# DIGITAL FORENSICS RETROSPECTIVE AND MAJOR CASES

FOCUS ON SECURITY

BUCKS COUNTY COMMUNITY COLLEGE

OCTOBER 4, 2019

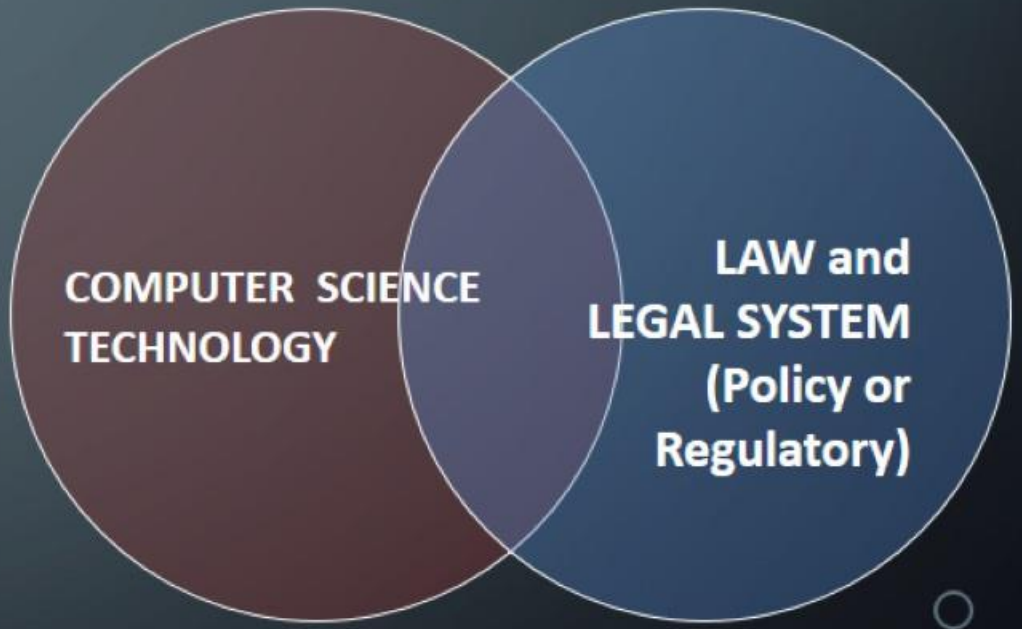
# WHO AM I?

- Pamela King
- Digital Forensics, Cybersecurity & E-discovery
- 1989 – 2005 law enforcement, civilian support in criminal cases
- 2005 – present civil cases, e-discovery, & part-time college instructor
  - 2008 – Woodside Consulting, LLC.
- 2013 – Full-time faculty at Chestnut Hill College (BS programs in Digital Forensics and Cybersecurity, Certificate in Digital Forensics, and Online MS in Cybersecurity)

# WHAT IS DIGITAL FORENSICS?

- What is digital forensics?
  - Collection and analysis of digital storage media, devices, and data in order to extract information relevant to legal matters (criminal, civil, regulatory, policy) in a manner that is scientifically acceptable and meets criteria to have findings be admissible in a court of law.

  - Combines knowledge of computer science technology with laws, rules of evidence, and legal systems.



