic disciplines have controls and best practices on evidence handling, and media forensics is no exception. The slightest error when handling evidence can have catastrophic consequences in the analysis, in the interpretation, and eventually in the court room.

No judicial system is perfect and judicial errors have occurred in the past and will occur in the future. With strict adherence to best practices and guidelines the probability of judicial errors can be reduced. Throughout history, there have been faulty sciences. However, today in the US, the Daubert and Frye standards help to mitigate the possibility of allowing faulty science into the court room. Daubert and Frye can ensure that the science behind an expert's opinion is relevant and reliable but these standards cannot guarantee that the expert's opinion is free from bias. Bias can be mitigated through automatic analysis that involves complex algorithms on a computer with limited human contamination. Professional societies also help eliminate bias with their individualized but generally similar ethics rules and regulations. The forensics community spans international borders, and even though national laws do not span these same borders the standards in forensics are widely accepted throughout the scientific community with modified but not entirely unique adaptations for their respective countries. Just as the principles of DNA hold true in one part of the world as they do in America, the principles of sound and audio also hold true no matter what country the recording is coming from. The laws that govern how the evidence is used in court may vary from country to country but the scientific principles behind the analysis of the evidence are the same everywhere.

Generally speaking, the rules and laws that govern AC electricity and digital recorders are the same regardless of global location. If a recording

contains ENF it will be nearly identical to the ENF variations in the entire grid it was recorded on at that moment in time. Because the grid variations are random, non-predictable, and have a high probability to never repeat, the ENF Criterion can potentially establish the date and time of a digital recording through consistencies or differences between a reference database and the evidence recording. Forensic ENF databases are complex and there are several ways to configure all the elements of a database.

The ENF probe has been explained and tests have been performed to determine the configuration that would best suit the NCMF and TFSL acquisition systems. When configured correctly, an ENF probe should be able to take the electric network US 120 V 60 Hz signal (UCTE 240 V 50 Hz) and step it down to a safe line-level signal that is suitable for a computer sound card. The signal should be free from clipping and distortions no matter what components are used to configure it. Using high-quality components and a well designed circuit will help minimize the risk of contaminating an ENF database with distortions. The schematic for the NCMF ENF probe has been presented [22] and utilizes a transformer that steps the incoming 120 V or 240 V signal down to 6 V. The signal then goes through a three-resistor voltage divisor and then, to protect the sound card from network spikes or higher voltages, a series of anti-parallel diodes filters voltages above +0.7 V and below -0.7 V (1.4 V). The NCMF and TFSL ENF probes are outfitted with an LED so that it is easy to tell when the devices are powered. The output signal of the probe is connected to RCA connectors. Two ENF probes can be utilized in each database, one for each independent acquisition computer. The ENF probe should always be connected directly to the electric network source (wall socket) because connecting an ENF probe to a voltage regulator, UPS, power conditioner, surge protector, or power strip has the potential to cause an un-quantified amount of error.

Acquisition system time-controllers have been investigated and explained. NIST provides the most accurate and reliable source for time synchronization as a free service. There are three methods to connect with NIST time to provide an accurate time-controller to a forensic ENF database. Atomic-radio broadcast configuration involves connecting an external atomic-radio clock to each acquisition computer. An atomic-radio clock receives signal on a 60 kHz frequency from the NIST WWVB broadcast station in Fort Collins, Colorado (the UK also uses 60 kHz but a different broadcast station). GPS time receiver configuration involves connecting a GPS receiver to each acquisition computer. Most GPS time receivers can output a 1 pps signal in RS-232 format. Both atomic-radio clocks and GPS time receivers are one-way communications and do

not involve security risks to the forensic ENF database. Both atomic-radio clocks and GPS time receivers should be situated in a place where there is a clear view of the sky so that the signal will be better received. NTP internet synchronization is the third method of configuring a forensic ENF database to NIST time. There are three sub-methods within the internet synchronization method known as RFC-1305, RFC-867, and RFC-868. The advantage of using internet time synchronization is that the signal is not subject to the same interference as radio and GPS signals. Interruptions in servers and trunk lines can be a communication issue however. The strongest disadvantage of using internet synchronization is that it introduces a security risk because this is a two way communication. In the instance of TFSL, the corporate internal network is not accessible from the general-public internet. In addition, the forensics labs are on an internal network inside the larger corporate internal network. The forensics labs internal network is only accessible from inside the forensics lab; even if someone is connected to the corporate internal network they will not have access to the forensics labs internal network.

Sampling frequency was investigated and explained. The application of sampling frequency was described as it pertains to a forensic ENF database. Recommendations to record the ENF signal at 6 kHz – 8 kHz were mentioned so that sufficient information is available for different types of ENF extractions. Sampling ENF at 6 kHz – 8 kHz also creates database files that are 1GB – 1.3GB per day. Managing files of this size is much easier than managing 24-hour 44.1 kHz .WAV PCM files because of storage requirements.

The advantages of a high-resolution forensic ENF database go hand-in-hand with the sampling frequency. High-resolution allows for better signal representation and better possibility for other extraction methods and scientific research. Capturing the ENF signal at high-resolution also captures more harmonics which can be useful for certain types of analysis or testing new algorithms. The resolution of the database can be defined as R= *fs* / FFT. Finding the balance between time and frequency resolution trade-offs can be challenging when applying FFT methods. When evidence is being compared to an ENF database they shall both share the same time and frequency resolutions.

Sound cards were explained and recommendations for a sound card that has a SNR of at least 94 dB and a THD of at least 0.003% were made. The sound card is the link between the analog and digital domains or A/D conversion. Using high quality circuits will help in maintaining an accurate and reliable ENF database. The input level is also important as this can be a source of distortions.

In many Windows OS the soundcard configurations can be modified through the Control Panel. RecAll Pro also has a tab under *Preferences* that allows for selecting which driver will be used. SNR is also explained and a helpful graph is given that displays false alarm probabilities based on evidence SNR.

HDD and SSD storage media are explained and a recommendation is made to use SSD because this type of storage media is less susceptible to write error. The results of media storage configuration tests are revealed and helpful graphs are offered. The main concern with write errors in a forensic ENF database is that these types of errors look similar to certain types of digital audio edits. Hypothetically, if the spectrographic extraction method were presented in court to show the areas of potential edits in a manipulated digital audio file, and the reference database displayed similar indications then this could be a challenging phenomenon to explain to the court. And the justification of the expert's opinion would be difficult.

DC bias and frequency bias are explained and investigated to demonstrate that these are important consideration when using the ENF Criterion. DC bias can result in wrong zero-crossings. The time vs. voltage waveform should be centered on zero. Frequency bias can cause the signal to appear at frequencies other than the nominal ENF frequency; frequency bias can be mitigated by subtracting the mean of the time and frequency vectors.

Distortions are explained and investigated. The importance is stressed of configuring a forensic ENF database in a way that will be free from distortions. Distortions can be created from many different sources such as aliasing, jitter, input level, and clipping. The optimal combination of components for the ENF probe that will produce a distortion free signal is open for discussion; the combination that worked best for the NCMF and TFSL acquisition systems was presented. All the mentioned distortions can be easily avoided by calibration and using well designed high-quality circuits.

Network failure and UPS units are explained and investigated. The recommendation is made to connect the acquisition computers to a UPS unit. UPS units can help to keep the database record enabled during the electric network failure and when the electric network returns to normal operation, recording should continue. Depending on the UPS unit that is utilized the database should remain operational for at least 15 minutes and possibly up to an hour. Peripheral equipment such as monitors should not be connected to the UPS, because this equipment will unnecessarily draw power from the battery. Only the

acquisition computers should be connected to the UPS units. The ENF probe should be connected to the electric network directly. Connecting an ENF probe to a UPS unit will result in recorded battery signals during an electric network interruption.

The advances in ENF database configurations are presented. This includes helpful flow charts showing how a forensic ENF database is redundantly configured and how sub-databases are compiled at the NCMF. The sub-databases can be helpful for saving processing time when the ENF Criterion is applied to a case. The recommendation is to have a database of 6 kHz – 8 kHz *fs,* a database of 144 Hz *fs* (US) (120 Hz *fs* (UCTE)), and a database of 360 Hz *fs* (US) (300 Hz *fs* (UCTE)). The examiner is free to configure any other sub-databases as they see fit. For the 6 kHz – 8 kHz *fs* database files will be 1GB – 1.3GB. Recommendations about the time-controller are also reinforced. A helpful chart showing three ENF extraction methods is provided.

There are other areas to pay attention to and these areas are briefly mentioned. The NERC has made a proposal to extend the US electric grid frequency thresholds and these changes could affect the extraction processes and types of filters used in ENF extraction. Another important note is the interference in the ENF signal from the neutral line carrying voltage. This type of interference has the potential to affect zero-crossings. Helpful ENF database management software is presented. The ENF Database Manager was compiled in Matlab and can help to streamline the configuration of multiple ENF databases.

Overall, there can be no single solution and one configuration method that will eliminate all possibility of error. However, by following the recommendations mentioned in many scientific articles and understanding how all of the elements in a database combine to create a forensic ENF database, the examiner will be much more likely to maintain a database that is suitable for use in the court room and scientific research. Deviating from the recommendations has the potential to introduce un-quantified amounts of error into an ENF database.

The possibility of broadcast ENF databases is introduced and investigated. Broadcast databases can be utilized to collect ENF information in one location and receive the information in a remote location. This type of configuration can be beneficial for establishing ENF monitoring in areas where continued technician interference is not a possibility or in areas where a full acquisition system is not feasible. By using an ENF probe that is equipped to

broadcast the ENF variations; the risk of losing an entire database is minimized at the cost of a simple device that is installed in high-risk areas. Three types of ENF broadcast probes are introduced: FM radio probe, Blue-Tooth probe, and Wi-Fi Probe.

