ST. JOHN'S UNIVERSITY

2023 IEEE ASEE Frontiers in Education Conference
College Station, Texas
October 18–21, 2023

Computer Squad Detectives: A Digital Forensics Case Exemplifying Social Justice

Authors: **Denise M. Dragos** & **Suzanna E. Schmeelk**
Affiliation: **St. John's University** – Queens, New York (United States)
Session: NCAE Annual Symposium – Charleston, South Carolina

Computer Squad Detectives:
A Digital Forensics Case Exemplifying Social Justice

- Introductions & University Background
- DFR Introduction
- Case Overview (Workshop slides on link below)
- Crime Scenes to Arrests with Exercises
- The Trial
- Conclusions & Attendee Survey
- Support material available at:

https://dmdragos.github.io/WiCyS-2023

Denise Dragos, M.S.

- Associate Professor, St. John's University
- Co-Founder M.S. Cyber and Information Security Program
- Doctoral Candidate, Pace D.P.S. Computing
- Private Consultant, NYS Lic. Private Investigator
- Manager, KPMG LLP, NYC Forensic Lab
- Detective (ret.), NYPD Computer Crimes Squad
- GIAC GSEC Gold, GCIH, GREM
- CISSP, CCO, CCPA, and Security+

Suzanna Schmeelk, D.P.S., Ed.D., M.B.A.

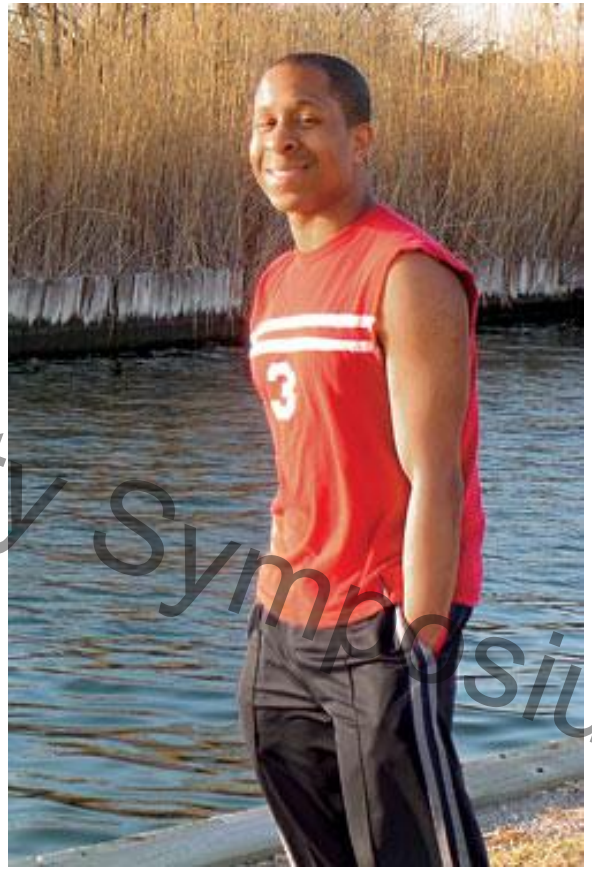
- Associate Professor, St. John's University
- Director of the M.S. Cyber and Information Security Program
- D.P.S. in Computing, Ed.D. in Mathematics
- M.B.A./M.S./B.S. in Computer Science/ Cybersecurity (8 Advanced Degrees)
- Alcatel Lucent / Bell Labs (Patent) / City of New York
- Health Informatics / Health InfoSec, BayArea
- Interdisciplinary and Technical Publications and presentations

Grave Mysteries – Death on the Highway
https://www.imdb.com/title/tt8749206/

(*See full slide deck for matching detective activities*)

Michael Sandy

- Michael J. Sandy, born 10/12/1977, originally from Bellport, NY
- Lived in Williamsburg, Brooklyn
- On October 8, 2006, Michael (age 28), met someone in online chatroom on website Adam4Adam
- Conversation moved to AOL Instant Messenger where they discussed meeting up - talk was very explicit in nature.



