

## Arcadio Nova Forensic Report

### NOVA CASE OVERVIEW

On February 3, 2022, eForensix was contacted by Craig Leeds, Esq., attorney for Arcadio Nova, hereafter defendant, for a petition on a post-conviction relief (PCR). The defendant was arrested on July 16, 2013 and the Passaic County Prosecutor's Office, hereafter PCPO, confiscated his cellphone at that time.

eForensix agreed to review the case and assess the matter for the PCR. eForensix provided Mr. Leeds with our findings regarding the testimony of the state's expert, Henry Hernandez, and the forensic analysis he performed.

On pages 144 through 145 of the trial transcript dated July 24, 2015, Mr. Hernandez opined that the video in question, 20130703\_200929.MP4, which the PCPO had proffered to have been a video of a sex act between the defendant and the minor victim, was created on July 3, 2013, and was the 29<sup>th</sup> video of the day. Mr. Hernandez also stated he was unsure of the date that the video was deleted. However, he was incorrect, as the naming convention does not identify how many videos were created on any specific day.

The naming convention shows that the video file was created on July 3, 2013, at 20:09:29 (Military Time), which is 8:09:29 PM. The naming convention for this cellphone is YEAR, MONTH, DAY\_HOUR, MINUTES, and SECONDS. The underscore separates the date from the time the file was created. This naming convention has been an industry standard for almost two decades. I believe a forensic examiner with six years of experience working in a forensic lab for a law enforcement agency should have been familiar with the aforementioned naming convention, as well as military time and, therefore, have been able to determine the time of the video, which was a critical component of this case.

### INITIAL STEPS

eForensix sought access to the forensic image of Mr. Nova's cellphone, created by the Passaic County Prosecutor's Office. eForensix arranged a time to pick up the image at the PCPO on March 29, 2023. I drove to the PCPO on King Road in Totowa and took possession of what I believed to be the forensic image of Mr. Nova's cellphone.

However, when I viewed the material provided, it was a PDF report containing limited information from Mr. Nova's cellphone. When I followed up with the PCPO, they stated that they no longer had the forensic image of Mr. Nova's cellphone.

The PCPO then requested that eForensix image the cellphone. eForensix arranged a date and time to conduct the imaging. When I arrived at the PCPO in Totowa, NJ, I was advised that they did not have the unlock code, so I could not image the cellphone. I informed the PCPO that I needed to test on a similar cellphone before attempting to unlock the defendant's cellphone forcibly. I did not want to unintentionally destroy potential evidence.

I returned to eForensix's lab in Fairfield, NJ and conducted a series of tests on a similar cellphone I had purchased. I attempted a forcible unlock, which I could not complete successfully. I then notified the PCPO that I could not image Mr. Nova's cellphone because the only way to unlock the cellphone would be to use the premium edition of Cellebrite, which is only available to law enforcement in criminal cases.

The PCPO agreed to image the cellphone using Cellebrite Premium. On August 7, 2023, eForensix purchased a 2TB (terabyte) hard drive and dropped it off at the PCPO. On August 25, 2023, eForensix picked up the 2TB hard drive from the PCPO, which contained the Cellebrite forensic image of Mr. Nova's cellphone.

#### **FORENSIC ANALYSIS OF THE CELLPHONE IMAGE**

I accessed the forensic image of the defendant's cellphone using Cellebrite Physical Analyzer, version 8.6.100.63. I identified 113 images of child pornography created on May 19, 2013, and all were located in a cache folder. When I reviewed each photo, I noted only 38 unique poses. However, while the MD5 hash values showed all the photos as unique files, it was due to how the Samsung operating system creates cached thumbnail photos.

When images are created on a cellphone, thumbnail images are typically made simultaneously and located in a cache folder where these images were found. However, in this case, the original photos were not recoverable. It should be noted that all of the 113 aforementioned photos of child pornography, which were the only child pornography photos found on the defendant's cellphone, were not accessible to the defendant because they were only located in the cache folder. It is only possible to determine how the original files arrived on the cellphone by knowing what folder they were located in before they were deleted.

On pages 158 through 159 of the trial transcript dated July 24, 2015, Mr. Hernandez opined that he could not determine how the files were placed on the defendant's cellphone. He stated, "It is impossible for me to know exactly where they came from."

eForensix purchased another cellphone that matches the defendant's exact make and model, a Galaxy S III SGH-T999, for testing to identify where specific data types are stored and to determine if data in cached areas of the cellphone are accessible to the user. As a result of our



testing, I determined that child pornography files identified on the cellphone in the cached folders were not accessible to the cellphone user.