After reading this thesis the reader should have a better understanding of all the elements that are used in a forensic ENF database and a better understanding of how these elements can be configured to minimize error and maximize results. In the future, the ENF Criterion will be introduced into the US courts and will satisfy all the Daubert/Frye standards. Formal best practice guidelines and standards will continue to develop around the ENF Criterion. ENF will continue to be a valuable source of scientific research and will continue to provide valuable forensic results. There is a significant amount of literature on the ENF Criterion. To learn more about the ENF Criterion, media forensics, or forensics in general please read any or all the references in the bibliography.

## APPENDIX A: ENF VOLTAGE REGULATION

The recommendation to connect an ENF probe directly to the electric network via wall socket has been mentioned several times. The thought process behind that recommendation is that voltage regulation circuits, power conditioning circuits, surge protectors, and power strips could potentially alter the 60 Hz signal and make the "conditioned" ENF database useless. The idea makes sense in theory, but when applied in practice, the results of one experiment suggest otherwise.

In a laboratory that was entirely powered from Power Distribution, Inc (PDI) voltage regulation cabinets the size of refrigerators, an ENF probe output was connected to a Sony PCM D-50. The ENF probe was connected to a power strip/surge protector that was connected to the power from the PDI cabinet. The power supply for the Sony was also connected to the power strip/surge protector. The signal was recorded for roughly eight hours. After processing the signal by down sampling to 144 Hz and Band Pass Filtering around 60 Hz a comparison was made against the ENF database. The results revealed that there was no indication that the PDI voltage regulator affected the ENF signal. From this experiment the recorded PDI ENF is still acceptable for spectrographic extraction methods. In Figure A1, the top spectrogram is the PDI ENF and the bottom spectrogram is the ENF database file.

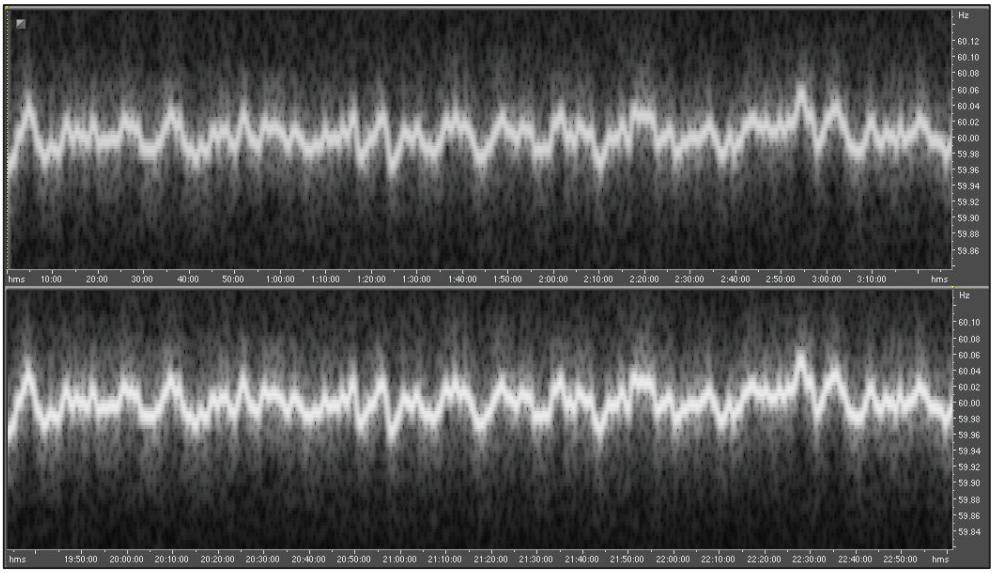

**Figure A1** Regulated Power Supply

## APPENDIX B: REAL CASE DATABASE CONFIGURATION

Through an investigative approach to combining the elements that make a forensic ENF database, a series of tests were carried out at the Target Forensic Services Lab (TFSL) while establishing the Eastern grid ENF database. Several elements, and the way they interact with each other under forensic conditions were evaluated in an attempt to configure the Minneapolis (MN-ENF) database in a way that will meet forensic standards. This is an evaluation of a four-day trial-run that was carried out after the initial set up. After analyzing the recorded files it is apparent that the database is functional but impaired. Some "bugs" have been identified and will need to be fixed before the database can meet forensic standards. The two elements of the configuration that are experiencing these "bugs" are the acquisition computer storage media and the Time-Controller, the "bugs" show up as artifacts in the recorded ENF database file. These artifacts look similar to typical deletions in digital audio.

ENF Probes

Two modern ENF probes were built for use in the TFSL Minneapolis ENF database (MN-ENF). The probes were built with the components recommended by the Audio Engineering Society convention paper 8492 (2011) [22]. The ENF probes were tested to confirm that the output voltage would be suitable for a computer sound card (~550 mV) and also tested to confirm that the output signal was free from distortions. Once the probes produced satisfactory results they were connected to the acquisition computers via RCA – $1/8^{th}$ inch stereo cable

Time Controller

In order to maintain accurate time synchronization the National Institute of Standards and Technology – Network Time Protocol (NIST-NTP) internet time service was utilized in the MN-ENF database. Because of the unique situation Target has concerning the internal network, it was determined that using the NIST-NTP internet time service would not introduce a significant security risk. The TFSL has a secure internal network that resides inside the larger Target internal network. The NIST-NTP internet time services configuration must be subjected to a security assessment by the Target Information Security Services to determine the penetration risk of the MN-ENF database. Failure to confirm the security of the MN-ENF database could have detrimental effects further down-stream in the judicial system. NIST provides free time services through a variety of methods; to assist with using the NTP internet time services NIST offers a free software program that can be downloaded from

http://www.nist.gov/pml/div688/grp40/its.cfm the program is called "*nistime-32bit.exe*". NIST also maintains several servers around the United States that can be pinged periodically to synchronize a computer with NIST time. A full list of NIST servers and other partner servers can be found at http://tf.nist.gov/tf-cgi/servers.cgi the site also provides information about server health and traffic congestion.

The basic way in which a computer is synchronized using the NIST-NTP time services is by installing the free program (nistime-32bit.exe) and selecting the server that should be pinged for time of day information. In Windows 7 64-bit the Task Scheduler can be used to configure a time synchronization event. During the trial-run of the MN-ENF database the time synchronization task was scheduled to run every morning at 01:00 and repeat every 15 minutes. After the trial-run it was determined that the task will be ignored if the nistime-32bit.exe is already running when the new task is queued hence there is no need to have the task start every 15 minutes.

The "bug" that was encountered occurred at roughly 01:00 the morning of 2011-10-23. By checking the Windows event logs it was determined that a *system restore* event was generated at 01:00:20 on the morning of 2011-10-23 (see Figure B1). At 01:05:24 on the morning of 2011-10-23 a warning appeared in the event logs that involved the RecAll Pro recording software (see Figure B2). This event corresponds precisely where the "bug" is seen in the ENF database file. Both ENF acquisition computers had the same "bugs" at the same time and reflected the same events in the logs.