Case Overview – 10/8/2006

- Michael drove to meet up with his new acquittance in Sheepshead Bay, but after seeing a few extra people, got spooked and drove off
- Shortly later, Michael messaged FisheyeFox again to meet him alone
- He returned and they headed over to Plumb Beach together
- He was Attacked by several white men and chased into the highway
- Michael was hit by car (that never stopped). They dragged him onto shoulder and rifled through his pockets.
- On Friday,10/13/2006, after five days in a coma, Michael was taken off life support and died. It was the day after his 29th birthday.

Plumb Beach

Initial Computer Crimes Response – 10/9/2006

- On October 9, 2006, we received a call for assistance from the 61st Precinct Detective Squad for a robbery investigation
- Michael Sandy was found unconscious on the side of the highway when police arrived, but Detectives were able to locate his wallet and running car
- At Michaels residence, his computer was on and still logged into AOL with open chat windows.
- I was tasked with documenting and preserving evidence from Michael Sandy's home computer

Live Analysis of Windows Laptop

- Michael's residence, his laptop running Windows XP (SP1) was logged into AOL with an open chat conversation between DrumNBass007 (Sandy) and FisheyeFox.
- Chat conversation was first saved directly to USB drive as .txt and .rtf file
- Digital photos also taken of the screen and PC setup
- Helix3 Live CD was then used to process the system and do RAM Dump
- Once live analysis was complete, the laptop was taken into custody, invoiced and transported back to CCS Lab for further analysis

Exigent Circumstances

- FisheyeFox AOL account was still connected and ‘online’
- Analysis of chat content indicated that victim was targeted based on lifestyle
- Violent attack witnessed by passersby
- Coordinated with CCS Office to expedite contact with ISPs
- Emergency request made to AOL for subscriber and connection log data
- AOL account registered to John Fox, of Sheepshead Bay. The connection IP – Optimum Cable, additional subpoenas sent out.

OOL Subpoena Results

- Subpoenas must reference specific:
  - XXX.XXX.XXX.XXX on Date at HH:MM:SS zST/zDT/GMT/GMT Offset
- Received Subscriber and Billing Information for IP Connection log data covering time of conversation
- CME and CPE MAC Addresses
- Received within ½ hour of initial request
- Residence several blocks from crime scene
  - Bringham St. Sheepshead Bay, BK, NY
- Shared information with Case Detectives
- CCS Responded back to Brooklyn

Sheepshead Bay, Brooklyn, NY

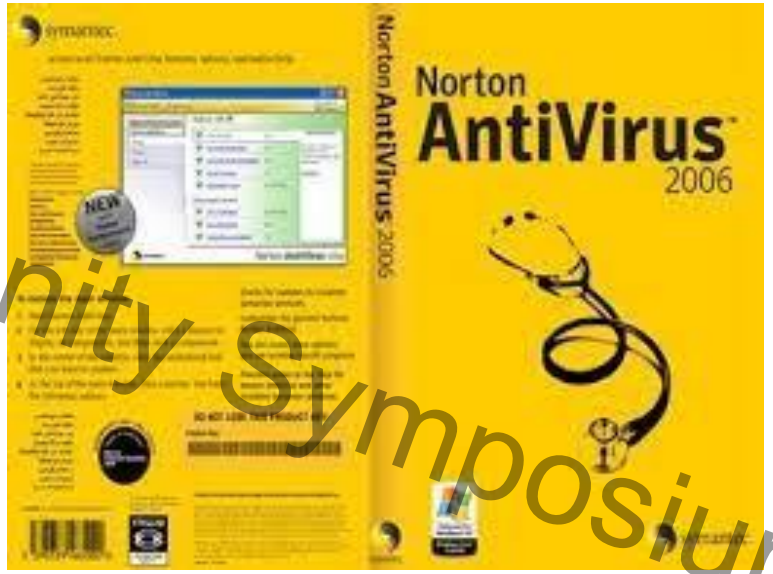
2nd Computer Crimes Response 10/9/2006

- Responded to location FisheyeFox where was connected
- Several Detective teams established surveillance of residence
- Wireless Site Survey Initially performed using NetStumbler (from a Windows PC) and Orinoco WIFI card with external Omni directional antenna- None Detected
- Male subject approached from door of residence
- Teams moved in made contact
- Individual identified self as off-duty NYPD Officer assigned to local Pct.
- Stated he was working all night, lived there with GF
- Confirmed he had Internet connection
- Explained he had just purchased wireless router and had “secured it with new Anti-Virus program”
- We were invited inside to talk

