INTRODUCTION TO DIGITAL FORENSICS

Dr. Nazli Hardy, MBA, Ph.D.

THE WIDE SPECTRUM COMPUTER SCIENCE

- Artificial Intelligence (AI)
- Networks
- Security
  - Digital Forensics
  - Steganography
  - Cryptography
- Human Computer Interaction (HCI)
- Software Engineering
- Video Game Programming
- Computational Logic
- … & much more…. impacting every industry

INTRODUCTION

- Why is the Study of Digital Forensics Relevant?
- What is Digital/Computer Forensics?
- What do you Need for a Careers in Computer Digital Forensics?
  - Educational Background
- Kinds of Cases a Computer/ Digital Forensics Expert Works on
- Let's Catch a Fake! You are the Computer Forensics Expert
  - Fake Photos
- Computer Forensic Resources for you
  - Job prospects
  - Certifications
  - Journals
  - Conferences

WHY IS THE STUDY OF DIGITAL FORENSICS RELEVANT?

Reality: Almost everything and anything we do online, can be and, probably is tracked …

- Social Networking (FB, Twitter, Pinterest…)
- Information Retrieval (Google , Bing, Yahoo ….)
- Personal Digital Devices (constant access online – smaller world) – iPhone, Android etc.
- Communication (Email, IM, VoIP incl. Skype, Vonage etc. …)
- GPS (we can track and … thus we are tracked)
- Video games (games and fitness)
- Stock market (the connected world economy, insider trading)
- IoT (Hey Alexa, Hi Siri …)
- … and so much more …

What does this indicate to you?
Let's discuss

WHAT IS DIGITAL FORENSICS?

- Digital forensics does not replace traditional forensic analysis
- But any action that modifies the crime scene could invalidate evidence in court

WHAT IS DIGITAL FORENSICS?

A branch of forensic science that pertains to **evidence** (criminal or civil) found in **computers and digital storage media**

Particularly important to legal cases at the present time because …?

Examples of the many functions that a digital forensics expert are responsible:

- Analysis of computer systems belonging to defendants (in criminal cases) or litigants (in civil cases)
- Recovering "deleted" data – using special software
- Determining how an attacker (e.g. from E. Europe, Asia) hacked the company database
- Investigate electronic data and evidence against an errant employee – conversely to uncover information about a company carrying out illegal activities online
- Building algorithms to help catch electronic fakes

What else?

DIGITAL FORENSICS PROCEDURES

Identification

Identify specific objects that store important data for the case a

Collection

Establish a chain of custody and document all steps to prove that the collected data remains intact and unaltered

Analysis & Evaluation

Determine the type of information stored on digital evidence and conduct a thorough analysis of the media

Reporting

Prepare and deliver an official report

Dr. Nazli Hardy, MBA, Ph.D.

WHAT DO YOU NEED FOR A CAREERS IN COMPUTER DIGITAL FORENSICS?

- For a career in digital forensics, it is helpful to have:

