Introduction to Digital Forensics

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: Almost everything and anything we do online, can be and, probably 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?

Evolution of the crime weapon:

old fashioned way

new way
What is Computer/Digital Forensics?

- a branch of forensic science that pertains to \textbf{evidence} (criminal or civil) found in \textbf{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)
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://www.hostip.info/
http://whatismyipaddress.com/
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 she 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)
2008 Iranian Missile (War)

“original”

“edited”

Forensic Expert: Hany Farid

http://www.scientificamerican.com/article.cfm?id=is-that-iranian-missile
LA Times March 31, 2003

Adapted for UNIV 103

Adapted from Computer Forensics and Investigations, Nelson,
2003 LA Times (War)

Adapted from Computer Forensics and Investigations, Nelson, Phillips, Enfinger, Stewart
Introduction to Digital Forensics

1989 O No! (Societal)
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.

---

4 Ways to Spot a Fake – 3. Specular Highlights

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

Adapted for UNIV 103
**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.

---

Hany Farid - Scientific American, Digital Forensics: How Experts Uncover Doctored Images
4 Ways to Spot a Fake – 4. Finding Cloned Regions

- 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.integralis.com](http://www.integralis.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.
- 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)
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
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