2024 SEARCH Membership Group Winter Meeting

SEARCH Program Spotlight: Cybercrime and Digital Forensics

Cybercrime & Digital Forensics
2024
The Team

Timothy Lott - Director

Lauren Wagner – Program Manager

Eric Jollymore – Digital Evidence Forensic Analyst

John Trenary – Linn County Sheriff’s Office

Christopher Dale – Albany Police Department

George Vasiliou – California Highway Patrol (Ret.)

Melinda Gobron – Sacramento County Sheriff’s Office (Ret.)

Robert Weaver – Springfield Police Department

Jonathan Funkhouser – Lake Oswego Police Department

Fred Sanks – United States Secret Service

Scott King – Albany Police Department (Ret.)
Cybercrime and Digital Forensics

Cybercrime Training and Technical Assistance
- ICAC Training
- Hands-on Technical Assistance
- ISP List

Digital Forensic Services
- California Department of Justice
- State of Vermont

Information Systems Security
- Emerging line of business
- Direct services to the Membership
In-person courses / Online courses

- Leveraging Social Media: Open-Source Intelligence
- Peer-to-Peer Investigations
- Introduction to Cybercrime
- Digital Forensics for Prosecutors (partnership with NDAA)
- Cybercrime Investigations for Prosecutors (partnership with NDAA)
- Nemesis (partnership with Child Rescue Coalition)
- Mobile Device Forensics for Investigators (under development)
- Freeware Forensics (under development)
- Excel for Investigations (online course)
Cybercrime and Digital Forensics Training

• Conference sessions
  ◦ OSINT
  ◦ Digital Forensics
  ◦ Artificial Intelligence
  ◦ Data Analysis
2023 Law Enforcement Persons Trained

Personnel Trained in 2023:

- California: 351
- Texas: 56
- Florida: 209
- New York: 125
- Other states: (various numbers)

Total: 2,679
2023 Technical Assistance Engagements

290 Technical Assistance Engagements
• Colchester Vermont
  ◦ Threat of violence to a school through an online video game
  ◦ Provided contact information for the platform and various investigative techniques that could identify a suspect
  ◦ Suspect identified and admitted to making the threats
• Law Enforcement Officer attended SEARCH OSINT class
  ◦ Deputy was called in to assist with a sex offense
  ◦ Offense happened in 2010
  ◦ Through techniques learned in the course the deputy was able to recover an old email account which revealed incriminating messages from the suspect
  ◦ Suspect was arrested
Other Resources

• Internet Service Provider List
  ◦ Over 3000 individual records
  ◦ **1.35 million** hits in 2023

• 77 Law Enforcement Guides
  ◦ Distributed over 24,500 in 2023

• White Papers
  ◦ Distributed over 1300 in 2023
Digital Forensics Services

• California Department of Justice – Medicare Fraud and Elder Abuse
• State of Vermont
• Established in Summer of 2021
• Assisted in the execution of 7 search warrants
  ◦ Multiple locations per warrant
• Processed 350 comprehensive forensic examinations
• Over 85 TB of data processed
• Charging decisions based off of SEARCH work
State of Vermont

• One time contract with the Attorney General’s office
• Examination of digital files on SharePoint
• Goals
  ◦ Provide direct services to the SEARCH Membership on protecting sensitive systems
  ◦ Expand training and services to state and local law enforcement agencies
  ◦ Assist agencies with the development of checklists to assist in maintaining security
Future Projects

• Expanding the digital forensics program
• Pursue additional federal funding
• Working with Artificial Intelligence
2024 SEARCH Membership Group Winter Meeting

A.I. Awareness for Information Security

Cybercrime & Digital Forensics

2024
Objectives

• Gain an understanding of
  ◦ What is Artificial Intelligence
  ◦ What are the different types of A.I. available
  ◦ How A.I. is making it easier to be a threat to an organization
What is Artificial Intelligence?

- **Artificial Intelligence**
  - A subfield of computer science that focuses on enabling machines to:
    - Process information
    - Make decisions
    - Solve problems.

