


May 15, 2023  
Cyber Forensics (Digital Dust)  
PWC G8 Gals@Technology

1



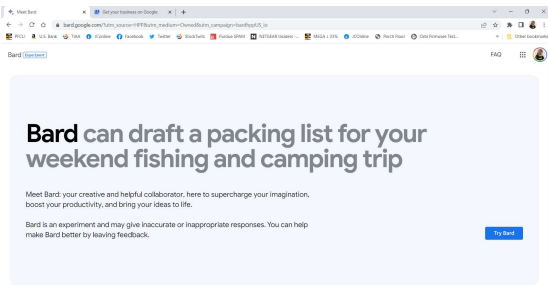
ELECTRONICS

WILDT

"I'm the oldest employee in the store...  
I've been here from Hi-Fi to WiFi."

### Current Topics

- Google Bard



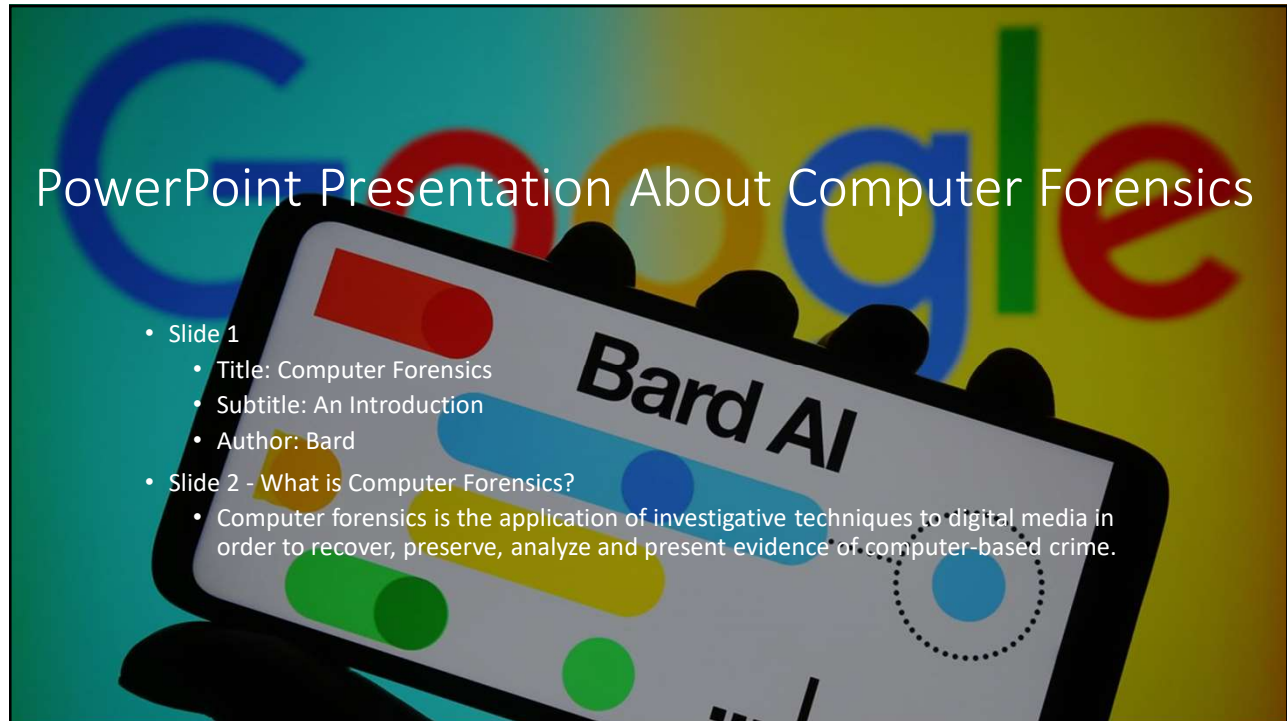
**Bard can draft a packing list for your weekend fishing and camping trip**

Meet Bard: your creative and helpful collaborator, here to supercharge your imagination, boost your productivity, and bring your ideas to life.

Bard is an experiment and may give inaccurate or inappropriate responses. You can help make Bard better by leaving feedback.

try it

2



# PowerPoint Presentation About Computer Forensics

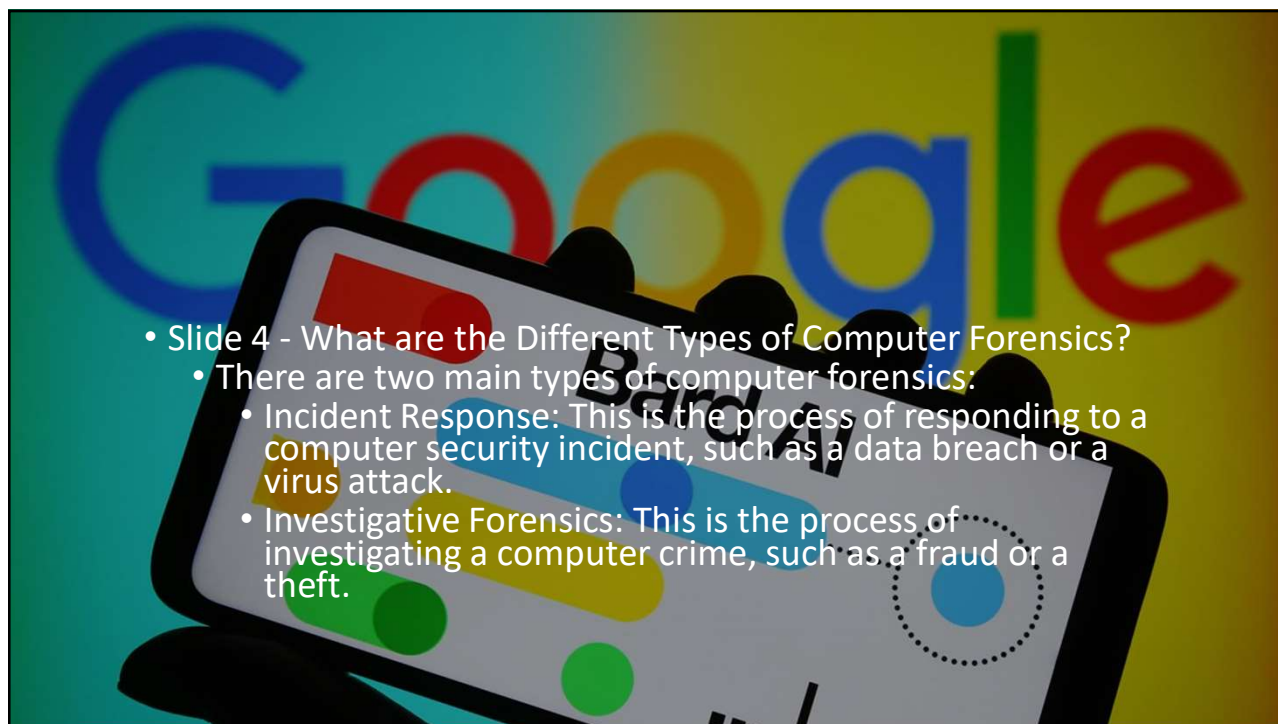
- Slide 1
  - Title: Computer Forensics
  - Subtitle: An Introduction
  - Author: Bard
- Slide 2 - What is Computer Forensics?
  - Computer forensics is the application of investigative techniques to digital media in order to recover, preserve, analyze and present evidence of computer-based crime.