I searched the cellphone using 154 keywords typically associated with child pornography cases and the search yielded zero hits. These included but were not limited to keywords such as pthc, stickam, babyshivd, Lolita, hussyfan, pedobear, kiddy porn, jailbait, prepubescent and @raygold.

I did not identify any artifacts that showed the cellphone user was searching for child pornography websites or known child pornography pictures. It is my opinion, within a reasonable degree of computer forensic certainty, that this phone was not used to search for child pornography. However, I did identify adult pornography artifacts in search history, web history, and media.

Based on my 35 years of experience, individuals involved in searching for and viewing child pornography have these files on more than one device, have hundreds and even thousands of illegal images on their devices, and they often include tens and even hundreds of different children, none of which were present on this single device.

#### **FORENSIC ANALYSIS OF VIDEO 20130703\_200929.MP4**

The video file 20130703\_200929.MP4 became an essential part of the case for two specific reasons. First, in Detective Danielle D'Annibale's affidavit dated October 17, 2013, pages 9 through 10, Detective D'Annibale wanted to search for "any video recordings/images of SL recorded contemporaneously when Arcadio Nova [allegedly] sexually assaulted SL", believing that the suspect made a video of the incident.

Second, on page 4 in the transcript of the pretrial proceedings dated July 1, 2015, Ms. Saltiel stated: "I then was notified shortly thereafter that the State was going to be seeking to admit an excerpt from the forensic report which they proffered to contain a – so the file, having been deleted, their proffer, my understanding, at least, is that it was created on July 3<sup>rd</sup>, 2013, the date of the incident, and that it was deleted on that date."

I located the video file named 20130703\_200929.mp4, identified in the prior paragraph, and confirmed that it was a zero-byte file, meaning the file no longer contained the video contents. This can happen when a file is deleted and then overwritten by new data saved to the cellphone.

According to Detective Danielle D'Annibale's affidavit dated October 17, 2013, she stated on page 7: "According to Ms. Montoya, SL was downstairs with the man from Direct TV for approximately 3 minutes when Ms. Deleon started screaming her name." According to Detective D'Annibale's affidavit, they looked for the man from Direct TV, but he left the scene without his tools.

At the pretrial proceedings held on July 7, 2015, the court asked Hernandez on page 16: "if the crime alleged in this indictment occurred approximately 7 PM or a few minutes after that, you have no way of knowing what time that was created, is that right?" Mr. Hernandez answered, "That is correct". The court was referencing the video named 20130703\_200929 .mp4, which the prosecutor's office apparently believed to be a sex act between the defendant and SL.

On page 144 of the trial transcript dated July 24, 2015, Mr. Hernandez opined that the file had been created on July 3, 2013 and was the 29<sup>th</sup> video created that day. He correctly identified the first portion of the file name, but was incorrect on what he stated regarding the file name after the underscore, where he opined that it was the 29<sup>th</sup> video of that day. He ignored the number 2009 and only mentioned the last two digits in the file name, 2 and 9, which he used to support his opinion on it being the 29<sup>th</sup> video of the day. The actual breakdown of the file name is as follows: YEAR, MONTH, DAY\_HOUR, MINUTES, SECONDS. The \_200929 is military time and is 8:09:29 PM, local time.

Mr. Hernandez stated that he worked in the forensic laboratory for six years, and I believe he should have known what \_200929 represented. He also works with a law enforcement agency whose reports typically use military time. As an example, a letter from Detective Danielle D'Annibale dated July 10, 2013, to Internal Affairs of the Paterson Police Department uses 18:00 and 21:00, which is 6 PM and 9 PM, respectively.

Mr. Hernandez's incorrect explanation of these numbers, date, and time likely led the court and jury to believe that the defendant created the video at the scene of the crime and that the deleted zero-byte video, which was an empty file recovered forensically, was the video of a sex act between the defendant and SL. However, this video file was created well after the defendant left SL's home.

Based on the naming convention of the file 20130703\_200929.mp4, the file was created on July 3, 2013 at 8:09:29 PM. According to statements by Detective D'Annibale in her affidavit dated October 17, 2013, and Dulse Maria DeLeon's in-court testimony on July 1, 2015, on pages 13 through 14, the defendant arrived at the home at approximately 7 PM. She started looking for SL after 3 to 4 minutes, and the defendant subsequently left the house.