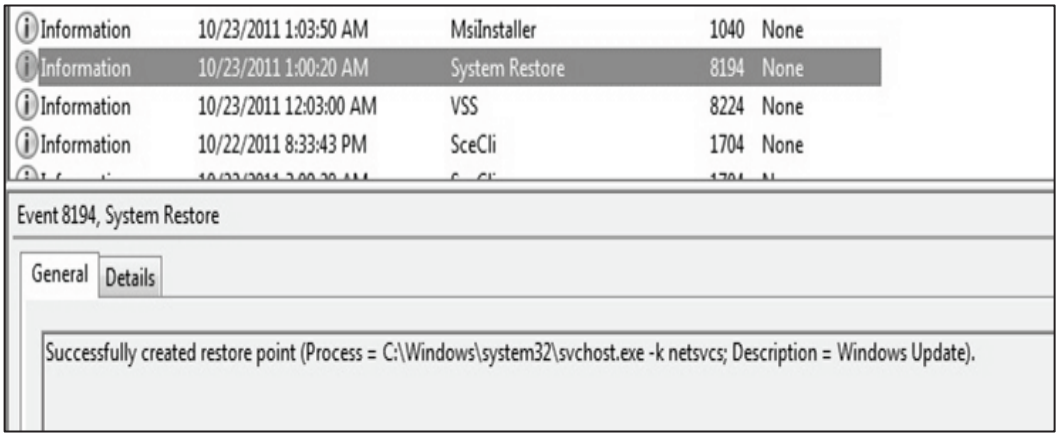


**Figure B1** Event Log (A)

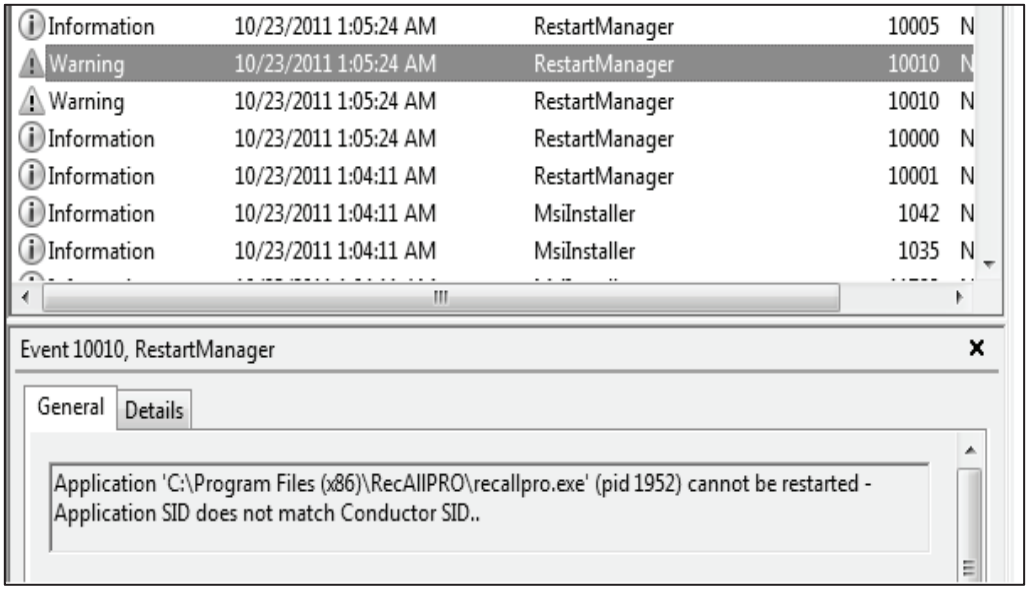


**Figure B2** Event Log (B)

One possible explanation is that the *system restore* event caused RecAll Pro to be interrupted when the program was told to restart and returned an unmatched *conductor SID*. Because the time synchronization task was scheduled for 01:00 daily and is a required task to maintain accurate time synchronization in this specific configuration, a decision was made to reconfigure the time synchronization task so that the task is queued once daily at the same time the ENF files are being saved. In this updated configuration, the task is scheduled to start when the ENF database files are saved, PC1 saves files every night at 23:59 and starts the nistime-32bit.exe; PC2 saves files every day at 11:59 and starts the nistime-32bit.exe. With this task configuration each acquisition computer should start the nistime-32bit.exe once a day when the ENF files are being saved. Once the nistime-32bit.exe program is running it should periodically ping the selected server once an hour. The settings used to reconfigure the time synchronization task are presented in Figure B3 and Figure B4. The complexity of an ENF database configured to use NIST-NTP time could be avoided by implementing an atomic-radio clock or a GPS time-receiver because these devices require no network connection and the PC will not be tasked with automatic updates. Another disadvantage to the NIST-NTP internet time synchronization configuration is that if the server health changes due to increased traffic then the PC could have trouble getting updates. Furthermore, Target has a sophisticated firewall that is great from a security perspective but this can make pinging a

NIST server challenging. There were five other tasks that occurred the same time as the write error and these tasks were disabled: Defragment Hard Drive Task, Diagnosis Maintenance Task, Disk Diagnostic Task, Maintenance System Performance Task, Windows Error Reporting Task.

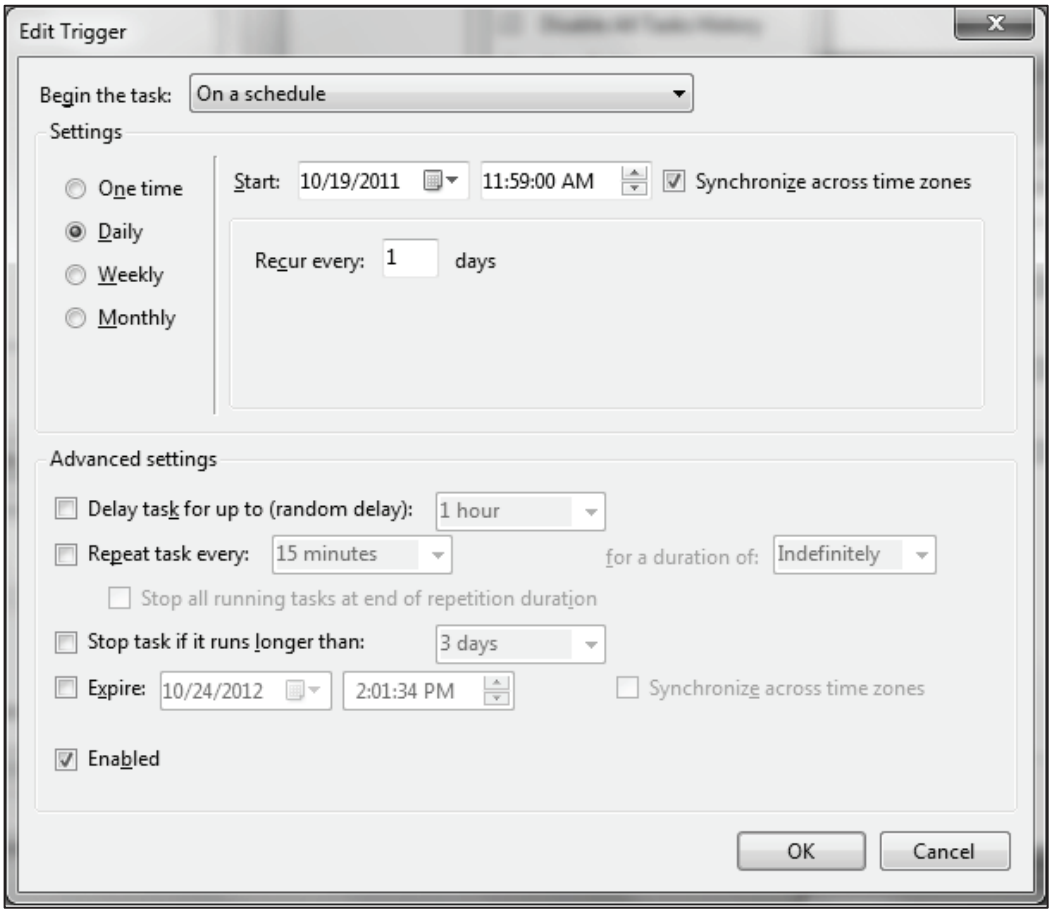


**Figure B3** Task Schedule

Sampling Frequency, High Resolution Databases, and Resolution/FFT Settings

The files of the MN-ENF database are configured to record 8 kHz 16-bit mono .wav PCM. The sampling frequency can be adjusted in two places on the database computers: in RecAll Pro under *options>preferences>wav* and in Windows under *control panel>hardware and sound>sound> then double click on the default audio device and click on the Advanced tab* and the sampling frequency can be adjusted in the drop down menu.

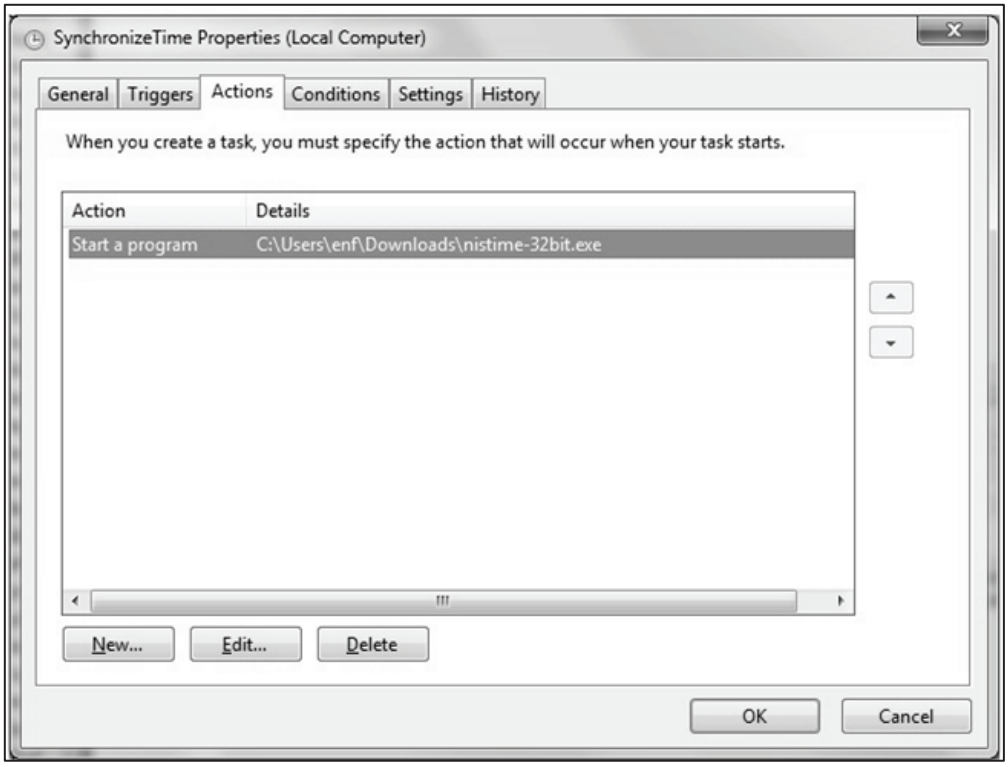


**Figure B4** Task Action

It is important to maintain a high resolution database so that further forensic scientific research can be carried out and so that accurate automatic ENF extraction methods can be employed for forensic examinations. The database files are ~1.3GB per 24-hours and do not require an unmanageable amount of storage space.

By post processing the trial-run MN-ENF files using Adobe Audition it is clear that the files are suitable for forensic analysis using the spectrographic method. This was determined through a forensic examination of mock evidence

Sound card, input level, and signal to noise ratio

Each sound card in the MN-ENF acquisition computers is built into the mother board of the computer and accepts audio line-in via 1/8$^{th}$ inch stereo plug. The sound cards are capable of recording 8 kHz sampling frequency. The input level is adjusted to be roughly -12 dB Full Scale (dBFS). The input level can be adjusted in Windows under *control panel>hardware and sound>sound> then double click on the default audio device and click on the volume slider*. In this

configuration the volume slider is set around 10. The signal to noise ratio (SNR) was measured ~84 dB. This SNR will satisfy forensic standards because the signal of interest is much higher in amplitude compared with the noise that surrounds it see Figure B5.

