VESTIGE
Digital Investigations

Digital Forensic Analysis

Report of Findings

Case: OH v Mendoza

Examiner: Chris Mammarella

Audience: Phillip Mendoza

May 6, 2024

Vestige Ltd
23 Public Sq., Ste. 250
Medina, OH 44256-2284
330.721.1205 / 800.314.4357
Fax: 330.721.1206
www.VestigeLtd.com

Turning Digital Evidence into Intelligence™

DEFENDANT'S
EXHIBIT
C

NOTICE

This report is confidential and is intended only for Phillip Mendoza and its legal counsel, Donald Malarcik. If you are not the intended recipient of this document, any use, dissemination, distribution or copying of this document or its contents is strictly prohibited. The information contained in this document may also be privileged and/or subject to the attorney work-product protection.

The included information in this Report of Findings is <u>not</u>, nor should be considered, a legal opinion. It is merely the results from our investigation and may be incomplete due to evidence having not been provided to Vestige. The reader must be aware that these results may not include all exculpatory and inculpatory evidence if it has not been provided.

Additionally, this report and its content may only be used by Phillip Mendoza for the purposes of this case (OH v Mendoza). No portion, in whole or in part, may be duplicated and/or used for any other purposes without the express written permission of Vestige Ltd.

Table of Contents

OVERVIEW

Objective

Pursuant to the request of Donald Malarcik, I have forensically examined multiple items related to a CyberCheck report provided as evidence in this case. At issue is the repeatability and accuracy of the claims made in the CyberCheck report.

BACKGROUND

Evidence

Vestige relied on only the specific data identified in this report in order to form its opinion.

- CyberCheck Report with case reference 20 097360

FINDINGS

Review of the Mendoza Discovery and Search Warrants

In reviewing the Akron Police Department Report of Investigation, record 20-097360, I analyzed the use of the Cybercheck information. Cybercheck claims to use Open Source information to provide location data of a specific Cyber Profile, at an approximate time. It is represented that this Cyber Profile is compiled from multiple responsive results from Open Source data and then placed in a spreadsheet. The data within the spreadsheet is created after receiving the "Request for Intelligence" or "Ask". This spreadsheet is identified as "master_supply_chain_templater.csv"(MSCT). The fields for the master_supply_chain_templater.csv are listed in Appendix A.

The MSCT contains the responsive information located within Open Source sites, but does not list the source of the information so that the information gathered can be verified. The MSCT is then used to populate the fields within the Cybercheck report. The information within the MSCT also does not advise how this Open Source data is associated with the individual's Cyber Profile. The MSCT is missing information like the type of mobile device that is associated with the Cyber Profile such as if the mobile device is an Apple or Android device and the associated MAC address of the mobile device. This information is important because more than one individual can use a mobile device to log into email, social media accounts and other items that can be a part of a "cyber profile." The resulting situation could allow multiple cyber profiles to exist on one device, transmit its data to a wireless router and subsequently be picked up by a CyberCheck report. Multiple phone numbers can be listed within the MSCT, but the MSCT does not identify which number is associated with the mobile device which connected to the wireless router and transmitted components of a cyber profile. The source information of all of the responsive data found within the MSCT, would be the bare minimum of what is needed to verify the results. An explanation of how the data is associated with the Cyber Profile is lacking and is instrumental in trying to verify the data.

Use of the Cybercheck Information

Within the Akron Police Department Report of Investigation, it references Cybercheck identifying that the cyber profile of Phillip Mendoza was in the area of the homicide at a probability of 93.13%. This report could have been used as a tip to get warrants to validate that information.

According to the Akron PD report, Sprint was the carrier for Mendoza's phone. Also, according to the Akron PD report, the Sprint carrier did not record location data for Mendoza's phone. This data would have consisted of Call Detail Records of the cellular towers used during the time period of the homicide. Call Detail Records have been tested and are accepted within the law enforcement and forensic community.

A warrant was issued for the Geo-Fence data from Google. A Geo-Fence is a virtual perimeter for a real-word geographic area. From the multiple Geo-Fence cases I have worked, the data for the Geo-Fence is collected from the mobile device, from the WIFI the device to which the phone is connected and from GPS data triangulated from the cellular towers. This Geo-Fence data has been tested and accepted within the law enforcement and forensic community. According to the Akron PD report, the Google Geo-Fence data requested for Mendoza did not provide any useful information.

Without Geo-Fence data or Call Detail Records from Spring, the location information provided in the CyberCheck report cannot be validated.

Intelligence Bulletin #1

The CyberCheck Report lists the "Full profile of Phillip Mendoza" at or near 1228 5th Avenue, Akron, OH 44306 based on a MAC address of a router collected from an Open Source. The CyberCheck report displays a +/- of 10 meters, next to the MAC address. The Open Source information of where this data was collected was not listed in the report. The Akron Police Department could have used this information as a tip and used warrants on the households within that perimeter.

The Cybercheck report does not indicate what part of the Cyber Profile connected with the wireless router. A warrant would need to have been issued to validate this data. The router is owned by a person or a business. Data within a privately-owned router is considered private. The Open Source data used should have been legally obtained, due to privacy laws. The CyberCheck report also lists a total of 11 cyber profile hits with this wireless router. The Open Source information of where the 11 hits of data was located is also not listed. This data would be needed to validate the results.

Identical Reports for Different Days

Vestige was provided by counsel the CyberCheck report issued in this case. To be specific two CyberCheck reports were issued for this case. The reports are attached as Exhibit 2 and Exhibit 3 to this report

Adam Mosher has testified and represented, that the creation of a CyberCheck report is an automated process. Once a licensed law enforcement agency submits an "ask" while logged into the CyberCheck portal, the automated process begins and no further human action occurs through the creation of the CyberCheck report.