3



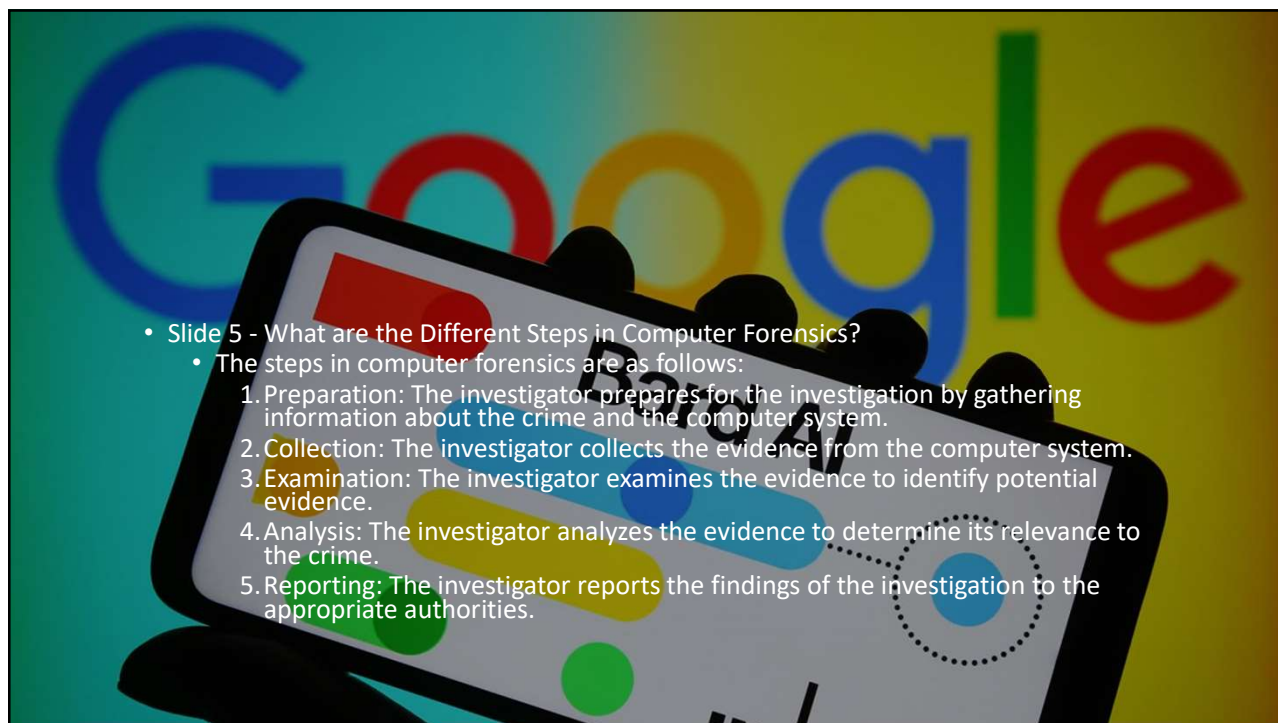
- Slide 3 - Why is Computer Forensics Important?
  - Computer forensics is important because it can be used to:
    - Recover evidence of computer-based crime
    - Preserve evidence for legal proceedings
    - Investigate data breaches
    - Identify cyber threats
    - Solve computer-related crimes

4



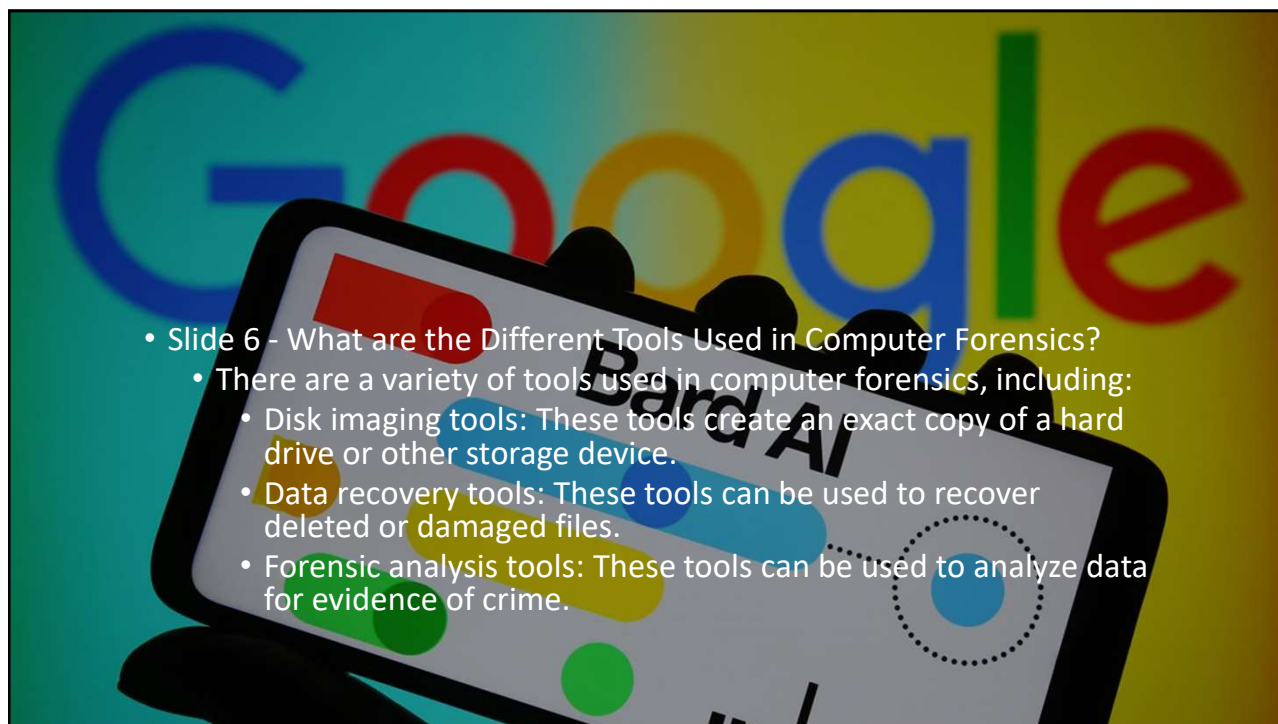
- Slide 4 - What are the Different Types of Computer Forensics?
  - There are two main types of computer forensics:
    - Incident Response: This is the process of responding to a computer security incident, such as a data breach or a virus attack.
    - Investigative Forensics: This is the process of investigating a computer crime, such as a fraud or a theft.