That being the case, the recovered video had nothing to do with SL or the crime scene, as it was created more than an hour after the defendant allegedly left the scene. Additionally, after a review of the forensic image of the defendant's cellphone, this was not the 29<sup>th</sup> video created that day but, instead, was the only video created that day. Mr. Hernandez could have counted the videos to support his conclusions but did not take additional steps to ensure his findings were correct. eForensix counted only one video file created on July 3, 2013, the deleted zero-byte file created well after the defendant left SL's home.

The video file contained no metadata, whether file system or EXIF, and only the date and time are identified in the file name 20130703\_200929.mp4. Therefore, there is no way to tell if the video was accessed after it was created and when it may have been deleted. Nonetheless,



during court proceedings, it was proffered to have been deleted on July 3, 2013. However, the state's own expert, Mr. Hernandez, stated he did not know when the zero-byte file was deleted.

Again, the proffer to the court that the video file was deleted on the same date it was created likely led to the assumption that there was a coverup and made the presence of the empty file appear nefarious when it had nothing to do with SL or her home.

The file 20130703\_200929.mp4 could have been deleted on July 3, 2013, and it could have been deleted up to and including the day of the defendant's arrest. Files are marked deleted on or after the file's last accessed date, which Cellebrite did not recover in the forensic image.

Based on the date and time of the file, the file name, police reports, and court documents, within a reasonable degree of computer forensic certainty, this file had nothing to do with SL or her home, as it was created well after the defendant left SL's home. Yet it was proffered using an expert who did not correctly characterize and interpret the file name to determine the military time. This should have been evident to the expert, detectives, and the prosecutor as the time followed the date in the file name (20130703\_200929.mp4).

#### **FORENSIC ANALYSIS OF DC PICTURES**

eForensix identified 113 DC pictures in the forensic image of the defendant's cellphone, all located in the cache. However, while all of the MD5 hashes were unique, there appeared to be numerous duplicates due to the creation of the same picture in different sizes created by the cellphone operating system or application(s).

An approximate count based on the subject's pose (child) in each photo revealed 38 unique photos. It appears that the cellphone's operating system or one of its applications created numerous cached files of each photo in different sizes, which resulted in a count of 113 photos.

According to police reports and court documents, the pictures do not contain SL's likeness, and the child depicted in the photograph is unknown. During pretrial proceedings on July 7, 2015, on page 18, line 12 through page 19, line 11, Mr. Hernandez opined that he did not know where the pictures originated or how they were placed on the cellphone. In fact, under cross-examination, Mr. Hernandez was asked whether or not he knew if the photos were taken with Mr. Nova's cellphone. He answered, "I do not know where they came from. I explained that they were in a folder, which is an image cache folder. I don't know the original source of it".

After a review of these photos, it is my opinion, within a reasonable degree of computer forensic certainty, that these images were not taken with Mr. Nova's cellphone. It is more likely that they were obtained from another source. However, without knowing the path of the original photos as opposed to just the thumbnails, which have less size and resolution, it is impossible to be sure where the images came from, as articulated by the state's expert.

### REVIEW OF MR. HERNANDEZ'S CURRICULUM VITAE

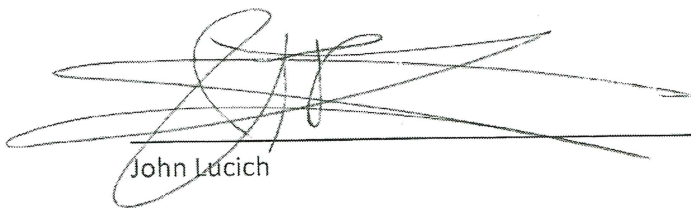
I reviewed Mr. Hernandez's Curriculum Vitae, hereafter CV. It is my understanding that this is not his resume from the time of the trial, but rather, post-2019. Mr. Hernandez listed the following:

- Setup computers throughout the office and provide troubleshooting and desktop support throughout the office.
- Use forensic tools to recover data from computer hard drives, cellphones and other electronic and digital sources to assist in the investigations of crimes in which these devices may have played a role.
- Prepare detailed reports describing the process used to examine the evidence which may be used in the prosecution of the case.
- Testifying in court when necessary regarding what part I played in the investigation.
- Prepare presentation materials for trial such as maps and charts.
- Deploy surveillance equipment used for tracking and monitoring suspect(s) believed to be involved in criminal activity.
- Create and maintain FileMaker Pro databases.
- Setup and maintain the office website.
- Retrieve surveillance footage from DVR systems throughout the county.

Mr. Hernandez lists his skills in a separate section, but none are related to digital forensics. He lists Cellebrite under his licenses and certifications but nothing else; no actual dates are provided for his Cellebrite training, and no licenses are actually listed in the license category. Therefore, I cannot determine if Mr. Hernandez received Cellebrite training before or after he testified as an expert in this case. Also, he states that he has experience collecting evidence from hard drives but does not list any software or certifications he has used to image and analyze hard drives.