Exhibit 2 and Exhibit 3 represent identical reports. The reports list the same accuracy, cyber profiles and intelligence bulletins, MAC Addresses and SSIDs. There is only one difference between the reports. Exhibit 2 has a date of August 2, 2020 in the Overview section (which has been represented as the "ask") as well as in Intelligence Bulletin #1 and Intelligence Bulletin #2. Exhibit 3 has a date of August 20, 2020 in the Overview section, Intelligence Bulletin #1 and Intelligence Bulletin #2.

If both CyberCheck reports are taken as being authentic CyberCheck reports, the CyberCheck system is stating that there is a 93.13% probability that Philip Mendoza's cyber profile was at or near 1228 5th Avenue, Akron, OH 44306 on both August 2, 2020 and August 20, 2020 between 9:00 PM and 9:15 PM Eastern Time. Of even more coincidence is that the number of cyber profile hits present on wireless routers at this location is identical on both days, at the same time each day.

CONCLUSIONS AND OPINIONS

Based on the evidence in this report, Vestige holds the following opinions to a reasonable degree of scientific certainty. Should additional evidence come to light. Vestige reserves the right to review that evidence and change its opinions if warranted.

1. The fact that the Cybercheck system produced a location of a Cyber Profile, when two proven and accepted methods did not record location data, calls into question the accuracy of the report. The Sprint carrier data and the Google Geo-Fence data would have been used for validation purposes. No source data is listed in order to the validate the Open Sources used.

2. The reporting of a router MAC address in the Cybercheck report is insufficient to verify that a mobile device connected to the router. The device that connected to the router is not listed in the report. The Open Source of the collected data is also not displayed for validation.

3. The wireless router data should have been verified though a warrant. The router was personally owned or owned by a business. The location of the router would have been within a household. Use of this data from an Open Source, should have been legally obtained, due to privacy laws.

4. The MSCT lacks source information and verified data, such as the mobile device associated with the Cyber Profile. The MSCT also lacks how the responsive data associates with the Cyber profile.

5. Without the source data or preservation of the source data, at the time of the MSCT was created, there is no way to validate the results at a later date.

6. The creation of two CyberCheck reports with identical results that were 18 days apart, brings into questions the accuracy of the reports. It is implausible that the same wireless router connected to the same cyber profile at the same time of day, 18 days later.

Chris Mammarella, EnCE
Vestige Digital Investigations

MISCELLANEOUS

This report and the opinions expressed herein are based upon the facts and knowledge at the time of its creation. Should additional facts come to light, those may affect the opinion and should be brought to Vestige's attention for consideration.

Statement of Independence

Vestige Ltd and its employees, including myself, serve as independent, neutral experts. We do not have, nor anticipate, any special relationship with any of the parties in this matter, nor any of the parties' counsel.

Compensation

The analysis and writing of this Expert Report are not contingent on our findings or the outcome of our analysis. Vestige Ltd is compensated based on costs for flat fee projects or for the time expended on completing the analysis and writing of this Report. When billed hourly, Vestige Ltd is compensated at a rate of $275.

Qualifications of Expert

Exhibit 1 is a complete and accurate copy of my Curriculum Vitae, which includes my qualifications as a Digital Forensic Expert as well as publications and Expert Witness work performed.

APPENDICES

Appendix A – Fields for master_supply_chain_template.csv

1. CaseNumber
2. ACES Viewed Contents
3. ESP Viewed Contents
4. Briefing
5. Online Communications
6. Profile Strength
7. Suspect
8. Suspect DOB
9. Employment
10. Suspect Online Aliases
11. Suspect Profile
12. Country
13. State
14. Regional Coordinates
15. Suspect Current Location
16. Distribution Gateway
17. Trade Corridor
18. Supply Chain Position
19. Suspect Email Addresses
20. Suspect Risk Rating
21. Suspect Cyber DNA
22. Top Three Relatives
23. Top Three Associates
24. Related URLs
25. Victim
26. Victim DOB
27. Victim Online Aliases
28. Victimology
29. Country of Victim
30. Victim State
31. Regional Coordinates of Victim
32. Victim Current Location
33. Victim Cyber DNA
34. COPINE
35. Victim Email Addresses
36. Victim Risk Rating
37. Last Known Interaction
38. Regionally Relevant Sex Offenders
39. Magnitude
40. Solvability
41. Technical Identified Risks
42. ProfilePic
43. CaseCreated
44. PhoneData
45. AutoData
46. AdditionalInformation

47. IdentifiedRisks
48. AgencyID

CYBERCHECK

CyberCheck Brief
(Homicide - Locate Suspect(s) at Scene)
Reference Case 20-097360

The purpose of this CyberCheck intelligence briefing is to deliver actionable cyber based intelligence only. CyberCheck follows digital trails for intelligence based on all pieces of data analyzed. This includes emails, phone numbers, geolocations, usernames, connection locations and communication end points. To clarify; a suspect may be using a phone which belongs to their friend but is being used for the suspect's email address.

Parameters Enforced: Geofence based on location and time of homicide (+/- 30 mins).

Overview

Agency: Akron Police Department

Request for Intelligence: Murder Investigation. Occurred at 1232 5th Avenue, Akron, OH, 44306 on 08/02/2020 at 2130 EST. Victim was Tyree Halsell.