5



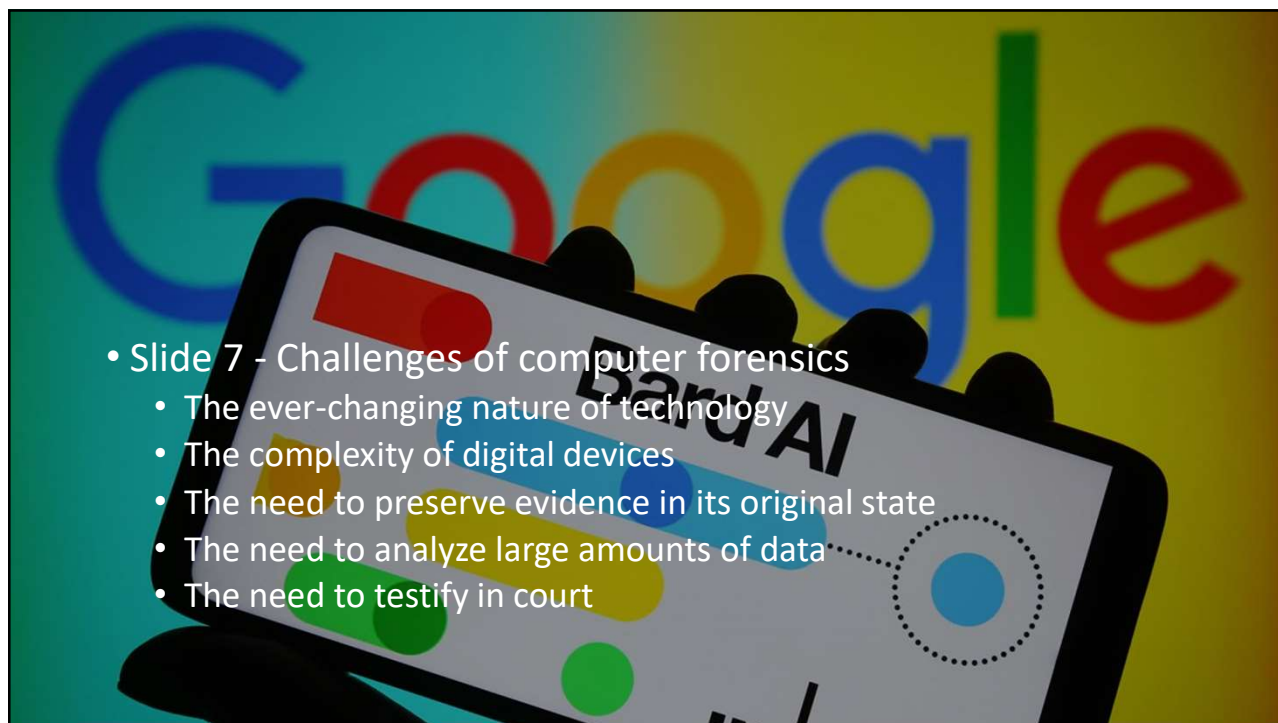
- Slide 5 - What are the Different Steps in Computer Forensics?
  - The steps in computer forensics are as follows:
    1. Preparation: The investigator prepares for the investigation by gathering information about the crime and the computer system.
    2. Collection: The investigator collects the evidence from the computer system.
    3. Examination: The investigator examines the evidence to identify potential evidence.
    4. Analysis: The investigator analyzes the evidence to determine its relevance to the crime.
    5. Reporting: The investigator reports the findings of the investigation to the appropriate authorities.

6



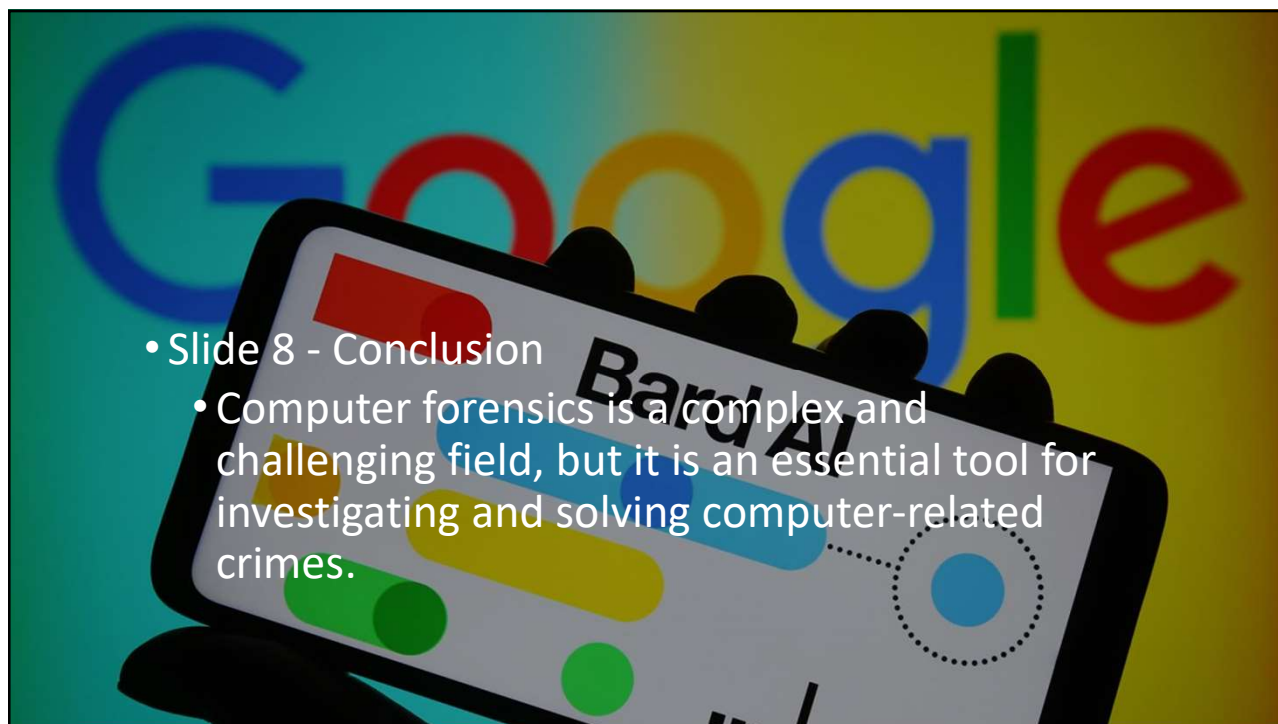
- Slide 6 - What are the Different Tools Used in Computer Forensics?
  - There are a variety of tools used in computer forensics, including:
    - Disk imaging tools: These tools create an exact copy of a hard drive or other storage device.
    - Data recovery tools: These tools can be used to recover deleted or damaged files.
    - Forensic analysis tools: These tools can be used to analyze data for evidence of crime.

