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
  ➢ Email Headers
  ➢ Fake Photos

Computer Forensic Resources for you
  ➢ Job prospects
  ➢ Certifications
  ➢ Journals
  ➢ Conferences
  ➢ Tools
Why is the Study of Digital Forensics Relevant?

- Reality: Everything and anything we do can and is tracked …
  - Social Networking (FB, Twitter, Pinterest…)
  - Information Retrieval (Google, Bing, Yahoo ….)
  - The Internet itself on PDAs (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)
- … and so much more …
What is Digital Forensics?
What is Computer/ 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 do you Need for a Careers in Computer Digital Forensics?

For a computer/ digital forensics career, it is helpful to have:

- a degree related to computer science (CS) or information technology (IT) or computer engineering (minor in criminal justice). Or even 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

- Framed by a virus?
- The Nigerian connection
- Saved by Facebook
- BTK killer: the depraved, egotist, and stupid
- Cracking Stuxnet, a 21st-century cyber weapon (TED video)
Employee Termination Cases

- Email/IM/Text Abuse Investigations
  - most often include emails that are inappropriate, threats, harassments

- As the forensics expert, you need the following:
  - electronic copies of emails (header data)
  - phone records for texts
  - email server logs (deleting does not erase)
  - .pst files (Outlook)
  - Word documents/temp files (why?)
  - Download folders
  - Picture folder for attached/posted pictures
  - Cache memory, if possible for copied items
**Industrial Espionage**

- Involves either previously “trusted” employees or disgruntled employees or seemingly ignorant employees.
  - 60% of employees who leave or are fired from their jobs, steal data
  - Coca-Cola example

- These are most often treated as criminal investigations

- As the forensics expert, you need to do the following:
  - examine all email/download records of suspects
  - server logs
  - print jobs
  - related Internet newsgroups/message boards for postings/inquiries
  - surveillance cameras
  - phone records (texts, PDA)
  - online searches
  - download folder

Adapted from Computer Forensics and Investigations, Nelson, Phillips, Enfinger, Stewart
Catching a Fake: the 2 most basic tools in CS forensics

Put on your Digital Forensics Expert hats and let’s solve some digital forensic cases

What is a header?
To find email headers go to this link:
http://mail.google.com/support/bin/answer.py?hl=en&answer=22454

What is an IP address?
xxxx.xxxx.xxxx.xxxx
e.g. IP address for Millersville University is: 166.66.64.xxxx
To find your IP address or any IP address go to this link:
http://ip-lookup.net/
http://www.hostip.info/
http://whatismyipaddress.com/
http://www.networksolutions.com/whois/index.jsp (given IP address, finds host)
**Catching Fakes: Investigating the Email Header**

**Simple Scenario A: Sick Day Blues**

Details of Penny’s business meeting in California:

- **Sunday:** leave Millersville for California for the meeting
- **Monday:** meetings all day
- **Tuesday evening:** leave California and fly back to Millersville

**Questions to ask:** Was Penny really sick?

If she was sick – where would be physically?

______________________________

According to the header, where is she located?

Anything else to know about her?
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
    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
2008 Qinghai-Tibet Rail Line + Endangered Tibetan Antelopes Living in Harmony?
The Fake Exposed (Environmental)

- Too-finely focused
- Bad splicing
- Moving right along
- Telltale rock
- Pregnant antelopes?
2008 Iranian Missile (War)

“original”

“edited”

Adapted for UNIV 103 from my talk at the Women in the Math & Science Conference, March 2014
LA Times March 31, 2003

Adapted from Computer Forensics and Investigations, Nelson, Phillips, Enfinger, Stewart

Adapted for UNIV 103 from my talk at the Women in the Math & Science Conference, March 2014
2003 LA Times (War)
1989 O No! (Societal)

Money-Saving Store Coupons Inside!

Oprah! The Richest Woman on TV?