Network Forensics

- On kitchen table was new router and antivirus as claimed
- Officer explained that they had one laptop and produced it
- We were given consent to examine the computer and router
- I connected via ethernet cable to Linksys AP
- Default PW for Router Web GUI (Admin:Admin), SSID: Lynksys
- 3 devices were assigned IP addresses via DHCP
  - My laptop, GF's laptop, and one Unknown Device
- Router Settings were documented via Screen Shots, Print-to-PDF, digital photographs, and Web Spider tool (Teleport Pro)
- IEEE Organizationally Unique Identifier (OUI) Lookup of MAC Addresses: https://ouilookup.com/

Linksys WRT-54G Wireless AP & Norton AntiVirus



(See full slide deck for matching detective activities)

DHCP Review

- Dynamic Host Control Protocol - RFC 2132, 1997
- Automated service run on routers that manages connected devices and assigns IP Addresses, Subnet masks, Default Gateway, and DNS server settings
- Attempts to maintain network stability- default lease time is 24 hours, with automatic renewal every 12 hours
  - *Specific to WRT-54G (set by vendor and user configurable)
- Data maintained in tables that are accessible via the web console (or via terminal)

Undercover Chat with FisheyeFox

- FisheyeFox AOL account was still logged in, possibly within feet
- Employed scanning and sniffing tools to probe network
- I was the working on my undergraduate CompSci Degree and was enrolled mid-semester in an advanced networking course.
- Started unobtrusively trying to PING the rogue device, then went more active with NMAP and watched for potential traffic with Wireshark
- With no local network generated from that IP, decided to go 'hands-on'
- Used an undercover AOL account to message FisheyeFox directly
- He responded almost immediately – Light convo, mentioned he was back at school and had 'PT' in the morning (Physical Training)
- Chat documented with logging tool (DeadAIM)

3rd Computer Crimes Response 10/10/2006

- While I was chatting with FisheyeFox, colleague was on phone with AOL After-hours Emergency Contact line
- With Legal Documentation already served, they explained that FisheyeFox account had also been logged in from SUNY Maritime College – Public IP Address
- Detective teams responded to the Bronx and liaised with campus PD
- John Fox was located in his dorm room and returned to 61 with Precinct Squad Detectives
- Fox's desktop PC from his dorm room was secured and later brought to CCS once a search was secured by case Detectives

4th Computer Crimes Response 10/10/2006

- John Fox was questioned that day and eventually placed under arrest by Precinct Squad Detectives
- Additional subjects were identified through traditional investigative techniques- interrogations, interviews, etc.
- Called the following day to assist with the execution of a Search Warrant two doors down from off-duty PO
- Residence of Anthony Fortunato, acquaintance of John Fox
- Looking for wireless enabled PC, among other evidence
- Attorney representation at residence