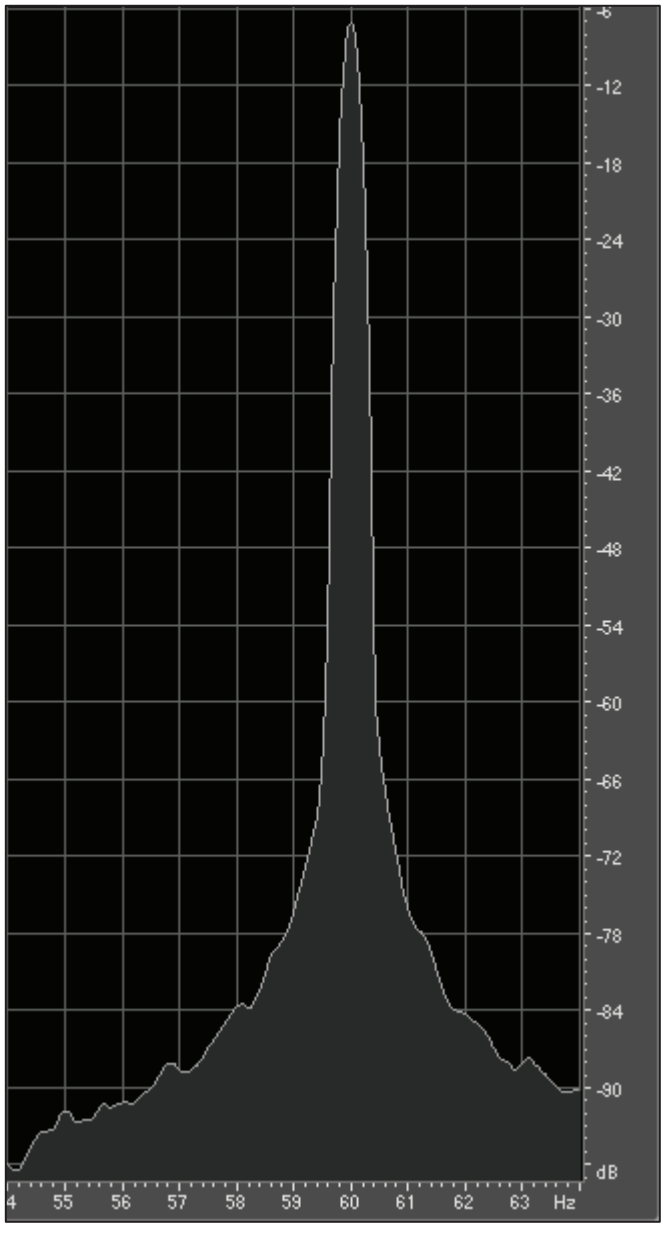


**Figure B5** Signal to Noise Ratio (SNR)

Storage Media

The MN-ENF database has been configured with two independent acquisition computers running in parallel. Each acquisition computer is equipped with a Windows 7 64-bit platform on a 7,200 RPM HDD. An auxiliary 64GB SSD is installed in each acquisition computer and this is where the database files are written. The reason SSD storage media is utilized over HDD storage media is because of the potential for write errors on the HDD. A wide range of media storage configurations were tested including:

- Running the operating system (OS) on the same storage media that the database files were being written to on a 7,200 RPM HDD.
- Running the OS on the same storage media that the database files were being written to on a 10,000 RPM HDD.
- Running the OS on a 7,200 RPM HDD and writing the database files to an auxiliary 7,200 RPM HDD.
- Running the OS on a 7,200 RPM HDD and writing the database files to an auxiliary 10,000 RPM HDD.
- Running the OS on a 10,000 RPM HDD and writing the database files to an auxiliary 10,000 RPM HDD.
- Running the OS on a 7,200 RPM HDD and writing the database files to an auxiliary SSD storage media.

The list of possible configurations for storage media could be nearly endless but given the circumstances the above configurations seemed like the most reasonable. Other experiments were carried out beyond just the configuration of the drives such as running multiple instances of RecAll Pro to multiple storage media simultaneously.

At one point there were two simultaneous write errors on two separate HDD, one spinning at 7,200 RPM and the other spinning at 10,000 RPM. The HDD's were in two separate machines each running two instances of RecAll Pro independently and the 7,200 RPM disk was being used as the OS drive in PC1 and the 10,000 RPM disk was being used as an auxiliary drive in PC2. It was through tests such as these that the cause of the write errors could be narrowed down. For example, in this case if the write error had been cause by an electric network fault then it would have shown up on all four HDD's. If the write error had been caused by the OS it would have shown up on both OS drives. If the write error had been caused by the speed of the disk it would be on both the 7,200 RPM HDD and not the 10,000 RPM HDD. Another experiment was

conducted by disconnecting the computers from the network to see if a network connection could be interfering with the recordings but the write errors showed up in that test as well.

If other experiments are to be carried out concerning the storage media then Redundant Array of Independent Disk (RAID) configurations should be experimented with. The last configuration from the list above had the lowest amount of write errors, having only one write error during 96 hours of recording time. This is a good start but does not meet forensic standards and must be addressed.

The thought at this time is that the write error found during the trial-run of the database was caused by software and not hardware. Because the Windows event logs have activity that corresponds to the time of the write error and events that involve the RecAll Pro program; it is highly likely that carefully configuring the software and OS scheduled events will eliminate these errors. An example of the encountered write errors are presented with a brief explanation in Figure B6.

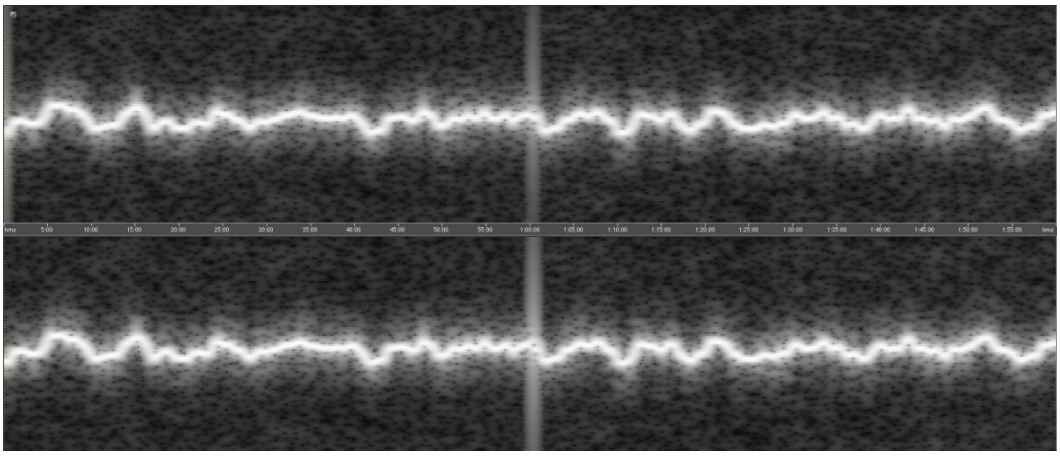

**Figure B6** 2011-10-23 01:00 Write Error

The write error in Figure B6 illustrates the result of the spectrographic ENF extraction method on MN-ENF-PC1 (top) and MN-ENF-PC2 (bottom) from the morning of 2011-10-23 at roughly 01:00. This error occurred simultaneously on both acquisition computers, independently of each other. Both of the Windows event log files on each PC document a *system restore* event at roughly the same time as these write errors. Additionally, approximately 5 minutes later the RecAll Pro program was told by the system to restart on both

machines and this is precisely where the write error occurred. Both MN-ENF-PC1 and MN-ENF-PC2 are configured to write the database files to SSD. This write error is not a hardware related issue, as there are no moving parts in the SSD. This is caused by a system interruption of the RecAll Pro software that created a disturbance in the audio signal.

Direct Current (DC) Bias and Frequency Bias

DC bias in a digital system is typically caused by poor-quality components or poor-quality design in an A/D system, DC bias can also be introduced along the analog signal path. Averaging the sampled values and subtracting the average is usually the simplest way to remove DC bias from a signal. If DC bias is not removed from recorded evidence before examining it for ENF then erroneous zero crossings can result. DC bias will cause the signal to be centered on some value other than zero and the peaks and valleys will not intersect with zero in the proper place (time vs. voltage/amplitude waveform). In order to implement the zero crossing extraction method as mentioned in [1], [4], [8], [14], [16] DC bias must be removed.

Different media recorders will produce different frequency bias but most recorders will introduce some degree of frequency bias into digital audio due to inaccurate clocks. If the original recording device is made available for the examination then determining the consistency of frequency bias from the specific recorder versus some other source can be examined.

The trial-run ENF files from the MN-ENF database have been examined to determine how much DC bias is being introduced. Figure B7 illustrates the time vs. amplitude waveform of an ENF database file that was recorded on MN-ENF-PC1, three wrong zero crossing have been circled for clarity. The peaks of the signal reach a normalized value of 0.48 and the valleys reach 0.45, this means that the signal is offset from zero by 1.5% towards positive voltage. By first down sampling and then band pass filtering the signal the process will essentially average the samples and remove the mean from all the samples and should eliminate the DC bias. In Adobe Audition, the DC bias can be confirmed under *window>amplitude statistics*.