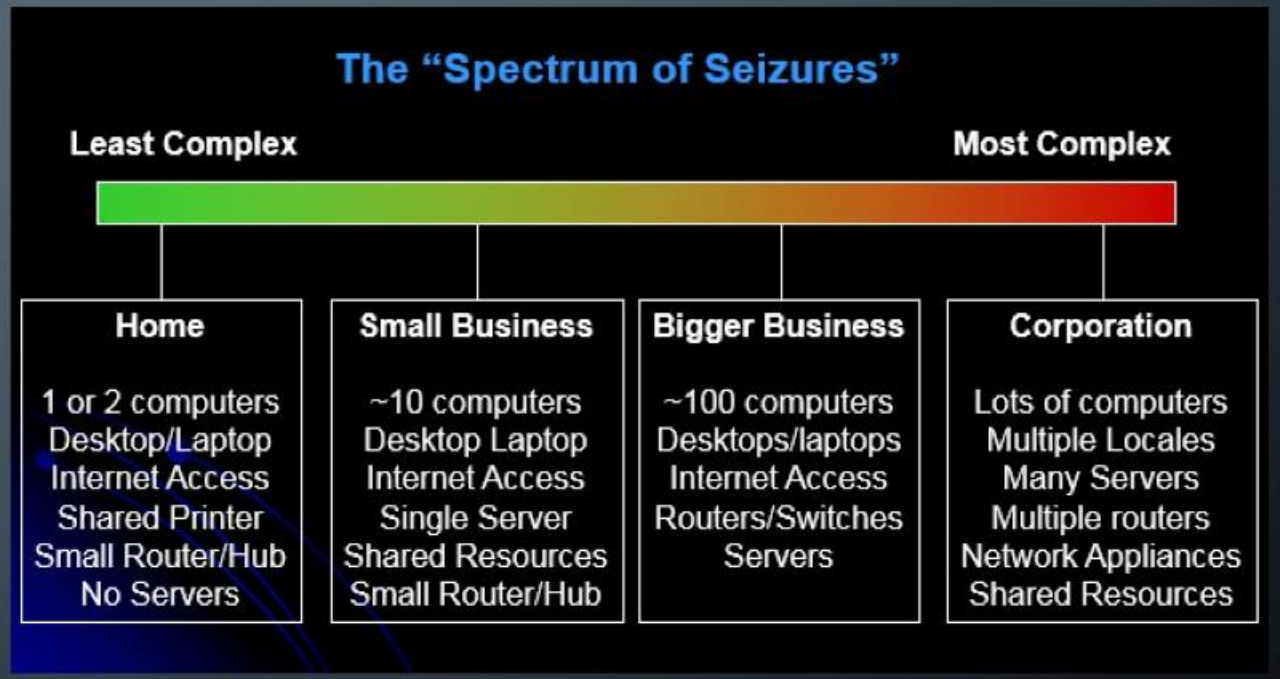
# CHALLENGES

## Technology Issues

- Quantity
- Volume
- Variety

## Management Support

- Money
- Time
- Training



# PRIOR TO 1990

- A lot of people didn't have home computers.
- Some had computers but no Internet Access

  (AOL via dialup?)
- Maybe one shared PC desktop in home.
- For business, might have a laptop.
- Maybe kids might have an Atari or Nintendo.
- Some floppies and a few CDs.


# PRIOR TO 1990

- Data Volume
  - Hard drive size
    - MBs
  - Floppies
    - 1.44MB each or less
  - CDs
    - 740MB


# PRIOR TO 1990

- Variety of Hardware
  - Limited storage media types
  - Limited Peripherals
- Variety of Software
  - Productivity, games
  - Operating Systems
  - Programming Languages

# APPROACHING 2020

- Multiple home computers
  - Home is a computer!
- Broadband and cellular access.
- Multiple devices per user
  - Gaming console
  - Cell phone
  - Tablets
  - Wearables
  - Medical devices
- Storage
  - Hard drives, USB Flash, Media Servers, Cloud

# APPROACHING 2020

- Volume
  - Amount, type, location, age
  - Exams are multiple TB and not exhaustive
- Variety
  - Hardware, Software (apps), Operating Systems
  - Storage Media, Cloud Data, 3rd Party Data

# DIGITAL FOOTPRINTS

- More Relevant
- Specialized skill set
- More Training
- More Tools
- More money