'Smoking Gun' Laptop Located

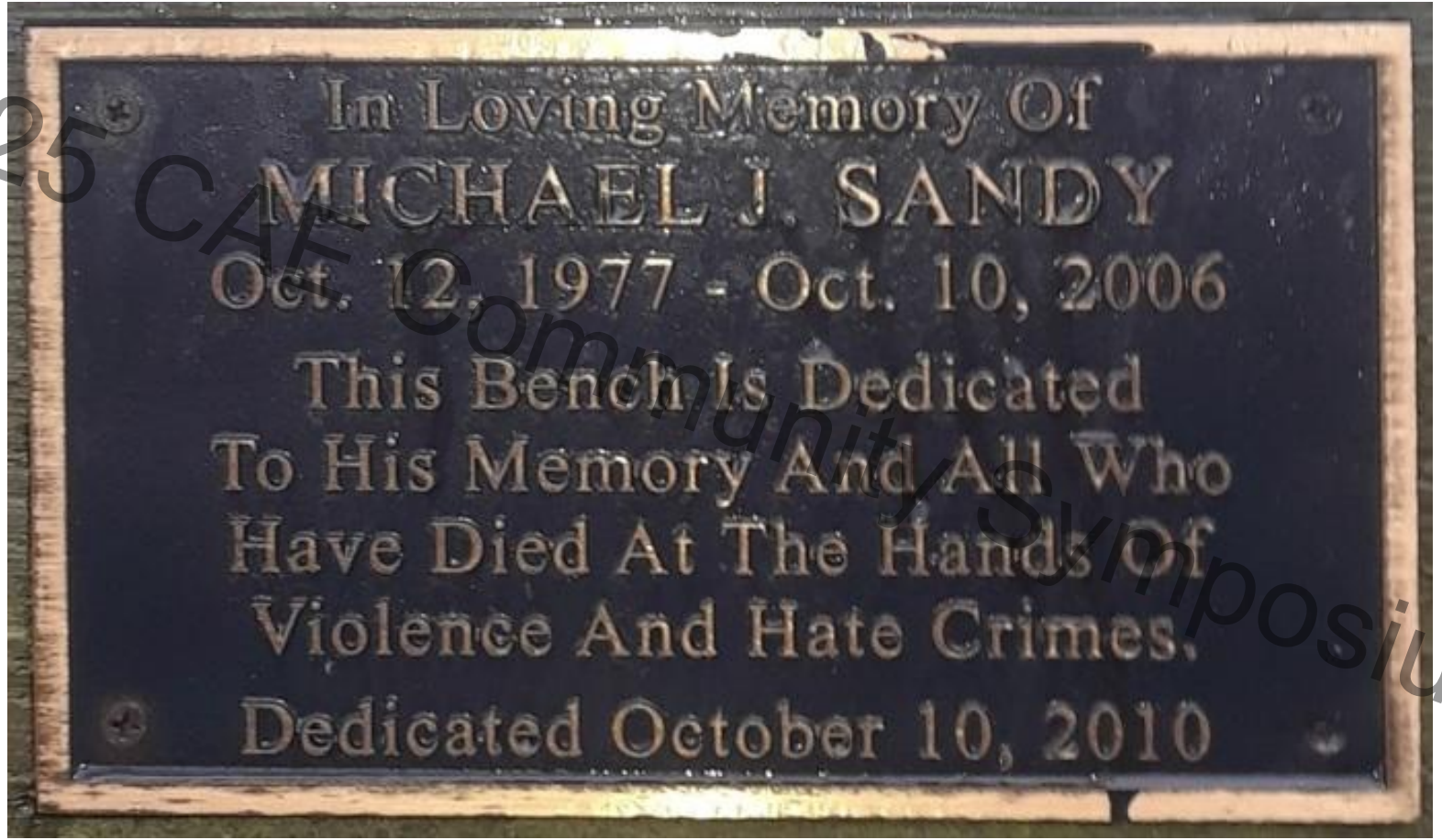
- Attorney offered the "only" laptop Family had
- Not Dell and MAC didn't match DHCP Log
- Dell Laptop located hidden in the basement garage
- MAC Address was physically located on the laptop
- Wireless NIC contained in accessible compartment
- Sticker affixed to NIC card located in device
- MATCHED the MAC from DHCP Client Table

Convictions and Sentences

- Fox and Fortunato were convicted by their juries after 1 month trial. Shurov subsequently plead guilty. Timmons plead guilty as part of deal where he had to testify against the other three, for reduced sentence.
- Fox - Manslaughter, Att. Robbery 1st and 2nd Deg. All counts were as Hate Crimes. (13-21 Yrs.) Released in Nov. 2017.
- Fortunato - Manslaughter as a Hate Crime and Att. Petit Larceny. (7-21 Yrs.) Paroled in 2015.
- Shurov - Plead Guilty to Manslaughter and Att. Robbery as Hate Crimes. (17 ½ Yrs.) Released in late 2021.
- Timmons - Plead Guilty to Att. Robbery as a Hate Crime. He cooperated. (4 Yrs.)

Conclusions / Lessons Learned

- Live Acquisitions are volatile, but can yield valuable evidence
- Practice on multiple Platforms
- Building relationships with ISPs is invaluable. Post incident follow up and feedback with ISPs helps with future cooperation
- Have as many tools available as you can afford- Best chance for success. Both open source and commercial.
- One and only one chance to retrieve data.
- Document all your actions.
- Need strong team work.
- IRB Feedback (Dragos and Schmeelk, 2023)



Contact Info and Questions

- Prof. Denise Dragos (Co-Founder of M.S. Cyber)
  dragosd@stjohns.edu

- Dr. Suzanna Schmeelk (Director of M.S. Cyber)
  schmeels@stjohns.edu