7



- Slide 7 - Challenges of computer forensics
  - The ever-changing nature of technology
  - The complexity of digital devices
  - The need to preserve evidence in its original state
  - The need to analyze large amounts of data
  - The need to testify in court

8




9

## Locard's Exchange Principle

"Every Contact Leaves a Trace"

The value of trace (or contact) forensic evidence was first recognized by Edmund Locard in 1910. He was the director of the very first crime laboratory in existence, located in Lyon, France.



The Locard's Exchange Principle states that "with contact between two items, there will be an exchange." For example, burglars will leave traces of their presence behind and will also take traces with them. They may leave hairs from their body or fibers from their clothing behind and they may take carpet fibers away with them.

10

## You have seen this in Pop Culture

- Locard's principle is mentioned in the sixteenth episode of CSI: Crime Scene Investigation, "Too Tough to Die", aired on 1 March 2001.[20]
- "Locard's Exchange" is the title of episode#75 of the television medical drama Crossing Jordan, aired on 10 April 2005.
- "Locard's exchange principle" is mentioned near the end of chapter 17 in the novel "Break No Bones" by Kathy Reichs.
- "The Locard exchange principle" is mentioned in the Jemima Shore novel, "Cool Repentance", by Antonia Fraser.
- "The Locard exchange principle" is mentioned in the novel The Bone Collector, by Jeffery Deaver.
- "The Locard exchange principle" is mentioned in the novel I Am Pilgrim, by Terry Hayes.
- "The Locard exchange principle" is described as "transference" in the 2002 film, Murder by Numbers.
- The exchange principle is mentioned while Dexter is examining Cassie's body in an episode of the final season of Dexter. S08 E08 'Are We There Yet?'
- "The Locard exchange principle" is mentioned in the final episode of 2018 drama, Queen of Mystery 2.
- "Locard's exchange principle" is mentioned in season 1, episode 12 of the detective drama Day and Night.
- And many more .....

11

## History & Development

- Francis Galton (1822-1911)
  - First definitive study of fingerprints
- Sir Arthur Conan Doyle (1887)
  - Sherlock Holmes mysteries
- Leone Lattes (1887-1954)
  - Discovered blood groupings (A,B,AB, & O)
- Calvin Goddard (1891-1955)
  - Firearms and comparison
- Albert Osborn (1858-1946)
  - Developed principles of document examination
- Hans Gross (1847-1915)
  - First treatise on using scientific disciplines in criminal investigations.
- First FBI CART Team (1984)
- Digital "wing" of the American Academy of Forensic Science (2007)



12

## Forensic Mindset

- Digital Forensic Mindset – Condensed Definition:
  - Using your skills to determine what has occurred or,
  - What most likely occurred as opposed to what is possible
  - You do NOT work for anyone but the TRUTH!
- The tools used are not nearly as important as the person using them!



13

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

*Crime investigation: physical evidence and the police laboratory.*  
Interscience Publishers, Inc.: New York, 1953

14

# Where It Began For Me October 14, 1999

- Student Suicide in ME Building
- Left electronic suicide note
- Called by PUPD to “print the screen”
- Time of death in question
- My first meeting with “Doc” (Martin Avolt, DVM)
- First discussion between PUPD and Coroner about “Computer Forensics”

INDIANA STATE DEPARTMENT OF HEALTH  
CERTIFICATE OF DEATH

Local No. 99-1132 State No. 036505

DECEASED NAME: Brian Michael Strickland  
 SEX: Male  
 RACE: White  
 DATE OF BIRTH: 8/03/75  
 DATE OF DEATH: 10/14/99

PERMANENT RESIDENCE: 1288 Mechanical Engineering Building, West Lafayette, IN 47906  
 PLACE OF DEATH: University Building, West Lafayette, IN 47906

DECEASED'S US RESIDENCE: Indiana  
 COUNTY: West Lafayette  
 CITY/TOWN: West Lafayette

DATE OF DEATH: 10/14/99  
 TIME OF DEATH: 12:00 PM  
 PLACE OF DEATH: University Building

CAUSE OF DEATH: Asphyxia - Due To hanging

DECEASED'S SIGNATURE: [Signature]  
 WITNESS SIGNATURE: [Signature]  
 HEALTH OFFICER SIGNATURE: [Signature]

15

## “The Device” and “The Network”

- Device as **Target** of the incident
  - Get to instructor's test preparation
  - Access someone else's homework
  - Access/Change a grade
  - Access financial information
  - “Denial of Service”
- Device as **Tool** of the incident
  - Word processing used to create plagiarized work
  - E-mail sent as threat or harassment
  - Printing used to create counterfeit material
- Device as **Incidental** to the incident (a **Witness**)
  - E-mail/file access used to establish date/timelines
  - Stored names and addresses of contacts or others potentially involved in the incident
  - Modile Device Evidence
  - Video Evidence
  - Automobile Evidence



16



## The Objectives of a Forensic Examination

---



- Conduct a **repeatable** and **verifiable** examination of “digital evidence” using established practices and procedures
- Successfully communicate results of the examination to the “trier of fact”
- Examiner must be a “teacher” as well as witness
- Maturing from “black art” to “science”
  - Computers – relatively mature
  - Mobile devices – close to mature
  - Video evidence – coming along quickly
  - Automotice evidence – wild, wild west