# FOUR "FAMOUS" CASES

The Serial Killer BTK

Scott William Tyree

Kevin Mitnick

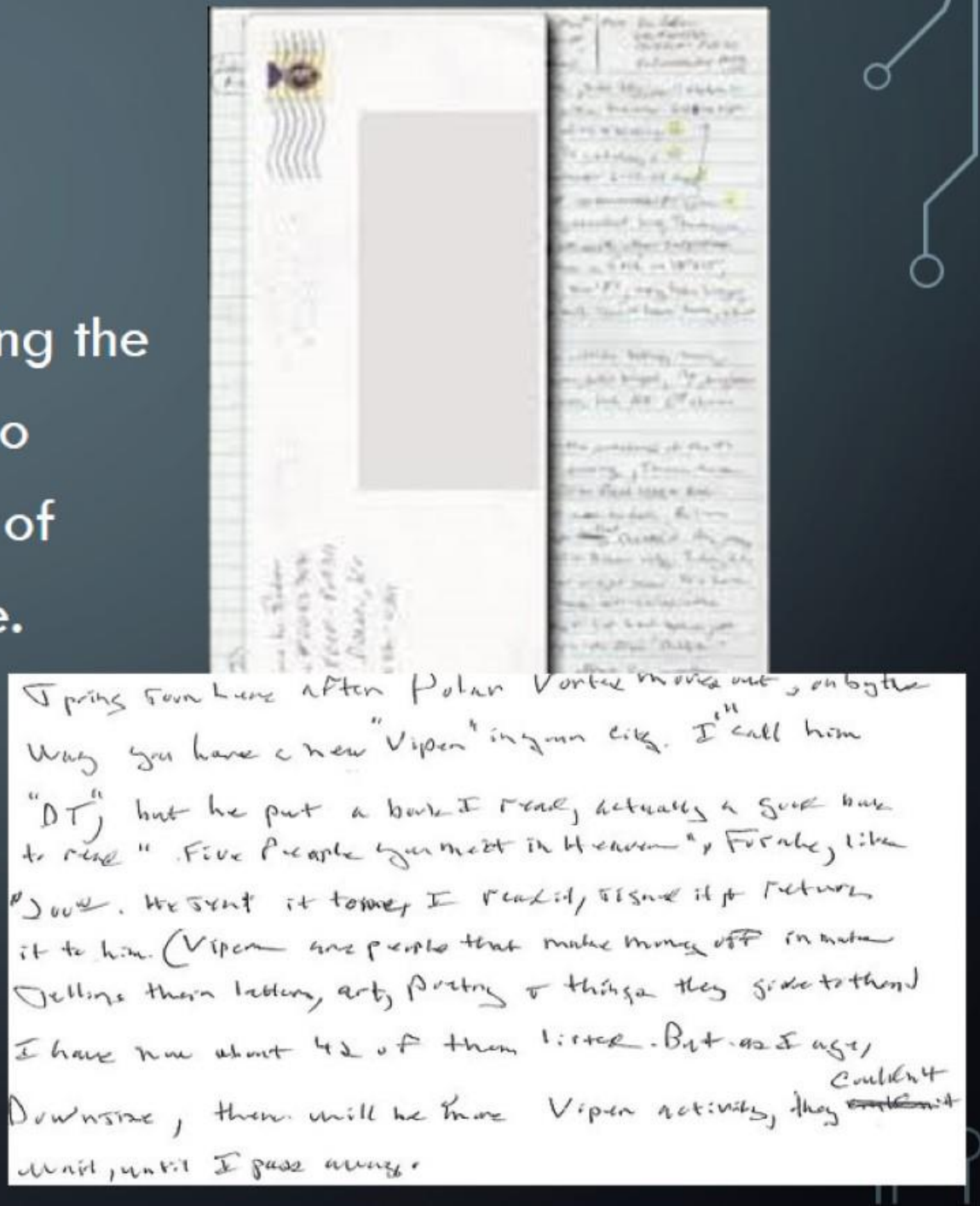
# CASE #1

# SERIAL KILLER BTK

- BTK stands for "Bind, Torture, Kill" which describe his typical modus operandi.
- At least 10 murders between 1974 and 1991 around area of Wichita, Kansas.
- Stalked his victims. Kept souvenirs. Killed mainly by strangling victims.