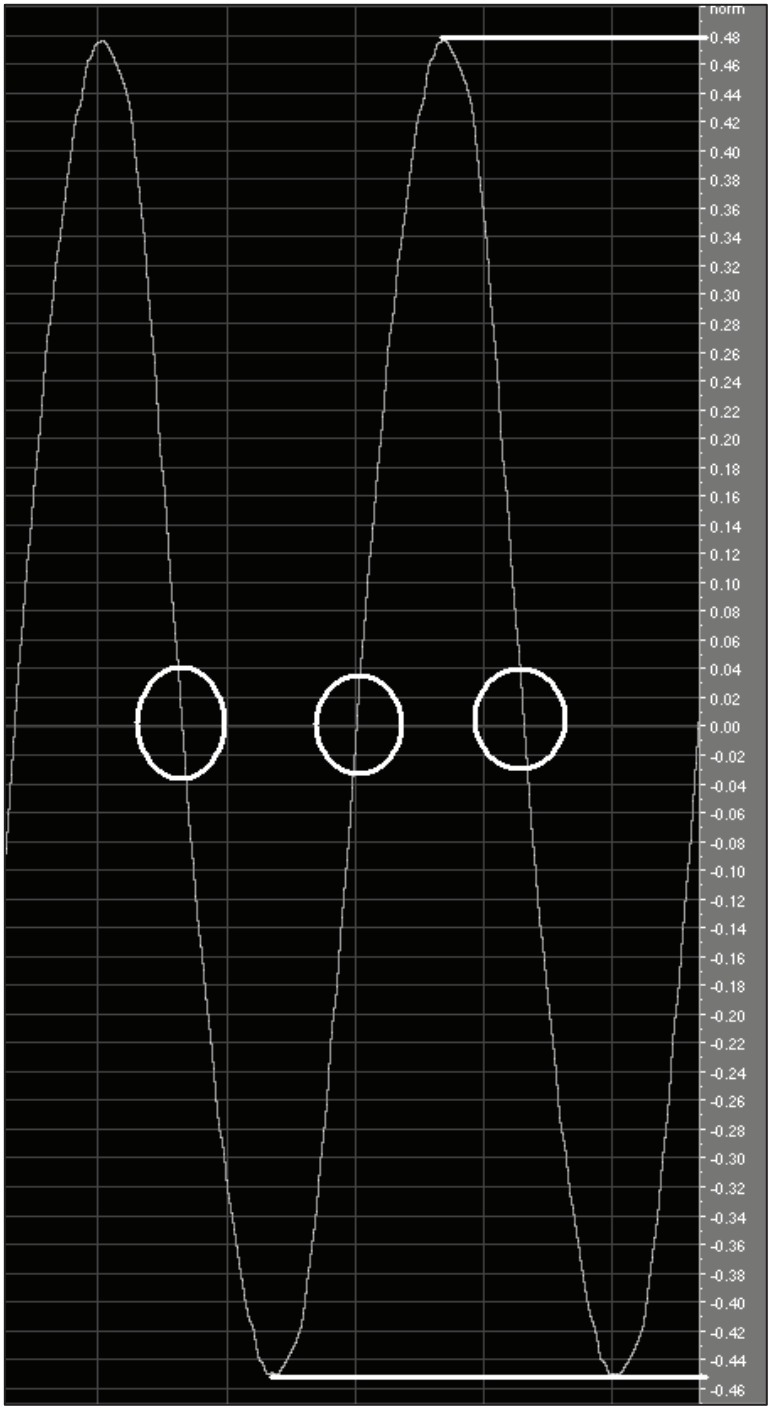


**Figure B7** DC bias on MN-ENF PC1

Distortions

The two main distortions of concern for the MN-ENF database were aliasing and jitter. The ENF probes had been tested and were known to be producing distortion free signals. The input level was adjusted correctly and no distortions were being created at the input. The files from the trial run had been processed and examined and are suitable for forensic case work. Because other types of distortions can be subtle, a test was conducted for aliasing.

The aliasing test was conducted by creating a sine wave sweep in Adobe Audition from 20 Hz – 20 kHz for a duration of 30 seconds 44.1 kHz sampling frequency, mono, 16-bit, .wav PCM. This file was then played through the sound card on MN-ENF-PC1 and recorded using RecAll Pro set to a sampling frequency of 8 kHz, 16-bit, mono, .wav PCM. The spectrogram of the original sine wave sweep is presented in Figure B8 and shows how the signal is capped at the 22.5 kHz ceiling, notice how the frequencies are capped at the 22.5 kHz mark in the upper right corner. The spectrogram in Figure B9 shows how the signal is folded over back into the audible bandwidth.

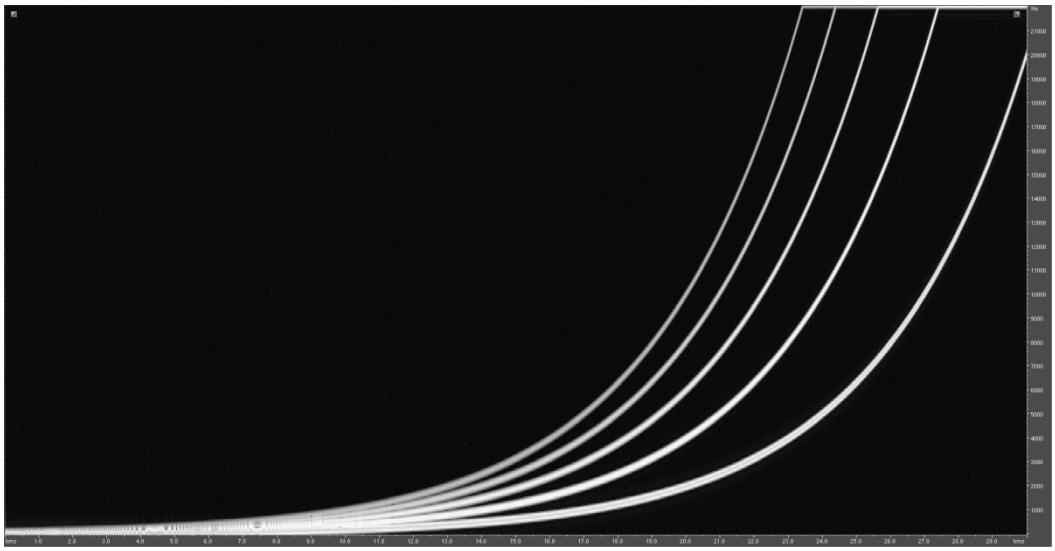

**Figure B8** 44.1 kHz Sine Wave Sweep

The original sine wave sweep from FIGURE B8 was created in a logarithmic scale and this is why the bright lines curve. There are five visible bright lines that signify areas of high amplitude. The X-axis represents 30-seconds and the Y-axis represents frequencies from zero to 22.5 kHz. It is important to note here that there are no signs of noise or aliasing distortions

because the sampling rate it capable of capturing all frequencies generated by the sine wave sweep with at least two samples.

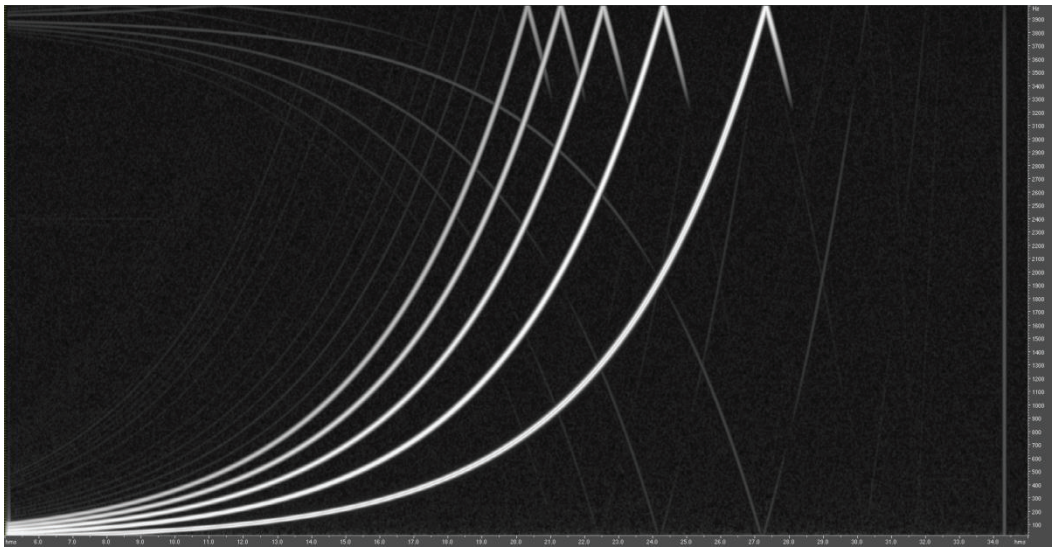

**Figure B9** MN-ENF-PC1 Aliasing

Jitter is a distortion that is created from the word-clock of a digital system being inaccurate. Jitter was also tested using the method presented in section 3.7 where a known sine wave of 60 Hz was used to verify that the pure tone is being accurately captured, i.e., 1 second can be divided by 60 Hz (1/60 = 0.016). By measuring the distance from peak to peak in the pure-tone and comparing that distance to the time line, the distance from one peak to the next or one cycle is 0.016 seconds. If the computer is capturing a pure signal correctly then any other signals should be correctly captured as well.

Network failure/Uninterrupted Power Supply (UPS) and safe guards

The TFSL provided two UPS units for the MN-ENF database, one UPS for each acquisition computer. The UPS units were tested by first charging the UPS units and then connecting an ENF probe to the UPS and then disconnecting the UPS from the wall socket. Both units failed and it was decided that replacement units must be provided. This was a simple and often over-looked test. A common misconception is that a UPS can be connected and will work when needed but this is not always the case. The UPS is basically a battery and if it is not given a charge periodically damage can occur.

Advances in ENF Database Configuration

The MN-ENF database has been configured in a way so that two independent acquisition computers run in parallel with each other. A modern ENF probe has been built and provided for each acquisition computer. The built-in sound cards on both acquisition computers have the ability to record audio at the desired 8 kHz sampling frequency. MN-ENF-PC1 records files from 00:00 – 23:59 and automatically saves them to the SSD. MN-ENF-PC2 records files from 12:00 – 11:59 and automatically saves them to the SSD. The NIST-NTP internet time service has been installed to synchronize both acquisition computer's time controllers. Files recorded on the auxiliary SSD can be transferred over the network and stored in several sub folders depending on the type of sub database to be compiled for example, 8k Hz, 360 Hz, and 144 Hz.