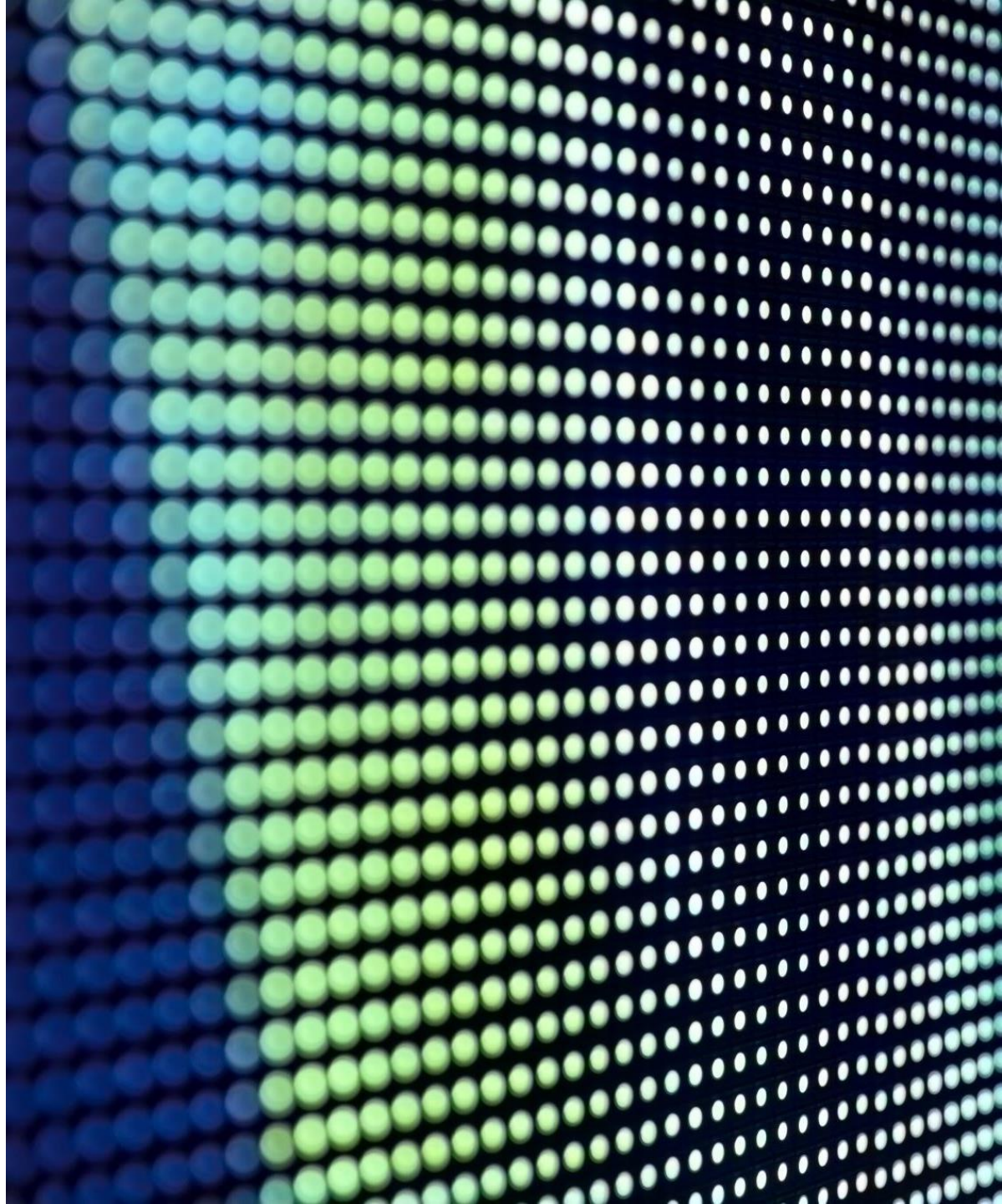
  - a degree related to computer science (CS) or information technology (IT) (with a minor in criminal justice) .
  - or a degree in criminal justice and a minor in CS/ IT
    - understanding of broad range of computer storage devices, computer architecture, operating systems, programming languages, software applications, databases, networking (IP addresses), security (cryptology), reverse software engineering, algorithms … and other CS concepts

  - computer forensics certifications (list at end of presentation)
    - up-to date forensic investigative knowledge and techniques
    - latest computer forensic tools and software
      - EnCase , Forensic Toolkit (FTK) & many others
    - latest "attacking tools"
      - such as keyloggers, password crackers, spoofing software & many others

KINDS OF CASES A DIGITAL FORENSIC EXPERT WORKS ON

- Child Pornography
- Civil Litigation (between organizations or individuals)
- False emails (email headers …) – people who can no longer testify
- Employee Termination Cases
- Media Leak Investigations (esp. sensitive info and stock market…)
- Industrial Espionage Investigations (Coca-Cola …)
- Doctored images
- Social networking – to track whereabouts of people (incl. GPS pics …)

SOME REAL-LIFE CASE STUDIES



PACE MAKER

- Ross Compton, 60, who allegedly set fire to his house in 2016, is charged with aggravated arson and insurance fraud for the incident at his Court Donegal house. The blaze caused nearly $400,000 in damages. Compton, who was indicted in January 2017, was arrested based in part on data taken from his pacemaker.
- The case is believed to be the first of its kind to use data from a beating heart as evidence. Last year, Pater ruled that evidence from Compton's pacemaker could be presented at trial.
- Middletown detectives said Compton gave statements that were "inconsistent" with evidence collected at the scene and from his medical device.
- Compton, who has an artificial heart implant that uses an external pump, told police he was asleep when the fire started. When he awoke and saw the fire, he told police he packed some belongings in a suitcase and bags, broke the glass of his bedroom window with a cane and threw the bags and suitcase out the window before climbing out the window himself and taking the bags to his car.
- The data taken from Compton's pacemaker included his heart rate, pacer demand and cardiac rhythms before, during and after the fire.
- A cardiologist who reviewed that data determined "it is highly improbable Mr. Compton would have been able to collect, pack and remove the number of items from the house, exit his bedroom window and carry numerous large and heavy items to the front of his residence during the short period of time he has indicated due to his medical conditions.

https://www.journal-news.com/news/crime--law/using-pacemaker-data-stealing-personal-information-judge-middletown-arson-case-says/BAGH5WM0iCxOTwTPfM3P7J/