Reason: Homicide - Locate Suspect(s) at Scene

Summary

Name:	Phillip Jose MENDOZA
DoB:	05/22/1962
Accuracy:	93.13%

Online Aliases

Phillip Jose Mendoza (Phillip Jose MENDOZA)
Phillip M Mendoza (Phillip Jose MENDOZA)
Phillip Mendoza (Phillip Jose MENDOZA)
Pmendoza205 (Phillip Jose MENDOZA)
Ladypimpjuice625 (Phillip Jose MENDOZA)
Phil Jose Mendoza (Phillip Jose MENDOZA)

DEFENDANT'S EXHIBIT
J

This is provided solely for the Akron Police Department and is classified **confidential**

Cyber Profiles

pmendoza205@gmail.com (Phillip Jose MENDOZA)
Tracking of GoogleID 100626735686768023723
ladypimpjuice625@aol.com (Phillip Jose MENDOZA)

Phone Numbers

(330) 475-9599 (Phillip Jose MENDOZA)
(330) 608-7874 (Phillip Jose MENDOZA)
(330) 459-9599 (reference to Phillip Jose MENDOZA)

Current Geolocations

CyberCheck intelligence highlights communications and / or connections, through the tracking and correlation of cyber assets of timeframe, throughout 2020, for Phillip Jose MENDOZA to the following locations.

184 Reid Terrace, Apartment 103, Akron, OH, 44310 (throughout 2020, 2021 and 2022)

Intelligence Bulletin

INTELLIGENCE BULLETIN #1

MAC ADDRESS
48:00:33:bf:c0:4a (+/- 10 meters)
VENDOR
Technicolor CH USA Inc.
SSID
Woodall5
APPROXIMATE LOCATION
At (or near) at 1228 5th Avenue, Akron, OH, 44306
DATE – APPROXIMATE TIME -- PROFILE HITS
08/02/2020– 2100 EDST (+/- 15 mins) – Total of 7
08/02/2020 – 2115 EDST (+/- 15 mins) – Total of 4
SUPPORTED INTELLIGENCE
Full profile of Phillip Jose MENDOZA

INTELLIGENCE BULLETIN #2

MAC ADDRESS
62:45:b6:c6:08:d0 (+/- 10 meters)
VENDOR
Not Broadcasted
SSID
Not Broadcasted
APPROXIMATE LOCATION
At (or near) at 1228 5th Avenue, Akron, OH, 44306
DATE – APPROXIMATE TIME -- PROFILE HITS
08/02/2020– 2100 EDST (+/- 15 mins) – Total of 3
08/02/2020 – 2115 EDST (+/- 15 mins) – Total of 6
SUPPORTED INTELLIGENCE
Full profile of Phillip Jose MENDOZA

This is provided solely for the Akron Police Department and is classified **confidential**

CYBERCHECK

CyberCheck Brief
(Homicide - Locate Suspect(s) at Scene)
Reference Case 20-097360

The purpose of this CyberCheck intelligence briefing is to deliver actionable cyber based intelligence only. CyberCheck follows digital trails for intelligence based on all pieces of data analyzed. This includes emails, phone numbers, geolocations, usernames, connection locations and communication end points. To clarify; a suspect may be using a phone which belongs to their friend but is being used for the suspect's email address.

Parameters Enforced: Geofence based on location and time of homicide (+/- 30 mins).

Overview

Agency: Akron Police Department

Request for Intelligence: Murder Investigation. Occurred at 1232 5th Avenue, Akron, OH, 44306 on 08/20/2020 at 2130 EST. Victim was Tyree Halsell.

Reason: Homicide - Locate Suspect(s) at Scene

Summary

Name:	Phillip Jose MENDOZA
DoB:	05/22/1962
Accuracy:	93.13%

Online Aliases

Phillip Jose Mendoza (Phillip Jose MENDOZA)
Phillip M Mendoza (Phillip Jose MENDOZA)
Phillip Mendoza (Phillip Jose MENDOZA)
Pmendoza205 (Phillip Jose MENDOZA)
Ladypimpjuice625 (Phillip Jose MENDOZA)
Phil Jose Mendoza (Phillip Jose MENDOZA)

DEFENDANT'S EXHIBIT 3

This is provided solely for the Akron Police Department and is classified **confidential**

Cyber Profiles

pmendoza205@gmail.com (Phillip Jose MENDOZA)
Tracking of GoogleID 100626735686768023723
ladypimpjuice625@aol.com (Phillip Jose MENDOZA)

Phone Numbers

(330) 475-9599 (Phillip Jose MENDOZA)
(330) 608-7874 (Phillip Jose MENDOZA)
(330) 459-9599 (reference to Phillip Jose MENDOZA)

Current Geolocations

CyberCheck intelligence highlights communications and / or connections, through the tracking and correlation of cyber assets of timeframe, throughout 2020, for Phillip Jose MENDOZA to the following locations.