After reviewing Mr. Hernandez's testimony and CV, I noticed that Mr. Hernandez had numerous responsibilities that have nothing to do with digital forensics, including but not limited to website design and maintenance, databases, troubleshooting computers, installing computers, retrieving surveillance footage, and deploying tracking devices.

It appears that Mr. Hernandez's expertise was not digital forensics but rather performed numerous duties unrelated to this area of expertise. Based on my review of the totality of information provided to me in this case, it is my opinion that Mr. Hernandez likely did not have the training and experience to serve as an expert and, therefore, may not have been the best choice to serve as an expert during the investigation and at trial regarding this case.



John Lucich

May 9, 2024



## **John P. Lucich**

John Lucich is retired from the New Jersey Attorney General's Office, Division of Criminal Justice, Organized Crime Racketeering and Corruption Bureau and is currently the President of eForensix, LLC, providing digital forensics consulting services, expert witness testimony, data analysis and hard drive data recovery. Mr. Lucich has been an expert in numerous high-profile cases and has been the subject of numerous media interviews on both radio and television regarding cybercrimes and computer forensics. He has been a repeat guest on the Fox News Shows including; Fox & Friends, Live Desk, Good Day New York, Neil Cavuto, Sean Hannity, Lou Dobbs, Glenn Beck, Mike & Juliet Show. John has also made many appearances on the Nancy Grace Show, Headline News, Jane Velez Mitchell and TruTV (formerly Court TV). Mr. Lucich started cybercrime investigations in 1988 for the New Jersey Division of Criminal Justice and taught cybercrime courses and digital forensics at their academy for more than a decade.

Mr. Lucich is a Forensic Explorer Certified Examiner, Magnet Certified Forensic Examiner, a Certified Data Recovery Professional, a Certified Cellebrite Physical Analyst and a Certified Cellebrite Operator. Mr. Lucich served five years as an adjunct professor of computer science for Felician College and is a nationally recognized expert, lecturer and author on a variety of high tech crime investigations and computer forensics. Mr. Lucich has lectured for special agents of several agencies and was the Keynote speaker with General Colin Powell and Bill Gates at CAWorld96, addressing computer security issues. John worked undercover for the US military helping to identify individuals involved in military computer intrusions and he testified as an e-mail expert during the removal of a New York State Judge who lied about sending an e-mail message to President Bill Clinton. John also testified against a New Jersey police officer as a computer forensic expert during a trial where the police officer was accused of taking a computer as a bribe. The officer was subsequently found guilty and removed from the force.

John Lucich was the first state law enforcement officer to testify before the United States Congress in 1993 on computer crime issues and in 1999 he testified as a high-tech crimes expert witness before the New Jersey State Commission of Investigation during state hearings on computer crimes in Trenton. John has lectured at nationwide conferences and seminars and provided training in the areas of computer forensics, digital investigations, information security and secure infrastructure design.

## **Experience**

eForensix, LLC, 271 Route 46 West, Building G204, Fairfield, New Jersey 07004. Mr. Lucich is the President and founder of eForensix, a computer forensics company providing litigation support for plaintiff and defendant firms as well as for employment law, family law as well as other civil and criminal law cases. The focus of this group is the acquisition and analysis of hard drive for the preservation and recovery of potential evidence for legal proceedings. The company has extensive experience in employment law, family law, unfair competition, sexual harassment, whistle blower cases, trade secret and criminal cases. Mr. Lucich has been involved in cases against police officers, teachers, attorneys and other public officials by providing computer forensic support for their criminal and or civil prosecution. The following is a brief example of some cases Mr. Lucich has been involved in.

- Provided computer forensic services and expert witness services to major corporations, attorneys, municipalities and the New Jersey Office of Attorney Ethics

- Incident Response, Computer Forensics & Analysis. These cases involved both criminal and civil law cases involving theft of trade secrets, family law, unfair competition, network intrusions, pornography in the work place, possession of child pornography, cyber-squatting, sexual harassment and whistle blower statutes
- Provided computer forensic expert services on behalf of the plaintiff during a civil trial in a case involving an alleged rape of a 12-year-old child by her teacher. The case was settled using the forensic report.
- Provided technical assistance with computer forensics during internal investigations for corporate and government clients
- Provided technical assistance with computer audits during internal investigations for corporate clients
- Provided expert testimony on high tech related crimes before the New Jersey State Commission of Investigation in 1999
- Under court order, conducted analysis of a computer system seized from a police officer during a bribery and official misconduct investigation and trial. Subsequently testified at trial as an expert, during which the officer was found guilty. (August 1999)