MURDERING MINISTER

- Matt Baker was a preacher with an active congregation in Waco, Texas, and a beautiful family, including two young daughters.
- But his seemingly picturesque life changed forever on April 7, 2006, when he found his wife, Kari, dead in their bed, apparently from an overdose of sleeping pills.
- But why would a perfectly healthy mother leave a typed, unsigned suicide note professing love for her children, her parents and her husband, apologize and then take her own life?
- In a 2008 interview, Matt Baker told ABC News that there were clues his wife was in a downward spiral. It began, he said, with one monumental tragedy -- the loss of their second daughter, Kassidy, who died over a decade ago. When she was a one year old, she was struck by a brain tumor and died four months after her diagnosis, leaving Kari grief-stricken. "The Hewitt Police Department was quick to rule Kari's death a suicide. However, her family still could not comprehend how the doting mom could leave her other two children behind. Lindsey Pick, Kari's cousin, was sure that Kari did not take her own life. "She would have never, ever left her children," she said.
- The Dulins were suspicious of their son-in-law. Further investigation indicated that Baker searched the Internet for information on “overdose by sleeping pills” and for pharmaceutical websites where Ambien and other drugs could be purchased without a prescription.
- Based on numerous facts: the improbability of Baker’s timeline the night of Kari’s death, his statements during the 911 call, searches of his office and home computers (digital forensics), an affair with Vanessa Bulls, the toxicology from the autopsy, and the JP’s change in the cause of death from suicide to undetermined – and ultimately to convicted.

https://abcnews.go.com/2020/texas-pastor-matt-baker-convicted-wife-2006-murder/story?id=11092046

APPLE & THE AUTOMATIC DRIVING CAR SECRETS

- Mr. Weibo Wang joined Apple in March 2016 as a member of the team that developed technology for autonomous systems
- In 2018, Mr. Wang took parental leave and visited China, and never returned to Apple. He instead joined a Chinese-based startup developing autonomous technology for cars.
- His abrupt departure gave rise to suspicion, prompting an investigation by Apple's New Product Security Team. The team used digital forensics tools to examine the engineer's network activity, and extract data from his Apple devices, including those he had left behind in his Mountain View, California home
- The investigation revealed that the engineer had downloaded a number of files from Apple's servers before he left. This included engineering schematics of a circuit board for an autonomous vehicle, and information about prototype and testing hardware. Most of this information was related to Apple's Project Titan self-driving car technology.
- The former Apple engineer pled guilty in August 2022

https://www.bbc.com/news/world-us-canada-65616384

CATCHING FAKES: DOCTORED PHOTOS

- Fraudulent photographs produced with powerful, commercial software appear constantly, spurring a new field of digital image forensics.
- Algorithms are used (theory of Computer Science in practice)
- Many fakes can be exposed because (non-trivial) algorithms can spot. E.g.

    1. inconsistent lighting, including the specks of light reflected from people's eyeballs (specular highlights)
    2. when an image has a "cloned" area or does not have the mathematical properties of a raw digital photograph
    3. angle of eyes
    4. repeating patterns
    5. inconsistent graphics
    6. direction of light source

    The source for the material is this section is taken from the research carried out by Dr. Hany Farid of Dartmouth University
    https://home.dartmouth.edu/news/2013/08/software-exposes-faked-photos-new-york-times

WHO WORKS ON DIGITAL FORENSICS CASES?

- Governmental (NSA, CIA, FBI)
- State/ Local
- International (Interpol, MI5)

- Examples of private security companies
  - https://idsinc.com/
  - https://www.opentext.com/
  - https://www.xactdatadiscovery.com/
  - https://www.fireeye.com/
  - https://www.pdf-i.com/
  - https://www.xactdatadiscovery.com/
  - https://exterro.com/
  - https://atola.com/
  - https://www.intaforensics.com/
  - https://www.logicube.com/

- Money contingent on experience and success rate

SOME CERTIFICATIONS FOR COMPUTER/ DIGITAL FORENSIC EXPERTS

- Certified Forensics Analyst (CFA)
- Certified Computer Forensics Examiner (CCFE) certification.
- Encase Certified Examiner (EnCE) certification
- Certified Information Systems Auditor (CISA)
- The International Society of Forensic Computer Examiners' Certified Computer Examiner (CCE)
- And security-related certifications (see introduction presentation)
- Global Information Assurance Certification (GIAC)

Dr. Nazli Hardy, MBA, Ph.D.

SOME JOURNALS AND REFERENCES OF INTEREST

- Digital Investigation (Open Access from ScienceDirect)
- Forensic Science Communications (FBI)
- Forensic Science International -- Genetics (ScienceDirect)
- Forensic Science, Medicine, and Pathology
- International Journal of Digital Crime and Forensics
- International Journal of Forensic Computer Science
- International Journal of Legal Medicine
- Journal of Digital Forensics, Security and Law
- Journal of Forensic and Legal Medicine
- Journal of Forensic Sciences
- Legal Medicine
- The Open Forensic Science Journal (Open Access on the web)
- Science and Justice (ScienceDirect)
- Small Scale Digital Device Forensic Journal (Open Access on the web)

CONFERENCES RELATED TO DIGITAL FORENSICS

- American Academy of Forensic Science
- Conference on Digital Forensics, Security and Law
- Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
- EuSecWest
- EuroForensics-Forensics Sciences Conference and Exhibition
- Computer Security Foundations Symposium
- International Conference on Security and Privacy in Communication Networks
- USENIX Security Symposium
- DEF CON Hacking Conference