184 Reid Terrace, Apartment 103, Akron, OH, 44310 (throughout 2020, 2021 and 2022)

Intelligence Bulletin

INTELLIGENCE BULLETIN #1

MAC ADDRESS
48:00:33:bf:c0:4a (+/- 10 meters)
VENDOR
Technicolor CH USA Inc.
SSID
Woodall5
APPROXIMATE LOCATION
At (or near) at 1228 5th Avenue, Akron, OH, 44306
DATE – APPROXIMATE TIME – PROFILE HITS
08/20/2020– 2100 EDST (+/- 15 mins) – Total of 7
08/20/2020 – 2115 EDST (+/- 15 mins) – Total of 4
SUPPORTED INTELLIGENCE
Full profile of Phillip Jose MENDOZA

This is provided solely for the Akron Police Department and is classified **confidential**

INTELLIGENCE BULLETIN #2

MAC ADDRESS
62:45:b6:e6:08:d0 (+/- 10 meters)
VENDOR
Not Broadcasted
SSID
Not Broadcasted
APPROXIMATE LOCATION
At (or near) at 1228 5th Avenue, Akron, OH, 44306
DATE – APPROXIMATE TIME -- PROFILE HITS
08/20/2020– 2100 EDST (+/- 15 mins) – Total of 3
08/20/2020 – 2115 EDST (+/- 15 mins) – Total of 6
SUPPORTED INTELLIGENCE
Full profile of Phillip Jose MENDOZA

This is provided solely for the Akron Police Department and is classified **confidential**

Curriculum Vitae of

Christian Mammarella, EnCE

Present Position

Senior Forensic Analyst
Vestige Digital Investigations
8668 Concord Center Dr, Englewood, Colorado 80112
M: (720) 670-2223 | O: 800-314-4357
cmammarella@vestigeltd.com
Licensed Private Investigator, Texas #17819101

Previous Positions

Senior Forensic Analyst
Cyopsis
Englewood, Colorado
December 2018 – April 2022

- Encase Certified Examiner who performed imaging and analysis of digital media and provides expert witness services including reports and testimony for a variety of clients across many industries.
- Examined computers, mobile devices and emails accounts.
- Created digital timelines of activity found on the devices.
- Analyzed the metadata within documents, to determine if modification took place.
- Examined cellular tower call detail records and testified in Federal court about his analysis.

Senior Consultant
B&V Pathway Forensics, LLC
Houston, Texas
June 2015 to November 2018

- Provide computer forensics and electronic discovery services including the acquisition, authentication and analysis of electronic evidence to clients across many industries.
- Provided expert testimony in Federal, military, state court civil and criminal jury trials.
- Examined computers, mobile devices and cellular tower records.
- Administered a CLE case study event on Cellular Tower Records and locations.

Curriculum Vitae of

Christian Mammarella, EnCE

Experience

Vestige Digital Investigations – Senior Forensic Analyst

Responsible for conducting forensic analysis on digital media as deemed appropriate by currently accepted standards.

Converse with clientele and convey standards, procedures, and results of forensic analysis in an easy-to-understand manner.

Test new programs and methodologies for adaptability in the forensic environment.

Experience with cases in fraud, employment relations, intellectual property theft, and criminal matters.

Experience with the acquisition and analysis of Windows and Macintosh computers and servers.

Experience with the acquisition and analysis of other digital storage media, such as CDs/DVDs, flash drives, and SD cards.

Experience with the acquisition and analysis of Android and iOS mobile devices, as well as standard cell phones.

Expert in cell phone and cell phone tower forensics.

Police Detective | Police Officer
Boca Raton Police Services
Boca Raton, FL
June 2004 to August 2014

- Worked computer crimes for the State Attorney's Office in the Sexual Predator Enforcement Unit.
- Examined Computers for the U.S. Secret Service MECTF task force.
- Performed Computer Forensic Examinations for many Local and Federal agencies.
- Assigned to Computer, Economic and Property Crimes while in the Detective Bureau for 6 years.
- Active Member of Internet Crimes Against Children.
- Created new methods for extracting evidence from cell phones.
- Wrote and executed multiple Federal and State Search Warrants.
- Investigated crimes by interviewing people, gathering information and organizing the results.
- Used knowledge of the Florida State Statues and civil process to assist and educate the public.
- Active member and Drill & Ceremonies Trainer of the Boca Raton Honor Guard.
- Worked as a Crisis Intervention Officer when dealing with subjects in emotional distress.
- December 2006 Officer of the Month, for using "street level" contacts to solve a crime.
- Provided training to other Officers

July 1994 to July 2011: Military Police Officer / Automated Logistical Specialist, U.S. Army, Fort Bragg, NC / Fort Stewart GA

- 5 years of Active Duty at Fort Bragg and 1 year of Active Duty at Fort Stewart.
- Deployed to Iraq in 2008
- Investigated crimes that happened on and off the military post, involving service members.
- Active member of the Special Reaction Team and Bike Patrol.
- Worked in protective services and Presidential Security when the President visited the posts.
- Handles supply actions for over 300 Army units, each consisting in excess of 700 people.
- Accountable for $1.1 Million of on hand supplies.
- Handled and fixed computer problems as a MP and Logistical Specialist.
- Received Army Commendation Medals for performances.
- Soldier of the Month, #1 out of 750 soldiers; runner-up for Soldier of the Year.

January 1999 to December 2003: Assistant Manager / Loss Prevention, Office Depot, West Palm Beach, FL

- Managed all areas of the store including, Computer sales and Business Machines.
- Handled the logistics of ordering and receiving supplies for the establishment.
- Supervised approximately 30 people and maintained their files.
- Worked as a computer trouble shooter when errors occurred and answers were needed.
- Investigated credit card and shoplifting crimes, in person or via computer.
- Operated equipment ranging from cash registers to computers.
- Repaired computer equipment on scene and instructed customers over the phone.