Office of the Attorney General, Department of Law & Public Safety, Division of Criminal Justice, 25 Market Street, Trenton, New Jersey 08625, served as an investigator in the Organized Crime & Racketeering Bureau. Primary duties included the investigation of criminal activity related to organized crime, as well as high tech crime investigations. Mr. Lucich was the lead computer crime investigator for the State and was responsible for the following:

- July 1990 attended the Federal Law Enforcement Training Center in Glynnco, Georgia for criminal investigations in an automated environment.
- Seized and subsequently conducted forensic analysis of numerous computer systems encompassing several platforms
- Conducted high technology related investigations for crimes which include corporate computer intrusions, homicide, child endangerment, narcotics, telecommunications fraud, electronic benefits transfer fraud, cellular fraud, organized crime activities and the use of explosives and incendiary devices
- Organized and lectured at the first statewide computer crime investigations course for law enforcement in the State of New Jersey. All 21 county prosecutor agencies were in attendance (1990)
- Assisted the United States Military on two occasions in the investigation and identification of individuals responsible for military computer intrusions
- Lectured for the State of Florida in the first terrorism conference that addressed Cyber Terrorism in 1994 entitled "After the Strike"
- Lead investigator conducting forensic analysis of the computer systems seized from Edward J. Leary (AKA New York Subway Bomber), at the request of the New York City Transit Police
- Provided expert testimony before a United States Congressional Sub-Committee investigating high tech related crimes in April 1993  
Lectured at the New Jersey Judicial College on computer crime investigations and computer seizures



- Provided expert testimony on high tech related crimes and electronic mail before the New York State Commission on Judicial Conduct during a hearing for the removal of a New York State Judge in September 1995
- Keynote Speaker for Computer Security Institute (CSI)
- Conducted the first state case of welfare fraud via debit cards in an ATM environment

Felician College, Lodi, New Jersey, served as Adjunct Professor assigned to the Computer Science Department for 5 ½ years. Course lectures include: Introduction to Computer Science, Database Management Systems, Systems Analysis & Design, Introduction to Assembly Language, Introduction to Pascal, and Management Information Systems.

Fairfield Township Police Department, Fairfield, New Jersey, served as a Patrolman. Mr. Lucich was responsible for the enforcement of state criminal statutes, motor vehicle statutes and local ordinances.

### **Education**

Jersey City State College, Jersey City, New Jersey, 1991. Master of Science.  
Fairleigh Dickinson University, New Jersey, 1987. Bachelor of Arts

### **Aviation Licenses**

Sea Plane Pilot  
 Commercial Pilot  
 Certified Flight Instructor  
 Airline Transport Pilot

## **Prior Testimony**

Amer vs Amer (Morris County, NJ)

FV 14-27-21

Testimony – September 15, 2020

Estate of George Jaye, Deceased (Union County, NJ)

R-3715 (Chancery Division)

Testimony – April 1, 2019

United States vs. Richard Adebayo (Federal Courthouse, Newark, NJ)

19-68 (MCA)

Testimony – June 17, 2019

Mooney vs Mooney (Union County, NJ))

FV20-93-1

Testimony – October 24, 2016

Santa Mallon vs. Hudson City Savings Bank et al (Bergen County, NJ)

BER-L-466-13

Testimony – May 17, 2016

James Cariffi vs. Township of Parsippany (Morris County, NJ)

MRS-L-2938-11

Testimony – November 5, 2015

Spectraserve, Inc. vs. Middlesex County Utilities Authority, et al (Middlesex County, NJ)

Expert for Judge Travis L. Francis

MID-L-002577-07

Testimony – June 2013

State of New Jersey vs. Charles K. Zisa (Bergen County, NJ)

Bergen County, Indictment No. 10-10-01812

Testimony – April 2012

State vs. David Webb (State's Expert) (Somerset County, NJ)

Indictment No. 98-08-00410-I

Testimony – August 1999



New Jersey State Commission of Investigation  
Trenton, New Jersey  
Testimony – 1999 (Cybercrime)

NY State Commission on Judicial Conduct vs. B. Marc Mogil a Judge of the County Court,  
Nassau County  
Testified for NY State Commission on Judicial Conduct in 1995  
Judge Mogil was removed from the bench

United State Congress, United States Capitol  
Representative Edwin Markey's Committee  
Testimony – 1993 (Cybercrime)