In summary, the MN-ENF database has been configured in a way to meet forensic standards and provide an accurate, reliable, and reproducible source of Eastern grid ENF information that is suited to be used in forensic examinations of digital media, the court of law, and further scientific research. The ENF probes have been built using presented methods [22] and high quality components. The time controller has been configured. The sound card, input level, and signal to noise ratio have been investigated and configured correctly. The storage media has been scrutinized with several tests and the results of those tests lead to the current configuration. The DC bias of the acquisition system has been calculated and the methods for compensating the DC bias are known. The distortions have been examined and are known to introduce negligible effects in the database. The Uninterruptable Power Supplies have been tested and configured. The advances in ENF database configuration have been explained and are available for further discussions. The only requirements now for the MN-ENF database are to replace the UPS units with ones that work, and assess the security risk of the NIST-NTP internet time services connection. A Memorandum of Understanding has been created between the NCMF and TFSL to help strengthen the ENF Criterion.

## APPENDIX C: BALANCING THE ENF

This appendix explains balancing fundamentals of the United States electric grids, which is a key element in how ENF works. Earlier in the text the fundamentals of ENF were described as an imbalance between production and consumption of electricity throughout an electrical grid; the more power consumed the lower the frequency and the more power produced the higher the frequency, but always fluctuating around 60 Hz. Descriptions also explained how it is possible to compile an ENF database in one point on an electric grid and make comparisons to recordings from another point on the same grid from that moment in time. This section will discuss more in depth the elaborate balancing of the electrical network and this appendix will explain how and why the ENF signal fluctuates over time to give an in depth understanding of ENF origins.

All of North America is connected by four electric grids; the Western grid covers the geographical area that is generally West of the Rockies and extends North through Canada, the Eastern grid covers the geographical area that is generally East of the Rockies and extends North through Canada, Texas is covered by the Texas grid, and Quebec is covered by the Quebec grid. For all intents and purposes the majority of this thesis has discussed the United States grids only, even though the same concepts and principles can be applied to the Canadian Eastern and Western grids, which is a concept tested and confirmed by Sanders [12].

Electricity can be generated by many different means such as coal power, hydro-electric power, and nuclear energy. For coal power and nuclear energy, high pressure steam is used to spin a turbine that is connected to the generator. Hydro-electric power utilizes large quantities of water under the force of gravity to spin a turbine that is connected to a generator. By which ever means the generator is powered the speed of the generator is the frequency at which the AC electricity is transmitted. The electricity is sent out of the power plant to a step-up station where the voltage is increased to the order of 500,000 Volts for the long distance travel via high voltage lines to a balancing authority where the power is stepped down and then distributed to the end user.

Mechanical systems with moving parts are theoretically impossible to remain in a perfectly steady state of motion. An example is the mechanical speed variations in analog tape recording devices, the inevitable variations in motor speed create what is known as “wow & flutter”, as a steady signal is sent to the tape to be recorded the speed of the tape speeds up and slows down slightly as

the moving parts adjust their speed, thus the reproduced signal reflects these small adjustments. Although the spinning motion of the generators in the electric network is abnormally consistent for a mechanical system, there is some variation in the speed at which the generators spin. In fact, the variations in speed are often intentional to keep the overall grid within a given threshold around 60 Hz. For all practical purposes the variations between the speeds of any given generators is so insignificant that it is negligible so long as the generators are spinning within a tight threshold of each other because all generators on a given grid spin in tandem with one another. The US Eastern grid for example, has an electric network frequency tolerance of +/- 0.02 Hz around 60 Hz [65]; meaning that when the frequency of the network reaches 60.02 Hz the generators are told to slow down and thus decrease the electric network frequency. On the other hand, when the frequency of the network reaches 59.98 Hz the generators are told to speed up thus increasing the electric network frequency. An entire electrical network can be thought of as a large machine made up of several generators that are pulling in tandem with each other, meaning that any given generator must be synchronized with the generators on either end of it. An analogy can be made to ships connected by rope; imagine three ships connected by tow-lines end to end to end, in order for the ships to sail smoothly they must all be moving in unison at the same speed. If the first ship in line slows down and the ships behind it continue at a faster speed there will be a collision. Like this, the generators on an electric grid must continue rotating at the same speed in order to keep from causing network impairment. A generator that spins as much as 2 Hz faster or slower than the others can quickly generate enough heat to destroy itself [65].

To help manage the communication between generators there is a complex network of “Balancing Authorities” that are established in strategic locations across North America, there are about 100 Balancing Authorities connected by high-voltage power lines. These Balancing Authorities are responsible for the amount of electricity in and out of their sub-station. North America is divided into eight regions with several Balancing Authorities within each region. Multiple regions can operate within a single electric network and some regions even span multiple electric networks. These Balancing Authorities are simply a means to keep track of how electricity should be bought and sold and where it should go to meet consumer demands and balance the produced power. These Balancing Authorities operate by being able to store a given amount of electricity so that when demand increases the balancing authority can release the needed electricity. The Balancing Authorities can also transfer electricity to one another when needed through buying and selling in Mega

Watts. Figure C1 displays a map of North America with several balancing authority locations.

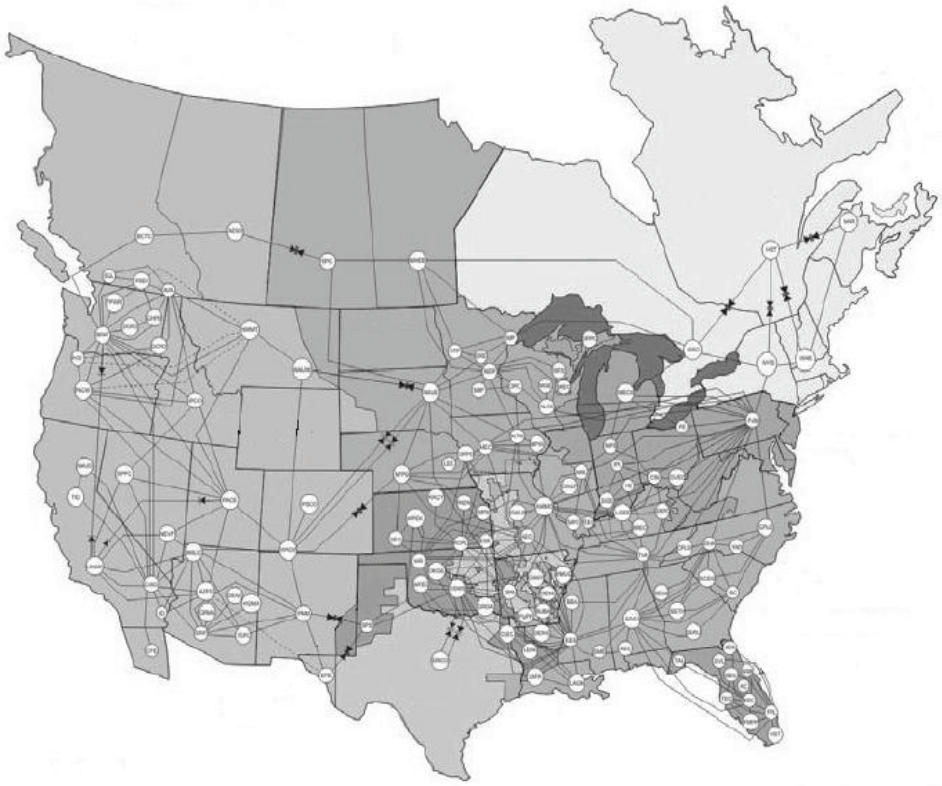

**Figure C1** North American Balancing Authorities

The entire balancing system is controlled by several types of frequency control mechanisms. The primary control responds to frequency disruptions within seconds and is used to stabilize the frequency when it reaches the set thresholds. The secondary control responds to frequency disruptions within minutes and is used throughout an average day to restore the network frequency to 60 Hz. The tertiary control will be responsive for intervals of time over 10 minutes and up to multiple hours. From these three main controls most minor changes in electric network load such as residential uses, are maintained by the primary control. Medium offsets such as small industrial uses that remain present in the system for minutes will be restored by the secondary control. Large offsets from events such as factories or subway stations coming on or off line will be

restored over time by the tertiary control. In addition to these controls there is also a time controller that will use the electric network frequency to control the ticking rate of a simple clock such as an alarm clock. The simple clock is compared against the NIST time reference and if the offset between the two clocks reaches a given threshold such as the US Eastern grids 10-second threshold, then balancing will begin as needed. For example, if the network frequency runs 5 mHz high (60.005 Hz) for 10 hours, a clock will speed up by 3 seconds [(60.005 – 60.000) / 60 * 10 * 3600 s/hr = 3s].

The North American Electric Reliability Corporation (NERC) has developed an equation to control the performance of the Balancing Authorities Area Control Error (ACE) [65]. The ACE is what tells the Balancing Authority whether the electric network is balanced or is in need of an adjustment.

$$ACE = (NIa - NIs) - 10B\,(Fa - Fs) - Ime \quad \text{[C1]}$$

Where $NIa$ equals the algebraic sum of the actual measured flow between the Balancing Authority and the electric network. $NIs$ equals the scheduled flow between the Balancing Authority and the electric network. $B$ expresses the Balancing Authority's frequency bias in MW/0.1 Hz, the $10B$ converts the bias measurement to MW/1Hz. $Fa$ & $Fs$ are the algebraic sum of the actual measured electric network frequency and the scheduled frequency, respectively. The scheduled frequency is typically 60 Hz but this may change due to demand. $Ime$ expresses the correction factor for meter error which is usually zero. The meters that the Balancing Authority's use are not always perfectly accurate but the error between actual instantaneous flow and the meter reading can be compensated for with this expression. For example, if a Balancing Authority in California with a bias of -30 MW/ 0.1 Hz wants to purchase 500 MW from a Balancing Authority in Colorado but the actual flow into the California Balancing Authority is 525 MW and the actual electric network frequency is 59.98 Hz then:

ACE = (-525 - -500) – 10 * -30 * (59.98 – 60.00) = -31 MW

The question then becomes "what happens to the 31 MW?" The answer is that the Balancing Authority should reduce power generation by 6 MW to meet its obligation to the electric network at that time. It may seem counterintuitive to reduce production when the electric network frequency is low but the reason is that the energy deficiencies in the area at that time amount to 25 MW and the

Balancing Authorities bias (obligation to fix area deficiencies) is 30 MW. The Balancing Authority can thus decrease production by the product of their frequency bias multiplied by the ENF offset otherwise the regions overall offset to compensate the deviation from the scheduled ENF will be increased to 31 MW instead of 25 MW. Typically the flow into a Balancing Authority is negative and flow out of a Balancing authority is positive, hence the negative values in the example above.