Curriculum Vitae of

Christian Mammarella, EnCE

Education

- Diploma from Atlantic Community High School in Delray Beach, Florida.
- Received 37 credits in General Education from Palm Beach Community College, Lake Worth, Florida.
- Certificate, 13-week Automated Logistical Specialist Course from Fort Lee, Virginia.
- Certificate, 2 Week TACCS/SAMS computer course from Fort Lee, Virginia.
- US Army Airborne School, Fort Benning, Georgia.
- Drivers Training, HAZMAT, Aircraft Load Master and Management Course from Fort Bragg, NC.
- Military Police Course, 8 weeks, Fort Leonard Wood, MO.
- Special Reaction Team Training 80 hours, Fort Stewart Georgia.
- Certificate, 700 hours Certificate of Compliance Law Enforcement Officer, Florida Department of Law Enforcement.
- Certificate, 40 hours Investigative Interviews Broward Community College, Florida.
- Certificate, Crisis Intervention Team Training, South County Mental Health Center, Florida.
- Certificate, 192 hours Basic Computer Evidence Recovery Training, US Secret Service, Alabama.
- Certificate, 64 hours Advanced Forensics Training, US Secret Service, Alabama.
- Certificate, 16 hours Computer Crimes Legal Issues, Broward Community College, Florida.
- Certificate, 40 hours Conducting Internet Investigations, Broward Community College, Florida.
- Certificate, 24 hours CAC/Sex Crimes Investigations, Palm Beach Sheriff's Office, Florida.
- Certificate, Certified Cellebrite UFED Mobile Device Examiner Course, Washington D.C.
- Certificate, Certified Cellebrite UFED Physical Examiner Course, Washington D.C.
- Certificate, 24 hours Search and Seizure in the Electronic Age, Broward Community College, Florida
- Certificate, 64 hours Encase v7 Computer Forensics I and II, Guidance Software Online
- Certificate, 32 hours Encase v7 Advanced Computer Forensics, Guidance Software Online
- 3 Day course, Encase v7 EnCE Prep Course, Guidance Software Online
- Certification, (EnCE) Encase Certified Examiner 15-0317-7548

Certifications

Encase Certified Examiner (EnCE)
Opentext™

Curriculum Vitae of

Christian Mammarella, EnCE

Affiliations

Active Member of Internet Crimes Against Children
Miami Electronic Crimes Task Force
Palm Beach County Sexual Predator Enforcement Unit
Grid Cop

Presentations

CLE Case Study (Beaumont, TX) 2017

- Spoke about how I used Cell Tower records and the data within the cellphone, to prove two clients were not involved in a homicide. Provided a possible new suspect, with the collected cell tower data collected.

P.I. Continuing Education Event (Houston, TX) 2018

- Spoke about the myths and reality of cellphone data and extractions. Explained how cell tower data can be useful in an investigation. Provided examples of how applications on a cellular device, can record your locations. The event was for the Texas Association of Licensed Investigators.

CLE Case Study (Centennial, CO) 2019

- Spoke about using Cell Tower records and the data within the cellphone, to prove two clients were not involved with multiple burglaries. Provided location data and communication logs, showing the clients were not involved with the burglaries. The event was with the Arapahoe County Bar Association.

Educational Bootcamp (Denver, CO) 2022, 2023

- Spoke to high school students and their parents about the dangers of social media, cyber-bullying and the use of electronic devices. Provided examples of how social media apps track your locations. Spoke about sexting and what can be recovered from a cellphone. The event was held at the office of Foster Graham Milstein & Calisher, LLP.

CLE Case Study (Thornton, CO) 2023

- Explained how cell tower data can be useful in an investigation. Provided examples of how cellular applications record your location. Spoke about using the data and how to collect it. The event was for the Professional Private Investigators Association of Colorado.

CLE Case Study (Centennial, CO) 2023

- Spoke about Electronically Stored Information (ESI), evidence of spoliation and using location data. Provided examples of social media ESI and how to collect it. Spoke about a case involving location data and how some of communication was deleted, from the cellphone. The event was with the Arapahoe County Bar Association.

Expert Witness Testimony & Case Experience

State of Ohio v Deshawn Coleman, Eric Farrey (Case No. CR-21-08-2734) Hearing, Court of Common Pleas, Summit County, Ohio, December 2023

- Testified as an expert in Open Source Intelligence.
- Testified about preserving evidence in civil and criminal investigations.
- Testified about the need to validate information, found in the Deep or Dark Web.

Jenne M Esch v Mark Precious and CarbonHelix et al (Case No. 20CV30030) Hearing, District Court, Douglas County, Colorado, May 2023

- Testified about remote wiping of a mobile device.
- Testified about the restore process of an iPhone backup stored in the iCloud.
- Testified about the metadata within the Apple iOS Property List (plist) files.

State of Colorado v Caleb May (Case No. 21CR1027) Jury Trial District Court, Arapahoe County, State of Colorado, September 2022

- Testified about the examination of a cellphone.
- Testified about the Keepsafe app and the effects of the encryption.
- Testified about the metadata of videos and thumbnails.

State of Florida v Corey B. Johnson (Case No. 18CF002758) Jury Trial and Deposition, 15th Judicial Circuit Palm Beach County Florida, September 2021, October 2021

- Testified about the examination of the cellphone.
- Testified about the Telegram app communication, prior to the homicide.
- Testified about violent videos and photos located on the cellphone.

State of Colorado v Braedon Bellamy (Case No. 20CR1451) Jury Trial, District Court, Boulder County, State of Colorado, August 2021

- Testified about the metadata, showing editing of videos on a cellphone.
- Testified about the last modified dates of videos on a cellphone.
- Testified about the deleted text messages and the SMS storage database.

State of Colorado v Aidan Atkinson (Case No. 19JD309) Jury Trial, District Court, Boulder County, State of Colorado, April 2021

- Testified about the metadata within pictures and videos.
- Testified about the creation dates and validity of the media.
- Testified about the Cellebrite software extractions.