17


## Basic Methodology

---

- The Three A’s
  - **A**cquire
  - **A**uthenticate
  - **A**nalyze



18

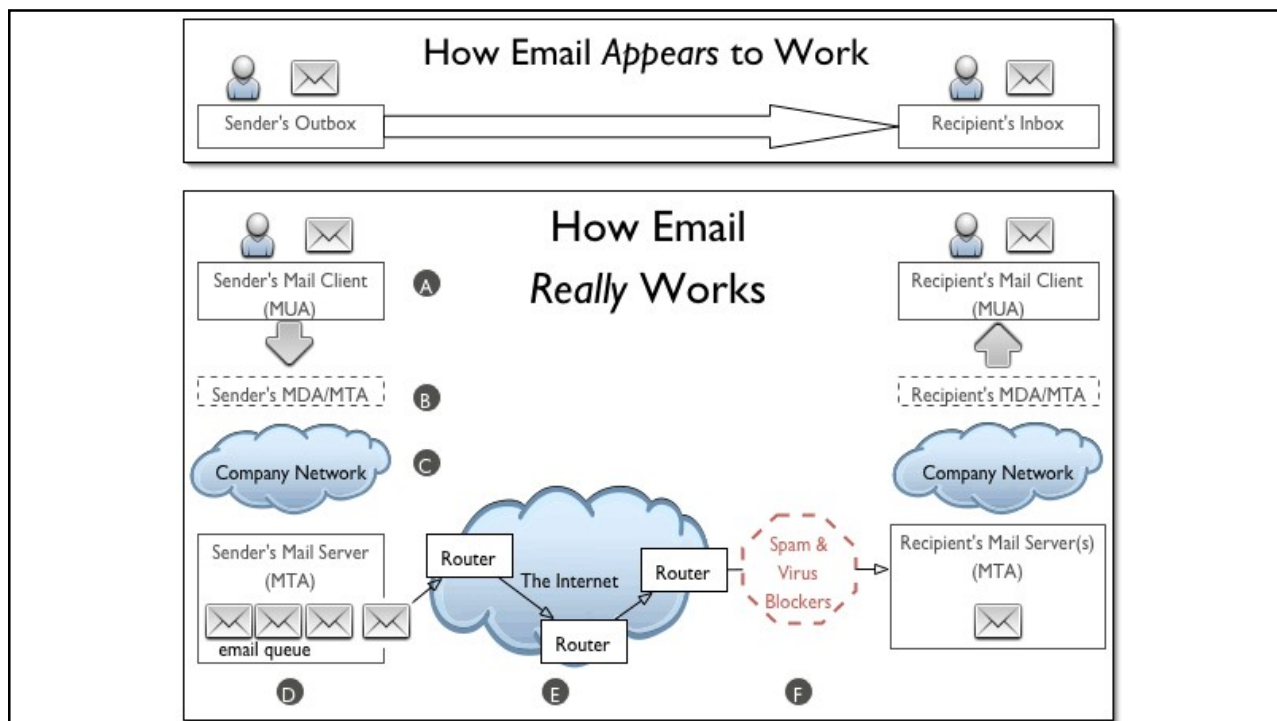


## General Types of Digital Forensics

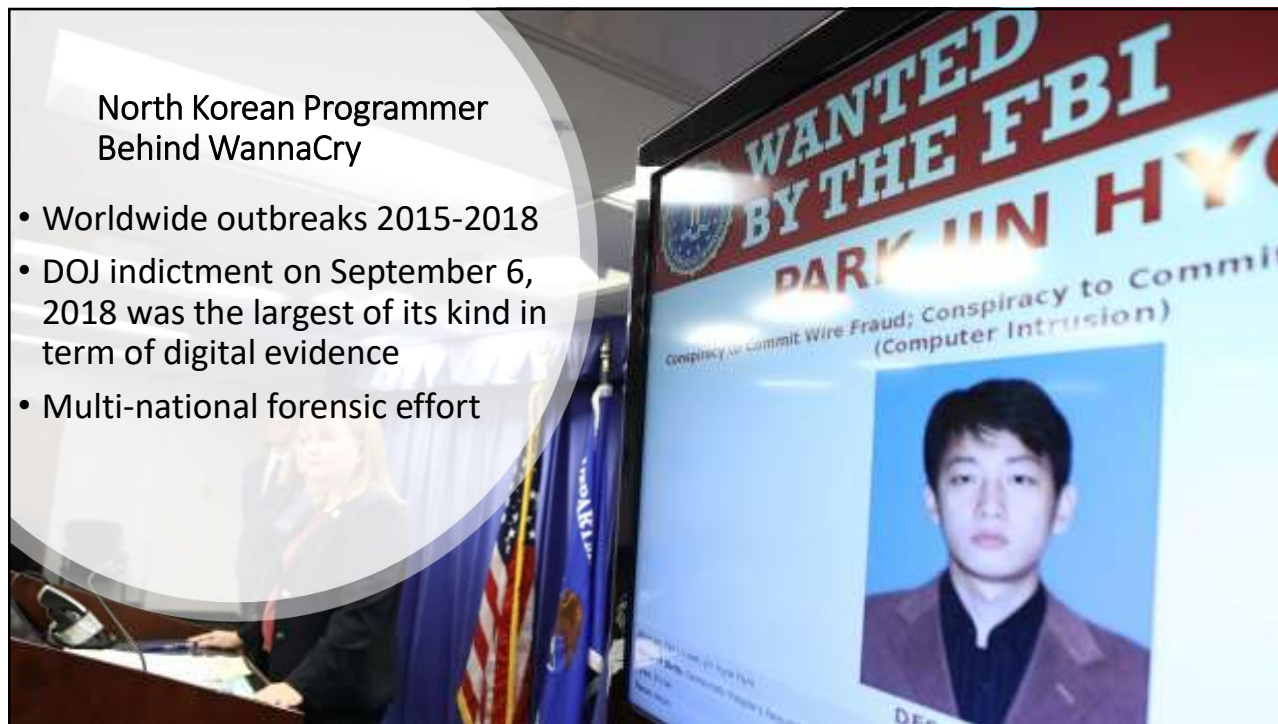
- “Network” Analysis
  - Communication analysis
  - Log analysis
  - Path tracing (what talked to what, when, why)
- Media Analysis
  - Disk imaging
  - MAC time analysis (Modify, Access, Create)
  - Content analysis
  - Slack space analysis (left over unerased memory)
- Code Analysis
  - Reverse engineering
  - Malicious code review
  - Exploit Review