# SERIAL KILLER BTK

- He sent a number of letters describing the details of the killings to police and to local news media during the period of time in which the murders took place.



# DIGITAL EVIDENCE

- BTK sends one of his letters to police on floppy disk.
- Digital Forensic Examiners examine the disk, which contained a Microsoft Word document.
- The document data contained information about the software's registration and registered user.
- The software was registered to a Lutheran Church and the user's name was "Dennis"
- They found a "Dennis Rader" working for a Lutheran church as a Deacon.



Two of the envelopes from the letters Rader sent to TV stations and newspapers.

Package #11, sent to the Fox News affiliate in Wichita, containing the disk that linked Rader to the BTK crimes and proof of one of them.

# DENNIS RADER'S HISTORY

- College educated.
- Married, with two children.
- Deacon and president of the Lutheran church's congregation council.
- Boy-scout troop leader.

# RADER'S SENTENCE

- Found guilty in August 2005, received 10 consecutive life sentences.
- Will probably serve his sentence in solitary confinement for his own protection.
- Confined to a cell 23 hours a day with one-hour exercise and a shower three times per week.

# CASE #2

# ALICIA KOZAKIEWICZ ABDUCTION

- Alicia Kozakiewicz
- 13-year-old girl
- Abducted from Pittsburgh area on Jan 1, 2002.
- Left or was abducted from home without money, coat, or talking to anyone in the family.

# ALICIA KOZAKIEWICZ ABDUCTION

- FBI begin by searching her computer.
  Chat logs with "dcsadist" and email address
- Received tip from man from Tampa who had seen the chats. He knew him as "Scott from VA" and had seen Alicia on Scott's webcam and connected her to the Pittsburgh abduction via the news.
- Police traced the contact information which led them to Scott William Tyree.

# ALICIA KOZAKIEWICZ FOUND

- Alicia was held hostage, tortured and sexually assaulted for four days in a weapon-filled dungeon. Leather collar around her neck, she had been chained to the floor.
- Police rescued her on the fourth day of her ordeal, finding her locked in a bedroom.
- She does speaking engagements to warn others about dangers of Internet predators, even today more than 10 years later!

# SCOTT WILLIAM TYREE

- 38-year-old computer programmer.
- Arrested by FBI on Jan 4, 2002 in Herndon, Virginia
- Pleaded guilty and was sentenced to nearly 20 years in prison.
- February 1, 2019 he was released from prison to a halfway house, in Pittsburgh(!), with no notification to the victim or her family.

# CASE #3

# INFAMOUS HACKER

- Kevin Mitnick, infamous computer hacker/phreaker.
- Hacked into his first computer network in 1979, at 16. He broke into DEC's computer network and stole their software.
- Criminally charged and convicted in 1988.