State of Ohio v Chinedu Nsidinanya (Case No. 15 CRB 2207Y) Jury Trial, Youngstown Municipal Court Mahoning County, Ohio, January 2017

- Testified about the location of a cellphone based on the cell tower connections.

U.S. v Joel Vargas, Angelica Vargas (Case No. 1:18-CR-00007) Jury Trial, U.S. District Court EDTX, Beaumont Division, March 2019

- Testified about the cellular provider, Call Detail Records and tower locations.
- Testified about the communication between the mobile devices and cellular towers.
- Testified about the validation of GPS locations within the provided reports.

U.S. v Syed R Mohiuddin (Case No. 15-34752-H1) U.S. Bankruptcy Court SDTX, Houston Division, October 2018

- Testified about missing email and the devices connected to the Gmail account.
- Testified about the use of the Eraser software program, on the collected devices.
- Testified about the synced internet cloud and recovery email accounts.

State of Texas v Ali Awad Mahmoud Irsan (Case No. 146560901010-3) Jury Trial, 184th District Court, Harris County Texas, July 2018

- Testified about the cellular communication records and the extracted Text Messages from the cellphones.
- Testified about the logged GPS locations over 11 months, with video presentations.
- Testified about surveillance practices and Microsoft file metadata.

State of Texas v Sean Lavergne (Case No. 15-23725, 18-28631) Jury Trial, Jury Retrial, 252nd Judicial District Court of Jefferson County, Texas, February 2018 and May 2018

- Testified about the two cellphones and their cellular communications to each other.
- Testified about the Text Messaging, Chat Applications and Multimedia Messaging Service.
- Testified about the cellphone damage and what could have prevented the cellphone's 911 call.

U.S. v A1C Jacob D. Burns (Case No. 408-C-112AD1-33431170411750) Jury Trial, Goodfellow Air Force Base, October 2017

- Testified in an Airforce Court Martial about cellphone and computer forensics.
- Testified about the drug related internet searches and using encryption messaging software.

Joseph Pressil v Jason A. Gibson, The Gibson Law Firm (Case No. 2013-51350) Deposition, 55th District Court Harris County, Texas, April 2017

- Testified about the metadata within a Microsoft Word Document.

Dora Alicia Williams v Robert Max Williams (Case No. 15-05-05360-CV) Trial, 418th Judicial District Court, Conroe Texas, May 2016

- Testified about cellphone and computer forensics.
- Testified about how an agreed forensic protocol would work and the distribution of information.

State of Florida v Jason Peritz (Case No. 2009-CF-009789 / 2011-CF-007149) Jury Trial and Depositions, 15th Judicial Circuit Palm Beach County Florida, April 2011, November 2012

- Testified about contraband located on his computers, transferred contraband and cellphone communications.

State of Florida v William Stewart (Case No. 2011-CF-009737) Depositions, 15th Judicial Circuit Palm Beach County Florida, March 2012

- Testified about contraband located on multiple computers, DVDs and external devices.
- Testified about the transmission of the contraband, through internet websites.

State of Florida v Brian Clancy (Case No. 2011-CF-010545) Depositions, 15th Judicial Circuit Palm Beach County Florida, August 2013

- Testified about the text messages, images and applications on the offender's iPhone.

U.S. v Gary Golberg (9:13-CR-80082-KAM) Depositions, Southern District of Florida, April 2013

- Testified about contraband images on his computer and the victim's cellphones.
- Testified about the dates and times they were created.

State of Florida v Curtis Leo Barber (2011-CF-011632) Jury Trial and Depositions, 15th Judicial Circuit Palm Beach County Florida, June 2013, July 2014

- Testified to the contraband found on the defendant's computer and iPod Touch.

State of Florida v Adolfo Espinoza (2011-CF-002912) Depositions, 15th Judicial Circuit Palm Beach County Florida, April 2013

- Testified to the contraband found on the defendant's computers and how it was transmitted.

State of Florida v Matthew Takahasi (2009-CF-008698) Depositions, 15th Judicial Circuit Palm Beach County Florida, February 2011

- Testified to the contraband found on defendant's computers and how it was transmitted.

State of Florida v Kevin Gauthier (2011-CF-002415) Jury Trial and Depositions, 15th Judicial Circuit Palm Beach County Florida, January 2012, April 2013

- Testified about contraband located on his computers, transferred contraband and cellphone communications.

State of Florida v Mihai Arnautu (08023058CF10A) Jury Trial, 15th Judicial Circuit Palm Beach County Florida, December 2011

- Testified about the ATM skimmer diagrams found in the computer. Testified about the internet search history and the credit card numbers found in multiple files.
- Testified about the use of Bluetooth and how it was used with the ATM skimmer.
- Demonstrated how the devices worked by reconstructing the dismantled ATM skimming device, camera and keypad.

VESTIGE
Digital Investigations

Digital Forensic Analysis

Report of Findings

Case: OH v Mendoza

Examiner: Greg Kelley

Audience: Phillip Mendoza

May 6, 2024

Vestige Ltd
23 Public Sq., Ste. 250
Medina, OH 44256-2284
330.721.1205 / 800.314.4357
Fax: 330.721.1206
www.VestigeLtd.com

Turning Digital Evidence into Intelligence™

DEFENDANT'S EXHIBIT
D

CONFIDENTIAL ATTORNEY WORK PRODUCT

NOTICE

This report is confidential and is intended only for Phillip Mendoza and its legal counsel, Donald Malarcik. If you are not the intended recipient of this document, any use, dissemination, distribution or copying of this document or its contents is strictly prohibited. The information contained in this document may also be privileged and/or subject to the attorney work-product protection.