The “puzzle” is a combination of all the above pieces

19



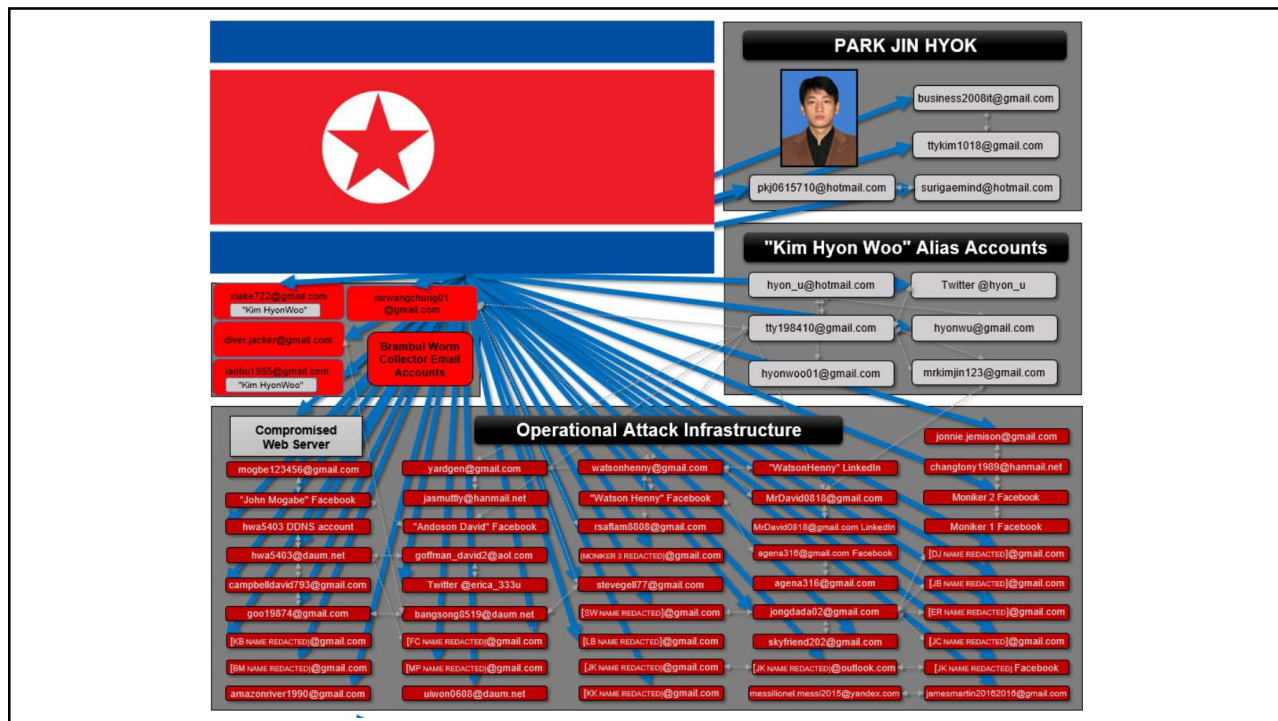
20



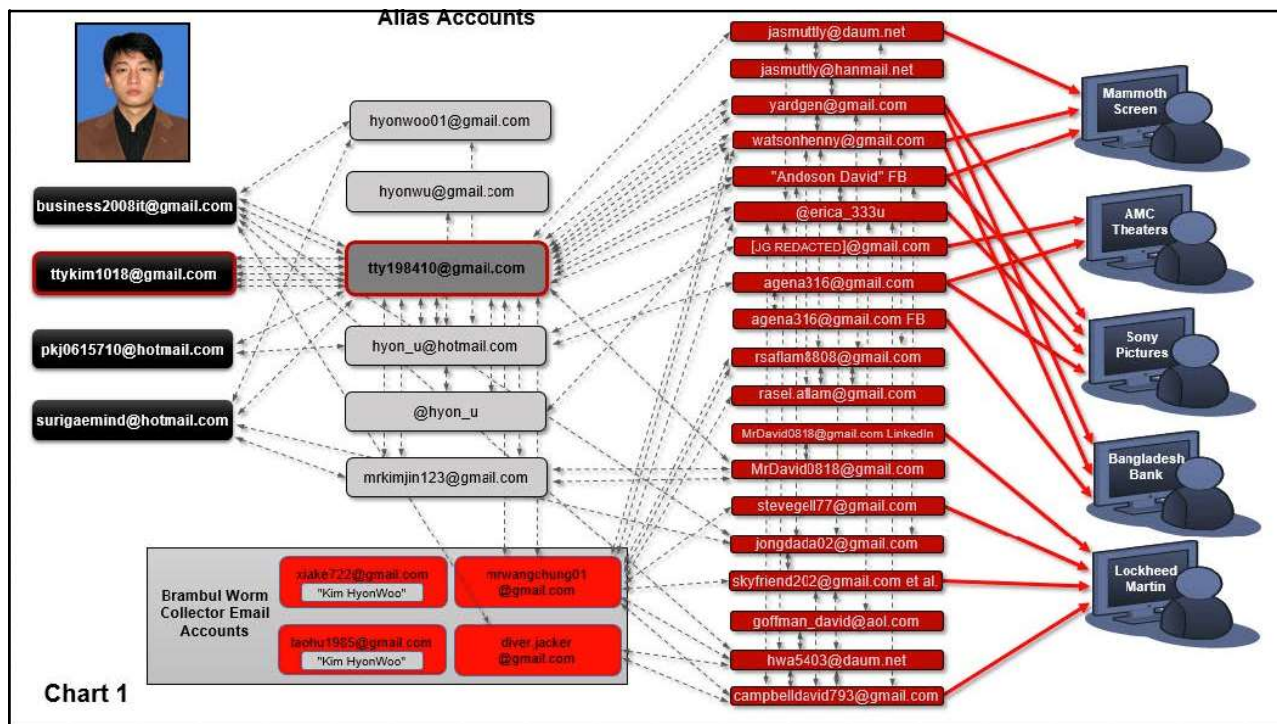
North Korean Programmer Behind WannaCry

- Worldwide outbreaks 2015-2018
- DOJ indictment on September 6, 2018 was the largest of its kind in term of digital evidence
- Multi-national forensic effort

