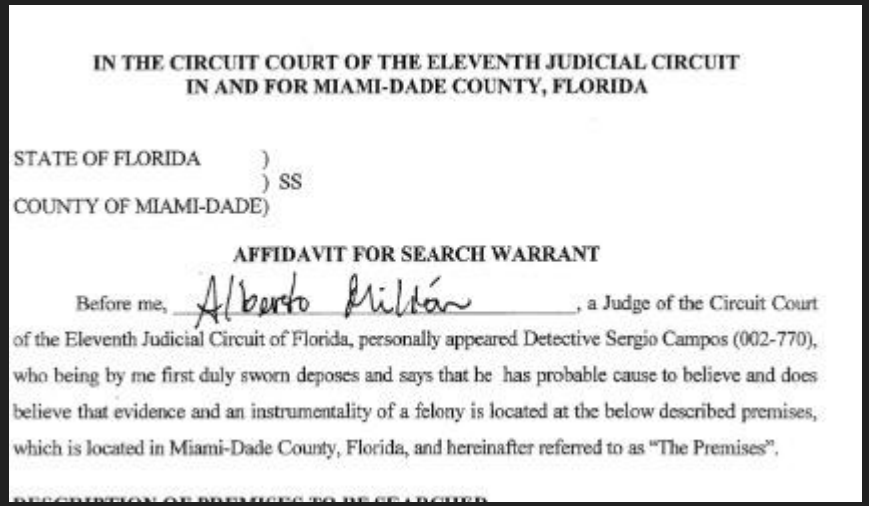
Cybercrime Case Study

State of Florida vs Wesley Victor

Christiane Galang

Introduction



IN THE CIRCUIT COURT OF THE ELEVENTH JUDICIAL CIRCUIT
IN AND FOR MIAMI-DADE COUNTY, FLORIDA

STATE OF FLORIDA)
) SS
COUNTY OF MIAMI-DADE)

AFFIDAVIT FOR SEARCH WARRANT

Before me, Alberto Milián, a Judge of the Circuit Court of the Eleventh Judicial Circuit of Florida, personally appeared Detective Sergio Campos (002-770), who being by me first duly sworn deposes and says that he has probable cause to believe and does believe that evidence and an instrumentality of a felony is located at the below described premises, which is located in Miami-Dade County, Florida, and hereinafter referred to as "The Premises".

- The documents from the affidavits provide the legal basis for issuing search warrants. It explores the investigators proof of probable cause, details of particularity, and connects digital forensics to criminal allegations.
- Case Study: State of Florida v. Wesley Victor
- Defendants: Wesley Victor & Hencha Voigt
- Allegation: Extortion (Release of explicit content unless $18,000 ransom is paid).
- In July 2016, the victim reported to Miami Beach Law Enforcement of messages via text threatening to release explicit videos unless $18,000 was paid. Investigators utilized digital forensics to trace back the messages to three mobile devices, all belonging to the defendants

How was Probable Cause Established?

- The victim received cyberthreats from Voigt and Victor of exposing explicit videos unless she paid $18,000.
- Law enforcement recovered multiple phones including a Black Samsung Cell Phone, an Apple iPhone (White, Model: H1633) and a Blackberry cell phone
- Phone numbers, time stamps, and messages were cross-checked and verified the involvement of the devices in the July 20-21, 2016 extortion crime.

How was Particularity in the place

- Device Make and Model: Apple iPhone, White, Model A1549.
- Identifiers of the device IMEI 356980637924645 and linked telephone number 754-202-6802.
- In custody of the Miami Beach Police Department case #2016-64911

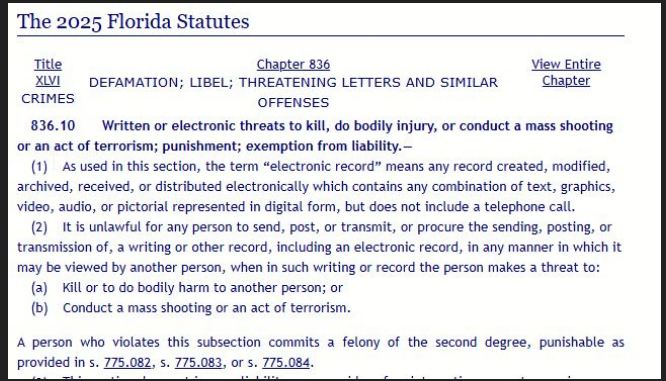
Apple iPhone, White, Model: A1549, IMEI: 356988063792465, that is assigned telephone number (754) 202-6802.

Particularity in the Things to be Seized

- Communication records: outgoing and incoming phone calls, text/multi messages, emails
- Contact lists
- Media and metadata: photos, audio/video recordings, web history, internet "cookies," IP addresses, MAC addresses, Internet Service Provider Account subscriber, billing and credit information

How does the affidavit establish a nexus between the evidence sought and the cybercrime committed?

- There were text messages that contained threats from the specific device (iPhone) and other connected devices.
- Voigt admitted to using the device to send messages and blamed Victor.
- Digital forensics can retrieve deleted data



The 2025 Florida Statutes

Title XLVI CRIMES | Chapter 836 DEFAMATION; LIBEL; THREATENING LETTERS AND SIMILAR OFFENSES | View Entire Chapter

836.10 Written or electronic threats to kill, do bodily injury, or conduct a mass shooting or an act of terrorism; punishment; exemption from liability.—

(1) As used in this section, the term "electronic record" means any record created, modified, archived, received, or distributed electronically which contains any combination of text, graphics, video, audio, or pictorial represented in digital form, but does not include a telephone call.