How she amassed her $250-million fortune

adapted from Computer Forensics and Investigations, Nelson, Phillips, Enfinger, Stewart

Hany Farid - Scientific American, Digital Forensics: How Experts Uncover Doctored Images
4 Ways to Spot a Fake – 1. Eye Position

- Because eyes have very consistent shapes, they can be useful for assessing whether a photograph has been altered.

- A person’s irises are circular in reality but will appear increasingly elliptical as the eyes turn to the side or up or down.

- An algorithm can approximate how eyes will look in a photograph by tracing rays of light running from them to a point called the camera center.

Hany Farid - Scientific American, Digital Forensics: How Experts Uncover Doctored Images
4 Ways to Spot a Fake – 2. Direction of Light Source

- Were the ducks or the MPs added?
Q. Were these 4 hanging out together for the photograph?

Surrounding lights reflect in eyes to form small white dots called specular highlights.

The shape, color and location of these highlights give us info about the lighting.
Doctored?

- The highlight position indicates where the light source is located.

- As the direction to the light source (yellow arrow) moves from left to right, so do the specular highlights.

- Many cases, however, require a mathematical analysis. To determine light position precisely requires taking into account the shape of the eye and the relative orientation between the eye, camera and light.

---

A: 

Hany Farid - Scientific American, Digital Forensics: How Experts Uncover Doctored Images

Adapted for UNIV 103 from my talk at the Women in the Math & Science Conference, March 2014
Political Ad from a 2004 US election campaign

Algorithm scans image and for, say a 6x6 block image, characterizes the make-up of color (pixels)

When the algorithm is applied to the image below from the political ad, it detects three identical regions (red, blue and green).
Circa 1860: Lincoln-Calhoun
Circa 1930: Stalin
Circa 1937: Hitler unhearts Goebbels
Circa 1997: Luxor, Egypt
Who Works on Digital Forensics Cases?

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

Examples of private security companies

- [www.arcsight.com](http://www.arcsight.com)
- [www.clearswift.com](http://www.clearswift.com)
- [www.datasec.co.uk](http://www.datasec.co.uk)
- [www.integrais.com](http://www.integrais.com)
- [www.forensics-intl.com](http://www.forensics-intl.com)
- [www.pentasafe.com](http://www.pentasafe.com)
- [www.savvydata.com](http://www.savvydata.com)
- [www.vestigeltd.com](http://www.vestigeltd.com)
- [www.vogon-international.com](http://www.vogon-international.com)
- [www.vordel.com](http://www.vordel.com)

- Money contingent on experience and success rate
Some Certifications for Computer/ Digital Forensic Experts

- Global Information Assurance Certification (GIAC)
- Certified Forensics Analyst (CFA)
- Certified Computer Forensics Examiner (CCFE) certification. The test candidate must pass a multiple choice exam with a score of 70% or higher.
- IACIS (the International Association of Computer Investigative Specialists), has offered a computer forensics certification since 1994: the Certified Forensic Computer Examiner (CFCE)
- Encase Certified Examiner (EnCE) certification
- Certified Information Systems Auditor (CISA)
- The International Society of Forensic Computer Examiners’ Certified Computer Examiner (CCE)
Some Journals and References of Interest

- Digital Forensics Magazine
- Cryptologia
- International Journal of Digital Evidence
- International Journal of Forensic Computer Science
- International Journal of Digital Crime and Forensics
- Journal of Digital Forensics, Security and Law
- Journal of Digital Investigation
- Journal of Digital Forensic Practice
- Small Scale Digital Device Forensic Journal
- The Journal of Applied Digital Forensics and eDiscovery
**Digital Forensic Software**

- Below are examples of some widely used digital forensic software companies

- **EnCase from Guidance Software** (~ $2,500 per user)

- **FTK from AccessData** (~ $600 per user)

- **Digital Intelligence**

- **Paraben**

- **Passware**

- **Further list of tools**

- **List of free forensic tools**
Conferences related to Digital Forensics (and Privacy/Security)

- American Academy of Forensic Science
- Conference on Digital Forensics, Security and Law
- Department of Defense CyberCrime Conference
- 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
- International Workshop on Security in Cloud Computing
- DEF CON Hacking Conference