21



22



23

## Mobile Device Forensics

- Incoming, outgoing, missed call history
- Phonebook or contact lists
- SMS text, application based, and multimedia messaging content
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browsing history, content, cookies, search history, analytics information
- To-do lists, notes, calendar entries, ringtones
- Documents, spreadsheets, presentation files and other user-created data
- Passwords, passcodes, swipe codes, user account credentials
- Historical geolocation data, cell phone tower related location data, Wi-Fi connection information
- User dictionary content
- Data from various installed apps
- System files, usage logs, error messages
- Deleted data from all of the above



24

## Credit For Current Info To


- **Master Detective Jason Leitze | CFVT | MCVE**
  - 21 years in law enforcement
  - Indiana Capitol Police
  - Marion County Sheriff / Indianapolis Metro P.D.
    - 2 years district detective / 9 years robbery & aggravated assault detective
    - 5 years video forensics detective (now digital forensics)
- **Detective Nick Clark | CFVT | MCVE**
  - 13 years in law enforcement
  - Indianapolis Metro P.D.
    - 6 years Incident Analysis Center detective
    - 3 years video forensics detective (now digital forensics)

25




26

## DVR/NVR/Cloud What's the difference?




**DVR**

- Local storage
- May or May Not be Internet Connected
- Analog Cameras (Coaxial cables)



**NVR**

- Local storage
- Likely to be Internet Connected
- IP/Ethernet Cables



**Cloud**

- Internet Connected, Cloud storage, micro-SD card storage
- Cloud systems change faster than we can observe
- Do some research on scene first, if needed.
- Will need owner cooperation or warrant to acquire video from Service Provider

27

## Legal

- **Federal Rules of Evidence**
  - 1001(d) - ...For electronically stored information, "original" means any printout (ex. Images) — or other output readable by sight — if it accurately reflects the information.
  - 1001(e) - A "duplicate" means a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original.
  - 1003 - A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity, or the circumstances make it unfair to admit the duplicate.
- **Court of Appeals**
  - Stott v State of Indiana (Marion County Case)
    - "It is no secret that it is increasingly easier in today's digital age to manipulate or distort images. See, e.g., 2 McCormick on Evid. § 215 n.17 (8th ed. 2020). Without suggesting any malfeasance in this case, we reiterate that it is the proponent's burden to establish the strong showing of authenticity and competency for the admissibility of photographs used as substantive evidence under the silent-witness theory. The State did not do so here. And thus, the trial [\*\*23] court abused its discretion in admitting the cell-phone photographs of the surveillance-footage."

28

## Working with Video

- Training is critical. Video is not always what it appears to be. Practitioners who are not properly trained may be unaware of the technical issues with video, such as dropped frames or distorted aspect ratios, and may mistakenly assume the cursory playback as truth.
- 85% of cases involve video evidence, and the number of video files are growing rapidly at a 94% CAGR (compound annual growth rate) since 2013\*

\* Steve Paxton. (February 2020). The massive growth of video evidence: What police administrators need to know. Police1.com.

29

## Why Proper Handling of Video Matters: Obtaining Original Video & Proper Conversion Ottawa: *In custody death – officers criminally charged*



30

Why Proper Handling of Video Matters:  
Obtaining Original Video & Proper Conversion  
Ottawa: *In custody death – officers found not guilty*



31

Infrared  
"Night Vision"



32





33



34

# Perspective

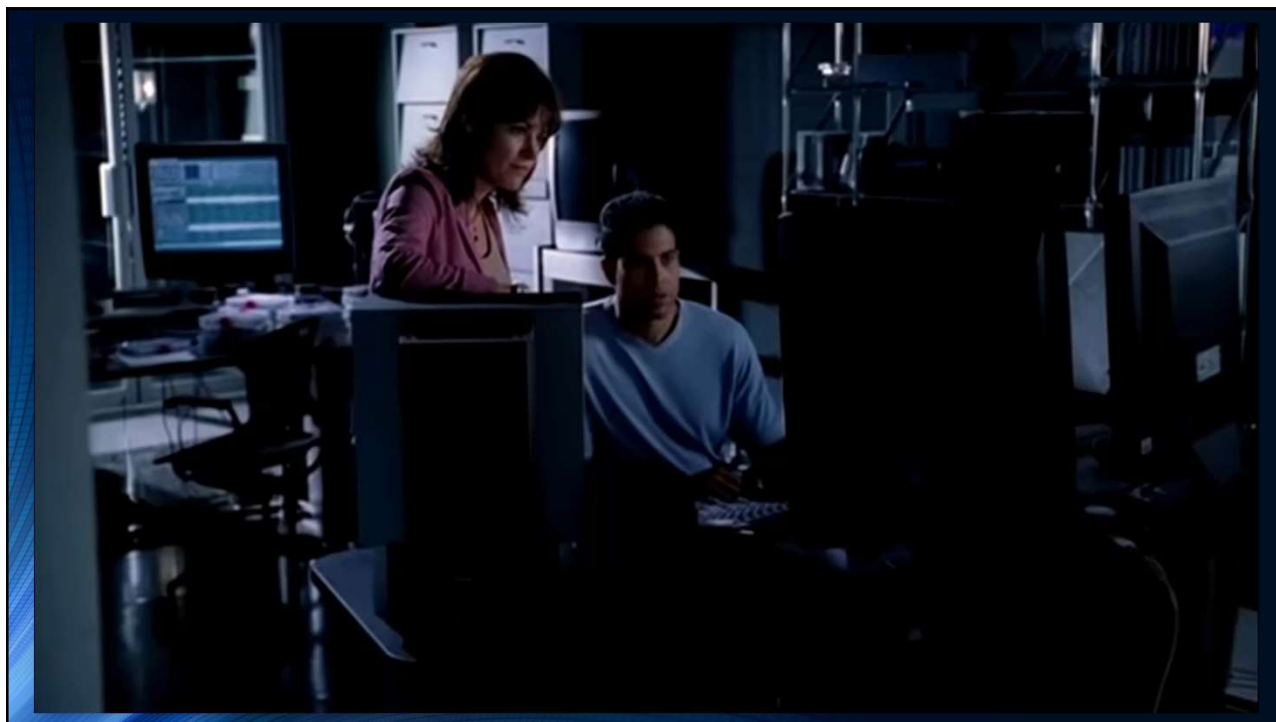


35

# Can be very important



36



37

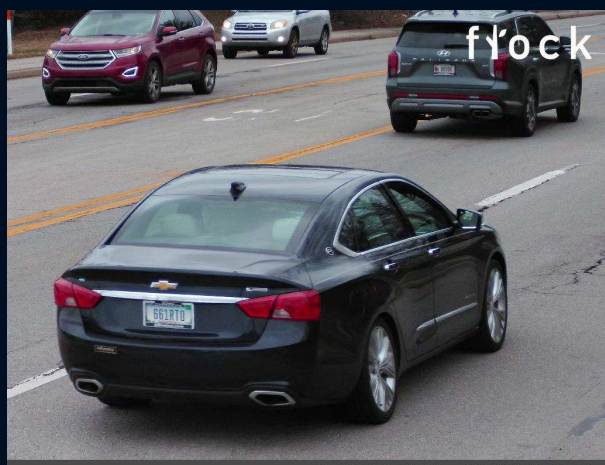
### Clarifications (i.e., "Enhancements")



While enhancements are often desired by law enforcement officers, with 95% of practitioners saying they recently had a case where they wanted to enhance a license plate, only 4% were able to make a marginal improvement through enhancement.