The included information in this Report of Findings is <u>not</u>, nor should be considered, a legal opinion. It is merely the results from our investigation and may be incomplete due to evidence having not been provided to Vestige. The reader must be aware that these results may not include all exculpatory and inculpatory evidence if it has not been provided.

Additionally, this report and its content may only be used by Phillip Mendoza for the purposes of this case (OH v Mendoza). No portion, in whole or in part, may be duplicated and/or used for any other purposes without the express written permission of Vestige Ltd.

Table of Contents

OVERVIEW

Objective

Pursuant to the request of Donald Malarcik, I have forensically examined multiple items related to a CyberCheck report provided as evidence in this case. At issue is the repeatability and accuracy of the claims made in the CyberCheck report.

BACKGROUND

Evidence

Vestige relied on only the specific data identified in this report in order to form its opinion.

- CyberCheck Report with case reference 20-097360

Software & Tools

CellHawk (https://www.leadsonline.com/main/cellhawk.php)

FINDINGS

Conversion of Raw Data to Intelligence Data

In speaking with Adam Mosher and in reviewing the code, Vestige identified that data harvested from various internet sources was sent to another system which Vestige was not able to review. That system, per Adam Mosher, was the Artificial Intelligence (AI) system which would analyze the raw data and determine, based on rules built in the AI and prior training of the AI, which raw data points would become intelligence data.

Discussions with Adam Mosher, involving Greg Kelley, Chris Mammarella and Daniel Colwell, indicated that the AI system responsible for determining what raw data would become intelligence data was trained on prior cases. The CyberCheck AI system was trained by identifying what raw data could become intelligence data and "solve" cases with known outcomes. Vestige was not given the opportunity to test or verify this claim.

Identical Reports for Different Days

Vestige was provided by counsel the CyberCheck report issued in this case. To be specific two CyberCheck reports were issued for this case. The reports are attached as Exhibit 2 and Exhibit 3 to this report.

In testimony and in discussions with Adam Mosher, it has been represented that the creation of a CyberCheck report is an automated process. After a licensed law enforcement agency submits an "ask" while logged into the CyberCheck portal, the process begins and no further human action occurs through the creation of the CyberCheck report.

Exhibit 2 and Exhibit 3 represent identical reports with identical accuracy, identical cyber profiles and identical intelligence bulletins, except for one significant difference. Exhibit 2 has a date of August 2, 2020 in the Overview section (which has been represented as the "ask") as well as in Intelligence Bulletin #1 and Intelligence Bulletin #2. Exhibit 3 has a date of August 20, 2020 in the Overview section, Intelligence Bulletin #1 and Intelligence Bulletin #2.

If both CyberCheck reports are taken as being authentic CyberCheck reports, the CyberCheck system is stating that there is a 93.13% probability that Philip Mendoza's cyber profile was at or near 1228 5th Avenue, Akron, OH 44306 on both August 2, 2020 and August 20, 2020 between 9:00 PM and 9:15 PM Eastern Time. Of even more coincidence is that the number of cyber profile hits present on wireless routers at this location is identical on both days, at the same time each day.

Cell Phone Numbers

The CyberCheck Reports list three phone numbers in the following manner:

(330) 475-9599 (Phillip Jose MENDOZA)
(330) 608-7874 (Phillip Jose MENDOZA)
(330) 459-9599 (reference to Phillip Jose MENDOZA)

Vestige utilized an online tool, CellHawk, which is a service utilized by law enforcement and other investigative agencies. CellHawk allows for querying of phone numbers to obtain carrier and subscriber information.

Vestige queried CellHawk for subscribers associated with the above three numbers. CellHawk identified all three numbers as being assigned to the provider T-Mobile. The below charts identify individuals and addresses associated with the numbers.

Number	Name
(330) 459-9599	S Owens
(330) 459-9599	Sanetta Owen
(330) 459-9599	Sanetta Renee Owens
(330) 459-9599	Sanetya Owens
(330) 475-9599	Sheryl Alissa Mendoza
(330) 475-9599	Sheryl Alissa Wilkens
(330) 475-9599	Sheryl Alissa Wilkins
(330) 475-9599	S Mendoza
(330) 608-7874	Tracy M Wise
(330) 608-7874	Tracy Marie Hamilton

Number	Address
(330) 475-9599	184 Reid Ter Apt 103 Akron, OH 4431
(330) 475-9599	195 Edward Ave. Akron, OH 44310
(330) 475-9599	270 Iuka Ave Akron, OH 44310
(330) 459-9599	2737 Sheraton Dr Macon, GA 31204
(330) 459-9599	40 Byers Ave Akron, OH 44302
(330) 459-9599	175 Dodge Ave Akron, OH 44302
(330) 459-9599	454 Crestwood Ave Apt 1 Akron, OH 44302
(330) 459-9599	666 N Howard St Apt 201 Akron, OH 44310
(330) 608-7874	4649 Tudor Ln Stow, OH 44224

The above information provides alternative names and addresses to what is in the CyberCheck Report. The CyberCheck Report does not cite from where it received its data for the phone numbers or specifically what the CyberCheck Report means when it states "reference to."

Documentation Surrounding Intelligence Data

A review of multiple CyberCheck reports as well as discussions with Adam Mosher revealed that the CyberCheck application does not do the following:

1. Record URLs where raw data or intelligence data was discovered.

2. Make forensic preservations of any raw data or intelligence data related to a CyberCheck report.

A review of multiple CyberCheck reports identified social media accounts or URLs pointed to accounts on social media sites which did not exist.