- **There are several A.I. types currently available.**
What is Artificial Intelligence?

• Machine Learning (ML)
  ◦ Subset of AI that enables machines to improve at tasks with experience.
    ◦ Netflix Recommendations
    ◦ Spotify Recommended Music
    ◦ Amazon Recommended Purchases
There are several definitions of Artificial Intelligence (AI) that are circulating. The most common is from John McCarthy at Stanford:

“It is the science and engineering of making intelligent machines, especially intelligent computer program.”
What is Artificial Intelligence?

- Natural Language Processing (NLP)
  - Involves interactions between computers and human language. It enables machines to understand and respond to humans.
    - Siri
    - Google Translate
What is Artificial Intelligence?

• **Robotics**
  ◦ Robots designed to perform tasks automatously or semi-automatously.
    ◦ Boston Dynamics
    ◦ Auto Manufacturing
• Generative Adversarial Networks (GANs)
  ◦ Generator: Part of network that generates new data
  ◦ Discriminator: Part of network that evaluates real data against generated data to improve capabilities over time.
    ◦ Image/Video Generation
    ◦ Audio Generation
What is Artificial Intelligence?

- Generative Adversarial Networks (GANs)
  - Generator: Part of network that generates new data
  - Discriminator: Part of network that evaluates real data against generated data to improve capabilities over time.

  - Image/Video Generation
  - Audio Generation

© SEARCH, The National Consortium for Justice Information and Statistics | search.org
What is Artificial Intelligence?
What is Artificial Intelligence?

• **Generative Pretrained Transformer (GPT):**
  ◦ Designed to generate human-like text by predicting the next word in a sentence given all previous words in the statement.
  ◦ Trained on a diverse range of text found on the Internet.
Concerns for Data Security

• Where does AI pose a threat to data security today?
  ◦ Lowering the bar for malicious actors to pose a threat.

• Ability to learn and detect patterns in speech, text and video easier.

• Ability to digest large amounts of publicly accessible information faster.

• Ability to assault password technologies with less thinking.
Concerns for Data Security

• Where does AI pose a threat to data security today?
  ◦ Lowering the bar for malicious actors to pose a threat.
    ◦ Source: World Economic Forum, 2024
Concerns for Data Security

• Ability to learn and detect patterns in speech, text and video easier.
Concerns for Data Security

• Ability to learn and detect patterns in speech, text and video easier.
Concerns for Data Security

• Ability to learn and detect patterns in speech, text and video easier.
Concerns for Data Security

• Ability to digest large amounts of publicly accessible information faster.
Concerns for Data Security

• Ability to digest large amounts of publicly accessible information faster.

• Public AI solutions like ChatGPT often have guardrails to minimize it’s weaponization.
• Offline AI / GPT resources area already freely available and they do not contain guardrails.
Concerns for Data Security
Concerns for Data Security

• Ability to digest large amounts of publicly accessible information faster.
Concerns for Data Security
Concerns for Data Security
Concerns for Data Security

• Ability to assault password technologies with less thinking.

“The mother of all breaches”: 26 billion records found online

Security researchers have discovered billions of exposed records online, calling it the “mother of all breaches”.

Posted: January 23, 2024 by Pieter Amtz
• Ability to assault on password technologies with less thinking.
• As this new emerging threat continues to evolve it remains important to focus on getting the fundamentals right.

  ◦ Be wary about urgency and pressure.

  ◦ Advocate “Thinking Before You Click”.

Concerns for Data Security
As this new emerging threat continues to evolve it remains important to focus on getting the fundamentals right.

- Create strong, unique passwords for each account. No more “Winter2024”.

- Enable Multi-Factor Authentication at any opportunity.
As this new emerging threat continues to evolve it remains important to focus on getting the fundamentals right.

- Test competency of those who are entrusted with sensitive data.

- Encourage your users to reach out and verify the authenticity of a request whenever it seems even slightly suspicious.
Questions?