38

### Clarifications (i.e., "Enhancements")



Indianapolis IN Metro PD-#115 W 56th @ Lafayette 39, 85287073715705, -86.26266208901956 2/9/2023 13:05:01 EST

flock

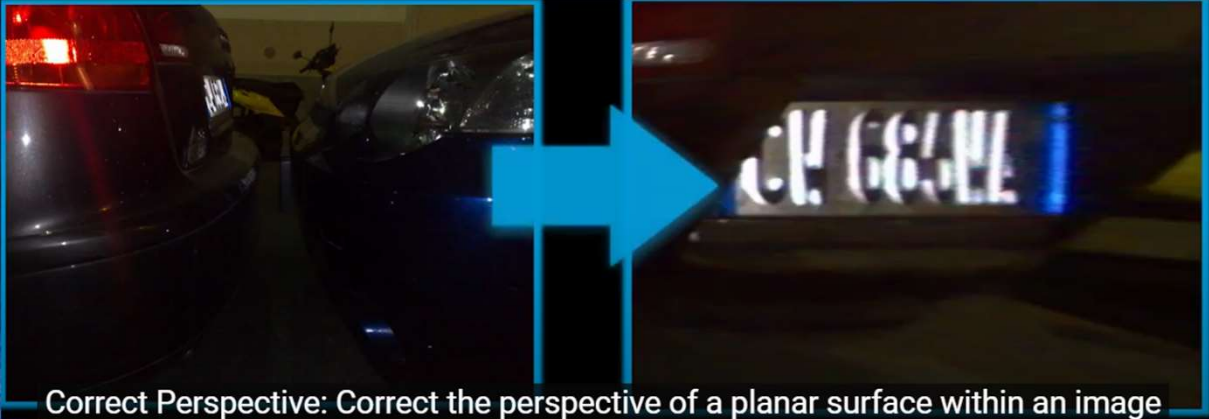
39

### Clarifications (i.e., "Enhancements")



40

### Clarifications aka. "Enhancements"



Correct Perspective: Correct the perspective of a planar surface within an image

41

### Clarifications aka. "Enhancements"



It depends!!!

42



## Vehicle Forensics


- **Wild Wild West of forensics**
  - Types of data available: Navigational, doors opening closing, seatbelts, throttle, speed, text messages, calls made/received, phones connected to car, other phones in car with Bluetooth on, video, etc....
  - Only about 50% of vehicles are supported, however this continues to increase.
  - Can be a very lengthy examination.
  - Very often requires removal of dash/center console/seats.
  - Likelihood to do damage to vehicle is very high. **Requires DFU supervisor approval!**
  - Vehicles are rarely done if you have suspect and have their phone.
  - Tesla and Rivian can be a gold mine for video(4K) if owner has the extra mode enabled(extra cost).

43

## Some Personal “Firsts”

- First meeting with Doc Avolt in early-90s regarding student death with digital suicide note
- First meeting with Chief Cox in mid-90s regarding WL death with computer system next to bathtub
- First murder case in 2001 regarding murder of two Purdue students in Purdue village
- First international case in 2005 regarding murder in Lafayette with body found in Illinois and suspect arrested and charged in China
- First Federal Court experience with 2006 case of Purdue student making threats against the US President and his family
- First time pretending to be an 18-year-old girl for chat with possible sexual attacker
- More porn and abuse cases than I care to remember

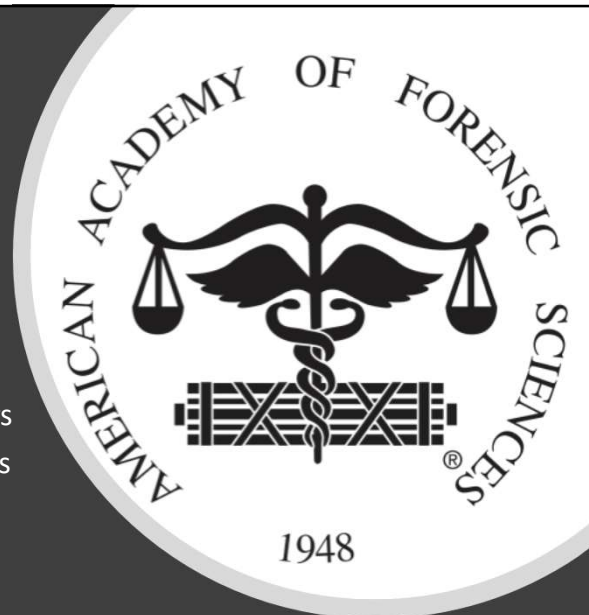
## Computer Forensics



44

## American Academy of Forensic Sciences

- Digital and Multimedia Sciences section established in 2010
- First new section in the Academy in over 50 years
- Three Purdue members in the initial 16 members
- Section now almost 200 members



45

We've come a long way ....

### HTCU Members

Purdue University Cyber Forensics Department  
 Tippecanoe County Prosecutors Office  
 Lafayette Police Department  
 West Lafayette Police Department  
 Purdue University Police Department  
 Tippecanoe County Sheriff's Department  
 Tippecanoe County Community Corrections  
 Tippecanoe County Probation Department



46


## Challenges Ahead

- The volume of data
  - Data Science
  - Data Mining
  - AI
- Worldwide legal issues
- The challenge of encryption
- Training examiners
- The cost of staying current
- Cloud forensics




47

Edmond Locard, also known as the "Sherlock Holmes of France" came up with a principle that states that **every contact by a criminal leaves behind a trace.**



"Elementary, my dear Watson!"



"I don't need to check anything with 'the boys in forensics', I know it was you."

48