To control the speed of the generators and react to the demands of the electric network, governors are used to control generator speed much like the way that cruise control maintains a set speed. The governors on electric network generators react within milliseconds of demand and can increase or decrease the speed of the generator as needed.

There are also some interesting statistics surrounding the affects of power usage on the overall frequency of the ENF in a given electric network. Cooper offers an abundant amount of information on this area in his 2011 IJSLL article [23] concerning the UK electric grid and the European UCTE grid. Cooper noted that the variations in the UK grid seem to be larger and more frequent than the variations in the European UCTE with the UK grid having 2.5 times the average daily range, nearly 3 times the average daily standard deviation, and 2 times the average daily Rate of Change than the UCTE grid. This phenomenon would be expected due to the relatively small size of the UK grid when compared to the European UCTE grid. An in depth study such as Cooper's has not been conducted on the North American electric grids but there is some statistical data that can provide some insight to the Eastern grid, Western Grid, Texas grid, and Quebec grid variations and the amount of power that is required on each grid to adjust the overall ENF by a slight amount.

In Table C1 the affect of a 1,000 MW power loss on a given electric grid is displayed in frequency variation of the electric grid. TABLE C2 displays the amount of power required to change the ENF of a given grid by 0.1 Hz. It is interesting to note the amount of power needed to change the ENF by an amount on the order of 0.1 Hz because when examining ENF the variations are large enough to make the authentication of a digital audio recording possible. The tables below give insight to the amount of power that is behind the seemingly small variations of ENF and further solidify the idea that a simple task such as turning off a light switch will have an impact on the overall ENF of the grid, even though it is a very small impact. The numbers from Table C1 and TABLE C2 can be found in the January 2011 NERC document [65]. The 1,000 MW

amount of power loss in TABLE C1 refers to 1,000 MW of generation loss. Inversely, if 1,000 MW of load were lost then the frequency changes would be positive. To obtain the values in the Table C2: 1,000/(0.036*10) for the Eastern grid. Then to obtain the inverse for the Eastern grid: 2,777*(0.036*10).

**Table C1** 1,000 MW Affect on Frequency

| Grid | Amount of Power Loss | Change in Frequency |
|---|---|---|
| Eastern | 1,000 MW | - 0.036 Hz |
| Western | 1,000 MW | - 0.067 Hz |
| Texas | 1,000 MW | - 0.154 Hz |
| Quebec | 1,000 MW | - 0.833 Hz |

**Table C2** MW Required to Change ENF by 0.1 Hz

| Grid | Required Power | Change in Frequency |
|---|---|---|
| Eastern | 2,777 MW | 0.1 Hz |
| Western | 1,492 MW | 0.1 Hz |
| Texas | 649.3 MW | 0.1 Hz |
| Quebec | 120 MW | 0.1 Hz |

The Balancing Authorities have a complex frequency monitoring system to keep track of the amount of power and the frequency of that power between themselves and the distribution stations. On the consumer side of the Electric network there is also a complex network for monitoring frequency called Frequency Monitoring Network (FNET). FNET utilizes several Frequency Disturbance Recorders (FDR) placed in strategic locations around North America to monitor electric grid frequency. Each FDR unit is equipped with a built in Low Pass Filter, A/D converter, GPS time receiver, a micro-processor, and network communication modules [9], [68], [69]. The FDR units deployed by Virginia Tech have a sampling rate of 1.44 kHz and the collected information is transmitted through the internet and later compiled in a database. The collected information can be used to gather statistics about ENF variations and also to triangulate the epicenter of frequency disturbances by calculating differences in time and frequency between multiple locations.

## BIBLIOGRAPHY

[1] Grigoras, Catalin. (2005). Digital Audio Recording Analysis: The Electric Network Frequency (ENF) Criterion, *International Journal of Speech, Language, and the Law,* 12 (1), 63-76.

[2] Kajstura, M., Trawinska, A., & Hebenstreit, J. (2005). Application of the Electrical Network Frequency (ENF) Criterion a Case of a Digital Recording*, Journal of Forensic Science International, 155*, 165-171.

[3] Simón Del Monte, F.J., Bouten, J., Grigoras, C., & Gonzalez-Rodriguez, J. (2006). Dating of digital audio recordings by matching of electrical network frequency patterns, *Presentation at Universidad Autonoma de Madrid, Spain,* 1-19.

[4] Grigoras, Catalin. (2006). Applications of ENF Criterion in Forensic Audio, Video, Computer and Telecommunication Analysis, *Journal of Forensic Science International, 167*, 136-145.

[5] Morjaria, Nisha. (2006). *An Investigation into the Electrical Network Frequency (ENF) Technique for Forensic Authentication of Audio Files.* Unpublished bachelor's thesis, Nottingham Trent University.

[6] Brixen, Eddy B. (2007). Further Investigation into the ENF Criterion for Forensic Authentication, *Journal of the Audio Engineering Society*, 123C, 1-6.

[7] Brixen, Eddy B. (2007). Techniques for the Authentication of Digital Audio Recordings, *Journal of the Audio Engineering Society*, 122C, 1-8.

[8] Grigoras, Catalin. (2007). Applications of ENF Analysis Method in Forensic Authentication of Digital Audio and Video Recording. *Journal of the Audio Engineering Society,* 123C, 1-13.

[9] Wang, L., Burgett, J., Zuo, J., Chun Xu, C., Billian, B.J., Conners, R.W., Liu, Y. (2007). Frequency Disturbance Recorder Design and Developments, *Journal of the Institute of Electrical and Electronic Engineers,* 1298 (6), 1-7.

[10] Brixen, Eddy B. (2008). ENF; Quantification of the Magnetic Field. *Proceedings of the Audio Engineering Society 33rd International Conference,* (pp. 1-6). *Denver, CO, USA*, *2008 June 5-7.*

[11] Cooper, Alan J. (2008). The Electric Network Frequency (ENF) as an aid to Authenticating Forensic Digital Audio Recordings – an Automated Approach. *Proceedings of the Audio Engineering Society 33rd International Conference,* (pp.1-10). *Denver, CO, USA, 2008 June 5-7*

[12] Sanders, Richard W. (2008). Digital Audio Authenticity Using the Electric Network Frequency . *Proceedings of the Audio Engineering Society 33rd International Conference,* (pp.1-11). *Denver, CO, USA, 2008 June 5-7*

[13] Cooper, Alan J. (2009). An Automated Approach to the Electric Network Frequency (ENF) Criterion: Theory and Practice, *International Journal of Speech Language and the Law*, 16 (2), 193-218.

[14] Grigoras, C., Cooper, A.J.,Micha£ek, M. (2009). Forensic speech and audio analysis working group best practice guidelines for ENF analysis in forensic authentication of digital evidence. *Proceedings of the Forensic Speech and Audio Analysis Working Group*, (pp.1-10). *ENFSI FSAAWG Steering Committee on June 2nd, 2009.*

[15] Huijbregtse, M., Geradts, Z., (2009). Using the ENF Criterion for Determining the Time of Recording of Short Digital Audio Recordings, *Netherlands Forensic Institute,* 001, 1-8.

[16] Grigoras. C. (2009). Applications of ENF Analysis in Forensic Authentication of Digital Audio and Video Recordings, *Journal of the Audio Engineering Society,* 57 (9), 643-661.

[17] Micha£ek, M. (2009). The Application of Power-Line Hum in Digital Recording Authenticity Analysis. *Problems of Forensic Sciences,* LXXX, 355-364.

[18] Koenig, B., Lacey, D. (2009). Forensic Authentication of Digital Audio Recordings. *Journal of the Audio Engineering Society,* 57 (9), 662-695.

[19] Rodríguez, D.P.N., Apolinário, J.A., Biscainho, L.W.P. (2010). Audio Authenticity: Detecting ENF Discontinuity with High Precision Phase Analysis. *Institute of Electrical and Electronic Engineers,* 5(3), 534-543.

[20] Smith, J. (2010). Building a Database of Electric Network Frequency Variations for use in Digital Media Authenticity. *Presentation at the American Academy of Forensic sciences. 2010 Seattle, WA Conference.*

[21] Grigoras, C. (2010). Statistical Tools for Multimedia Forensics. *Proceedings of the Audio Engineering Society,* (pp.27-31). *39th International Conference, Hillerød, Denmark.*

[22] Grigoras, C., Smith, J., Jenkins, C. (2011). Advances in ENF Database Configuration for Forensic Authentication of Digital Media. *131st Audio Engineering Society Convention*, 4892, 1-6.

[23] Cooper, A.J. (2011). Further Considerations for the Analysis of ENF Data for Forensic Audio and Video Applications. *International Journal of Speech, Language, and the Law,* 18 (1), 99-120.

[24] Hewlett Packard. (1997). *Fundamentals of Quartz Oscillators* (Application Note 200-2 Electronic Counters Series) Englewood, CO: Test and Measurement Call Center.

[25] Lombardi, M.A. (2010). How Accurate is a Radio Controlled Clock? *National Institute of Standards and Technology Horological Journal*, 2429, 108-111.