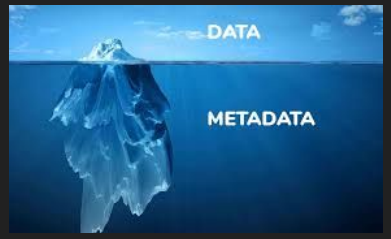
(2) It is unlawful for any person to send, post, or transmit, or procure the sending, posting, or transmission of, a writing or other record, including an electronic record, in any manner in which it may be viewed by another person, when in such writing or record the person makes a threat to:

(a) Kill or to do bodily harm to another person; or

(b) Conduct a mass shooting or an act of terrorism.

A person who violates this subsection commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

Investigation (Additional Component)



- **What investigative techniques were used?**
  - Victim reported threatening texts demanding $18,000 in exchange for not releasing explicit videos
  - Investigators utilized digital forensics to confirm the primary source of threats.
    - Tools used:
      - Device Identifiers: IMEI, SIM cards, Account Numbers
      - Carrier Records and Subscriber data
      - Metadata: timestamps, sent/received logs, encrypted message recovery

Investigation (Cont..)

- **How did the search warrant assist in the investigation?**
  - Affidavit sworn by Detective Sergio Ocampo (Aug 17, 2016)
  - Court authorized seizure of four devices:
  - White Apple iPhone, IMEI - 356988063792465, Model A1549, (754)-202-6802
  - Black iPhone 6S (786)-351-1058
  - A Samsung Phone (305)-783-8445
  - A Blackberry device (754)-202-6802
  - Search warrant enabled lawful seizure and forensic examination, ensuring evidence was admissible in court.

Investigation (Cont..)

- **Were there challenges related to encryption, anonymity, or cooperation?**
  - Defendants attempted to delete incriminating texts to conceal involvement.
  - Forensic tools recover deleted data and reconstructed partial messages.
  - Cooperation from service providers was critical in linking phone numbers to defendants.

Investigation (Cont..)

- **What role did interagency collaboration or third-party cooperation play?**
  - Service providers supplied subscriber and communication logs
  - Collaboration allowed investigators to match timestamps and numbers to the victim's report (July 20-21,2016).
  - This ensured independent confirmation beyond collected devices.

Investigation (Cont..)

- **Did the investigation involve and innovative or emerging methods?**
  - Use of mobile device forensic tools to extract deleted messages.
  - Recovery of encrypted data beyond what was visible on the device
  - Communication logs
  - Metadata
  - Timestamps
  - Integration of victim testimony, defendant statements, and forensic results created a comprehensive evidence strategy.

Timeline of Events – State of Florida v. Wesley Victor

- July 20–21, 2016
- Victim receives threatening texts demanding $18,000
- July 21, 2016
- Victim reports threats to Miami Beach Police; investigation begins
- August 17, 2016
- Detective Sergio Campos swears affidavit; search warrant issued listing four devices
- May 3, 2017
- Court filing related to the case recorded
- May 15, 2017
- Additional court activity entered into record
- May 17, 2017
- Follow-up procedural filing documented
- June 9, 2017
- Further court record entry connected to case

Timeline Continued (Publicly known outcome from other news sources)

- Victor and Voigt were formally charged with extortion, conspiracy, and unlawful use of devices, linked to threats against the victim
- A judge ordered them to turn their phone passcodes in so investigators could access encrypted devices, despite arguments over fifth amendment rights.
- Voigt was later jailed for 180 days for refusing to hand over her Iphone passcode
- Victor claimed he “forgot” his passcode and was not jailed under that same order

Key Players

- Who are the major actors (suspects, victims, investigators, prosecutors)?
  - Hencha Voigt and Wesley Victor were the suspects.
  - The victim was Julieanna Goddard (unnamed in the affidavit).
  - The witness was unnamed.
  - The Affiant was Detective Sergio Campos, Badge #002-770, Miami Beach Police Department
  - The judges were Hon. Alberto Milian, Diane Ward, Charlie Johnson, Dennis Murphy.
  - The Prosecutors were Miami-Dade State Attorney's Office and Florida Department of Law Enforcement.

Key Players

- Did any individual or team play a pivotal or exceptional role?
  - Detective Sergio Ocampo and his team:
    - Detective Ocampo created an affidavit showing the connection among multiple devices, phone numbers, and two suspects.
    - Worked with forensic examiners to decrypt and recover deleted data.
    - Discovered evidence that connected the two suspects (Voigt and Victor) to the messages sent to the victim.

Key Players

- How did their actions influence the investigation or outcome?
  - Digital evidence traced back to the suspects
  - Forensic Data (IMEI/SIM) data confirmed the devices were used for extortion
  - Voigt's attempt to blame Victor tied both of them to the threats.
- Were any victims particularly vulnerable, powerful, or controversial?
  - The victim was particularly vulnerable as Victor and Voigt exploited her with threats to release explicit material unless ransom was paid
- What do the roles of these individuals reveal about the nature of cybercrime enforcement?
  - This case reveals that cybercrime enforcement relies heavily on digital forensics and collaboration between agencies
  - Accountability in cybercrime depends on technical skill and digital traceability