Distances Applied to a MAC Address

The CyberCheck Report provides the following information with respect to what the CyberCheck Report refers to as "Intelligence Bulletin #1."

> MAC ADDRESS
> 48:00:33:bf:c0:4a (+/- 10 meters)

A Media Access Control (MAC) address is a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment (https://en.wikipedia.org/wiki/MAC_address). According to the specification on MAC addresses, MAC addresses can be universally assigned or locally assigned. The determination of the type of MAC address is based on the second least significant bit of the first octet of the MAC address. In the example above, the first octet is 48 which converts to a binary value of 01001000. The second least significant bit is a "0" which indicates that this MAC address is universally assigned. Universally assigned addresses can be connected with a vendor via looking up the values for the first three octets. In the example above, 48:00:33 is the value assigned to Vantiva USA LLC which was previously Technicolor USA.

A review of the code and discussion with Adam Mosher revealed the calculus behind the above statement in the CyberCheck Report. CyberCheck will use open source information to calculate the possible radius that a wireless router can broadcast its signal. CyberCheck will then take the location where that wireless router allegedly exists, overlay a map on the location and utilizing algorithms, identify potential obstructions which can limit the wireless signal. According to Adam Mosher, this calculus does not consider the different make-ups and materials of the obstructions.

CONCLUSIONS AND OPINIONS

Based on the evidence in this report, Vestige holds the following opinions to a reasonable degree of scientific certainty. Should additional evidence come to light, Vestige reserves the right to review that evidence and change its opinions if warranted.

1. The fact that the CyberCheck system produced two reports with identical results in all aspects except for the activity in the report being attributed to two different days (but identical times on those two days) calls into question the accuracy and legitimacy of the CyberCheck system. It is implausible that the same number of cyber profile hits, for the same cyber profile, was picked up by the same wireless routers at the same time on two different days.

2. The reporting of a MAC address in the CyberCheck report followed by a metric of plus or minus a number of meters is misleading. The use of "plus or minus" is usually connected with and interpreted as a statement of accuracy. In the case of the CyberCheck Report the plus or minus distance is intended to convey a calculated distance that the wireless router can transmit its signal. The calculated distance comes with no explanation or disclaimer in the report about any potential variances. Factors not considered in the calculus of the wireless distance are:

    a. Differences in wireless broadcast distance based on the exact model of the wireless router.
    b. Vertical height of the placement of the wireless router
    c. Age and condition of the wireless router
    d. Actual effect of the obstructions on the wireless router signal

3. No information is reported by CyberCheck regarding what specific aspects of someone's cyber profile was identified in the Intelligence Bulletins and identified in connection with a wireless router.

4. The lack of any documentation on where intelligence data in the CyberCheck Report was obtained leads to a lack of credibility of the intelligence data. Furthermore, without knowing the source of the intelligence data it is nearly impossible to compare any contradictory data in order to determine which data point is more credible.

5. The lack of any preservation of intelligence data in the CyberCheck Report prevents any rebuttal from inspecting, testing or examining the intelligence data to come to the same conclusion or a different conclusion. Data on the internet is added, changed and removed and what is present one day may not be present the next.

6. No specificity has been provided regarding the process of how the Artificial Intelligence system was trained outside of the representation that it was trained on cases with known outcomes. Information such as the types of cases, venues where the cases took place, types of charges associated with the case and the specifics of the accused and convicted are unknown.

Greg Kelley, EnCE, DFCP
Vestige Digital Investigations

MISCELLANEOUS

This report and the opinions expressed herein are based upon the facts and knowledge at the time of its creation. Should additional facts come to light, those may affect the opinion and should be brought to Vestige's attention for consideration.

Statement of Independence

Vestige Ltd and its employees, including myself, serve as independent, neutral experts. We do not have, nor anticipate, any special relationship with any of the parties in this matter, nor any of the parties' counsel.

Compensation

The analysis and writing of this Expert Report are not contingent on our findings or the outcome of our analysis. Vestige Ltd is compensated based on costs for flat fee projects or for the time expended on completing the analysis and writing of this Report. When billed hourly, Vestige Ltd is compensated at a rate of $275.

Qualifications of Expert

Exhibit 1 is a complete and accurate copy of my Curriculum Vitae, which includes my qualifications as a Digital Forensic Expert as well as publications and Expert Witness work performed.

APPENDICES

Appendix A – Fields for master_supply_chain_template.csv

1. CaseNumber
2. ACES Viewed Contents
3. ESP Viewed Contents
4. Briefing
5. Online Communications
6. Profile Strength
7. Suspect
8. Suspect DOB
9. Employment
10. Suspect Online Aliases
11. Suspect Profile
12. Country
13. State
14. Regional Coordinates
15. Suspect Current Location
16. Distribution Gateway
17. Trade Corridor
18. Supply Chain Position
19. Suspect Email Addresses
20. Suspect Risk Rating
21. Suspect Cyber DNA
22. Top Three Relatives
23. Top Three Associates
24. Related URLs
25. Victim
26. Victim DOB
27. Victim Online Aliases
28. Victimology
29. Country of Victim
30. Victim State
31. Regional Coordinates of Victim
32. Victim Current Location
33. Victim Cyber DNA
34. COPINE
35. Victim Email Addresses
36. Victim Risk Rating
37. Last Known Interaction
38. Regionally Relevant Sex Offenders
39. Magnitude
40. Solvability
41. Technical Identified Risks
42. ProfilePic
43. CaseCreated
44. PhoneData
45. AutoData
46. AdditionalInformation

47. IdentifiedRisks
48. AgencyID