[26] National Institute of Standards and Technology. (2011). Time and Frequency Services: Time Scales. Retrieved September 9, 2011 from the NIST website: http://www.nist.gov/pml/div688/grp50/timescales.cfm

[27] National Institute of Standards and Technology. (2002). *NIST Time and Frequency Services* (NIST Special Publication 432, 2002 edition) Boulder, CO: US Department of Commerce.

[28] National Institute of Standards and Technology. (2005). *NIST Time and Frequency Radio Stations: WWV, WWVH, and WWVB* (NIST Special Publication 250-67) Boulder, CO: US Department of Commerce.

[29] National Institute of Standards and Technology. (2001). *NIST Time and Frequency Broadcasts from Radio Stations WWVB, WWV, and WWVH* (NCSL International Workshop and Symposium) Boulder, CO: US Department of Commerce.

[30] National Institute of Standards and Technology. (2009). *WWVB Radio Controlled Clocks: Recommended Practices for Manufacturers and Consumers* (NIST Special Publication 960-14, 2009 edition) Boulder, CO: US Department of Commerce.

[31] National Institute of Standards and Technology. (2011). Time and Frequency Services: Time Scales. Retrieved September 11, 2011 from the NIST website: http://www.nist.gov/pml/div688/grp40/its.cfm

[32] Lombardi, M.A., Nelson, L.M., Novick, A.N., Zhang, V.S. (2001). Time and Frequency Measurements Using the Global Positioning System. *National Institute of Standards and Technology Cal Lab Journal*, 1424, 26-33.

[33] Lombardi, M.A. (2008). The Use of GPS Disciplined Oscillators as Primary Frequency Standards for Calibration and Metrology Laboratories. *National Conference of Standards Laboratories Journal*, 3 (3), 56-65.

[34] Lombardi, M.A. (1999). Traceability in Time and Frequency Metrology. *National Institute of Standards and Technology Cal Lab Journal*, 1305, 33-40.

[35] McDermott-Wells, P. (2005). What is Bluetooth? *Journal of the International Electronics and Electrical Engineers*, 0278-6648 (04), 33-35.

[36] Merriam-Webster Dictionary (11th ed.). (2003). New York: Merriam-Webster.

[37] History of Crime Scene Investigation. (2011). ehow. Retrieved July 20, 2011 from the Ehow website: http://www.ehow.com/about_5371617

[38] History of Crime Scene Investigation. (2011). ehow. Retrieved July 20, 2011 from the Ehow website: http://www.ehow.com/about_5920263

[39] Tales From the Practice of Medicine: Ancient Chinese Forensic Medicine. (2011). Pure Insight. Retrieved July 20, 2011 from the Pure Insight website: http://www.pureinsight.org/node/1517

[40] Visable Proofs: Forensic Views of the Body. (2011). Galleries. Retrieved July 20, 2011 from the National Library of Medicine website: http://www.nlm.nih.gov/visibleproofs

[41] Federal Rules of Civil Procedure. (2010). United States Federal Law.

[42] Case Law. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

[43] Case Law. Frye v. United States, 293 F. 1013. (1923).

[44] Strengthening Forensic Science in the United States: A Path Forward (2009). National Academy of Science. Retrieved August 1, 2011 from the National Academy of Science website: http://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf

[45] The Forgotten Victim of Mckie Case, Whose Killer Remains Free (2007). The Scotsman. Retrieved August 5, 2011 from the Scotsman News website: http://www.scotsman.com/shirley_mckie_fingerprint_case_1_1813034

[46] David Grieve Quote From Testimony. (1997). *Byron Mitchell v. the United States of America,* 96-407-1. (pp. 34).

[47] Mistaken Identity: Brandon Mayfield (2008). Where is Your Data? Retrieved August 5, 2011 from the Where is Your Data website: http://whereismydata.wordpress.com/2008/08/03/mistaken-identity-brandon-mayfield/

[48] Know the Cases: David Shawn Pope (2007). Innocence Project. Retrieved September 7, 2011 from the Innocence Project website: http://www.innocenceproject.org/Content/David_Shawn_Pope.php

[49] Forensic Report. (2011). National Institute of Criminalistics Expertise, 10753/1/2008. Bucharest, Romania.

[50] Forensic Report. (2011). National Institute of Criminalistics Expertise, 6367/2/2010. Bucharest, Romania.

[51] Forensic Report. (2009). *Alin Nicolae Zevedeanu v. Romania*, SRI 1067339, (1-3).

[52] Setback for Steele's Bid to Challenge FBI Tapes (2011). The Spokesman. Retrieved September 7, 2011 from the Spokesman website: http://m.spokesman.com/stories/2011/apr/21/setback-steeles-bid-challenge-fbi-tapes

[53] The History of Phrenology (2008). Phrenology. Retrieved September 9, 2011 from the Phrenology website: http://www.phrenology.org/intro.html

[54] The Forensic Academy (2011). Locard's Exchange Principle. Retrieved September 9, 2011 from the Forensic Academy website: http://www.theforensicacademy.com/forensic.htm

[55] The Watergate Report (2010). Watergate and Forensic Audio Engineering. Retrieved October 29, 2010 from the Audio Engineering website: http://www.aes.org/aeshc/docs/forensic.audio/watergate.tapes.introduction.html

[56] Blauert, Jens. (1997). *Spatial Hearing – Revised Edition: The Psychophysics of Human Sound Localization.* Massachusetts: The MIT Press.

[57] Brixen, Eddy. (2011). *Audio Metering Measurements, Standards, and Practice.* United Kingdom: Focal Press.

[58] Audio Engineering Society (2007). AES Recommended Practice for Forensic Purposes – Managing Recorded Audio Materials Intended for Examination. Retrieved November 12, 2010 from the Audio Engineering website: http://www.aes.org/publications/standards/preview.cfm?ID=29

[59] Scientific Working Group on Digital Evidence (2008). SWGDE Best Practices for Forensic Audio v1.0. Retrieved May 5, 2011 from the SWGDE website: http://www.swgde.org/documents/current-documents

[60] How AC Electricity Works (2010). How Stuff Works. Retrieved October 2, 2011 from the How Stuff Works website: http://science.howstuffworks.com/electricity5.htm

[61] Pohlmann, Ken. (2005). *Principles of digital audio.* New York: McGraw-Hill.

[62] International Telecommunication Union. (1996). *Definitions and Terminology for Synchronization Networks* (ITU-T Recommendation G.810) Helsinki, Finland: World Telecommunication Standardization Conference.

[63] Power Outages Reported in Southern California, Arizona, Mexico (2011). CNN. Retrieved September 18, 2011 from the CNN website: http://news.blogs.cnn.com/2011/09/08/extensive-power-outages-reported-in-southern-california

[64] Wide Power Failure Strikes Southern Brazil (1999). The New York Times. Retrieved September 18, 2011 from the NYT website: http://nytimes.com/1999/03/12/world/wide-power-failure-strikes-southern-brazil.html

[65] North American Electric Reliability Corporation. (2011). *Balancing and Frequency Control* (Technical Document 01262011) Princeton, NJ.

[66] World Record Bluetooth File Transfer (2004). Deep Green Crystals. Retrieved October 2, 2011 from the Deep Green Crystals website:http://www.deepgreencrystals.com/archives/2004/08/world-record-bl.html

[67] Reddy, V.S., Rijutha, K., Ramani, K.S., Mohammad Ali, S.K. Reddy, C.H.P. (2010).Wireless Hacking – A Wi-Fi Hack by Cracking WEP. *Journal of the Institute of Electronic and Electrical Engineers,* V-I, 189-193.

[68] Zhong, Z., Xu, C., Billian, B.J., Zhang, L., Tsai, S.J.S., Conners, R.W., Centeno, V.A., Phadke, A.G., Liu, Y. (2005). Power System Frequency Monitoring Network (FNET) Implementation. *Journal of the Institute of Electronic and Electrical Engineers,* 20 (4), 1914 – 1921.

[69] Liu, Y. (2006). Panel on Current and Prospective Applications of Phasor Measurement Devices in Power System Dynamics. *Educations Committee and Power Systems Dynamics Committee Panel Session Paper*, (pp.1-8).

[70] Zhang, Y., Jia, C., Yuan, Z., Xia, T., Zhang, G., Liu, Y. (2010). Magnetic Field Based Phasor Measurement Unit for Power Grid Frequency Monitoring. *Journal of the Institute of Electronic and Electrical Engineers,* 1 – 6.

[71] Chen, L., Markham, P., Chen, C., Liu, Y. (2011). Analysis of Societal Event Impacts on the Power System Frequency using FNET Measurements. *Journal of the Institute of Electronic and Electrical Engineers.* 1 – 8.

[72] International Centre for Settlement of Investment Disputes Tribunal Report (2009). ICSID Case No. ARB/05/13. EDF Limited vs. Romania. pp. 66.

[73] Who is Lying? (2011). Lumea Justitiel. Retrieved November 15, 2011 from the Lumea Justitiel website: http://www.luju.ro/institutii/inec-inm/cine-minte-un-expert-inec-a-declarat-in-instanta-sub-juramant-ca-intre-institut-si-dna-s-a-incheiat-un-protocol-pentru-efectuarea-de-expertize-noul-director-al-inec-procurorul-ceort-neaga-oficial-existenta-protocolului

[74] Romania Must Take into Account the ECHR (2011). Lumea Justitiel. Retrieved November 15, 2011 from the Lumea Justitiel website: http://www.luju.ro/institutii/inec-inm/romania-trebuie-sa-tina-cont-de-cedo-in-materia-expertizelor-criminalistice-in-cauza-prepelita-vs-moldova-s-a-statuat-daca-statul-e-parte-in-proces-expertizele-nu-pot-fi-facute-de-institutii-ale-statului-ci-de-experti-independenti