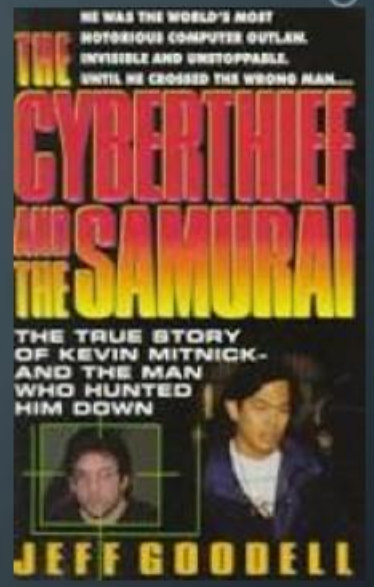
# MORE CRIMES

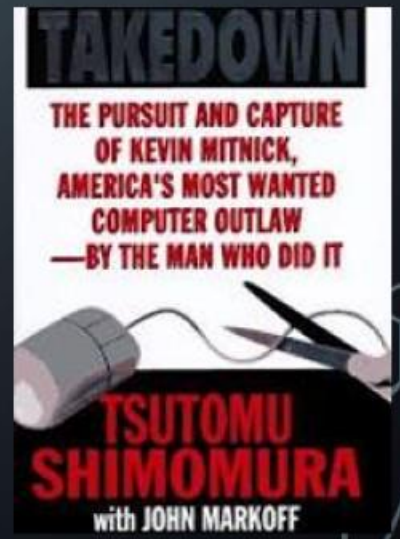
- Gaining full administrator privileges to an IBM minicomputer at the Computer Learning Center in Los Angeles in order to win a bet.
- Hacking Motorola, NEC, Nokia, Sun Microsystems and Fujitsu Siemens systems.
- Stole computer manuals from a Pacific Bell telephone switching center in Los Angeles.
- Read the e-mail of computer security officials at MCI Communication.
- Wiretapped the California DMV.


WANTED
BY U.S. MARSHALS

# TAKEDOWN – GEEK WAR

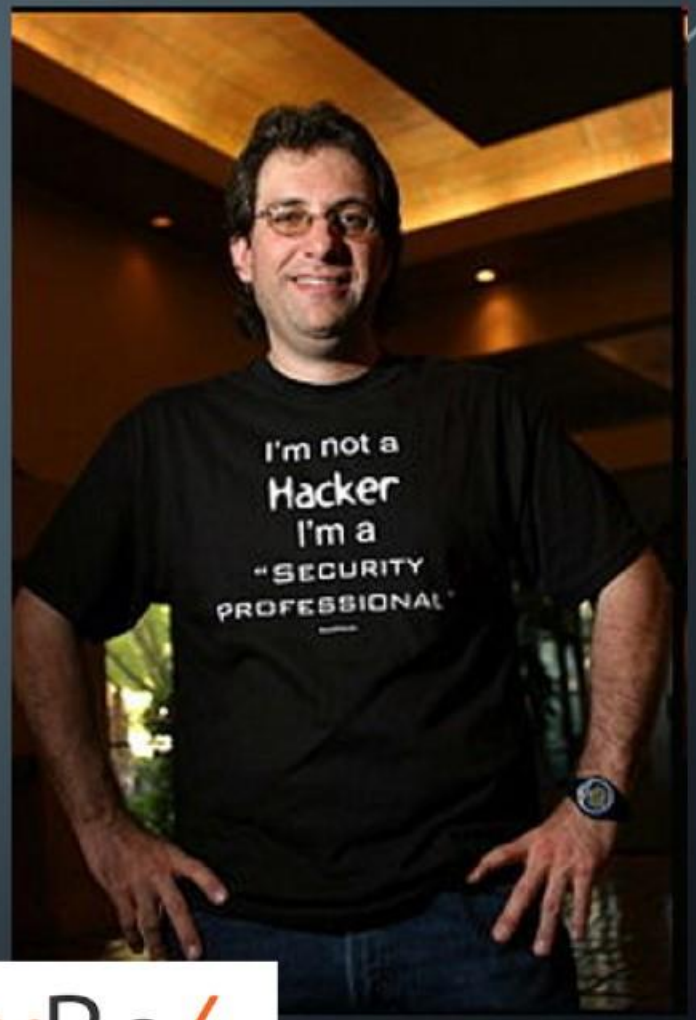
- On February 1995, in Raleigh, North Carolina, FBI (with civilian and telecom aid) arrested Mitnick on federal offenses related to a 2½-year period of computer hacking.
- He pled guilty to several offenses and was sentenced to 46 months in prison. Eight months were in solitary confinement because prosecutors convinced the judge that he had the ability to "start a nuclear war by whistling into a pay phone".
- He was released on January 21, 2000.
- His supervised release ended on January 21, 2003.



# KEVIN MITNICK TODAY!

- Now a famous computer security professional.
  - "Mitnick Security Consulting
  - KnowBe4
- But, in July 2009 Mitnick's company servers were hacked.




KnowBe4
Human error. Conquered.

KEVIN MITNICK
Security Awareness Training

# THANK YOU!

- Contact Information
  - Pamela King
  - Chestnut Hill College
  - kingp@chc.edu