Digital Forensics

Slides by Prof. Kevin Fu with material from Dr. Simson Garfinkel (NIST) and Prof. Rachel Greenstadt (Drexel)

Today: Digital Forensics

- An Enigma: Harold Thimbleby
- Image forensics
- Data sanitization
- Code stylometry
- Osama bin Laden

EECS588 W18 Graduate Security
Tues/Thu 1:30-3:30PM
4 credits

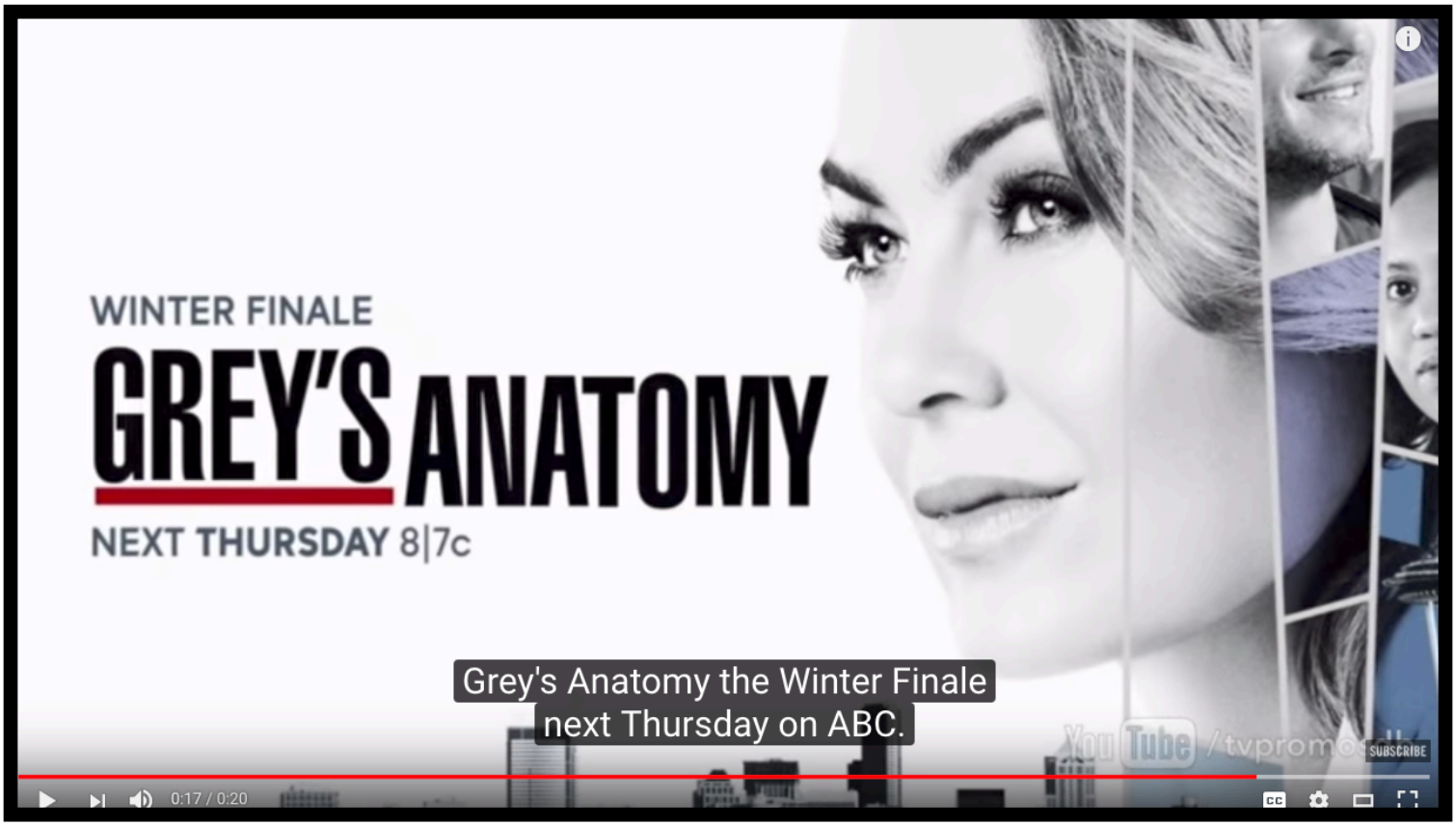
Prereq: 482 (OS) or grad standing, computer engineering experience helpful. Target: CE, CS, ECE
(**incorrect lab time listing**, not weekly)

- Graduate-level security research
- Emphasis on embedded security
- Hands-on cryptanalysis with oscilloscopes and electronics
- Physics of computer security and privacy: acoustics, RF, light, etc.

Grey’s Anatomy tonight at 8PM

Hospital Cyberattack…

https://www.youtube.com/watch?v=bMXxFUP372g



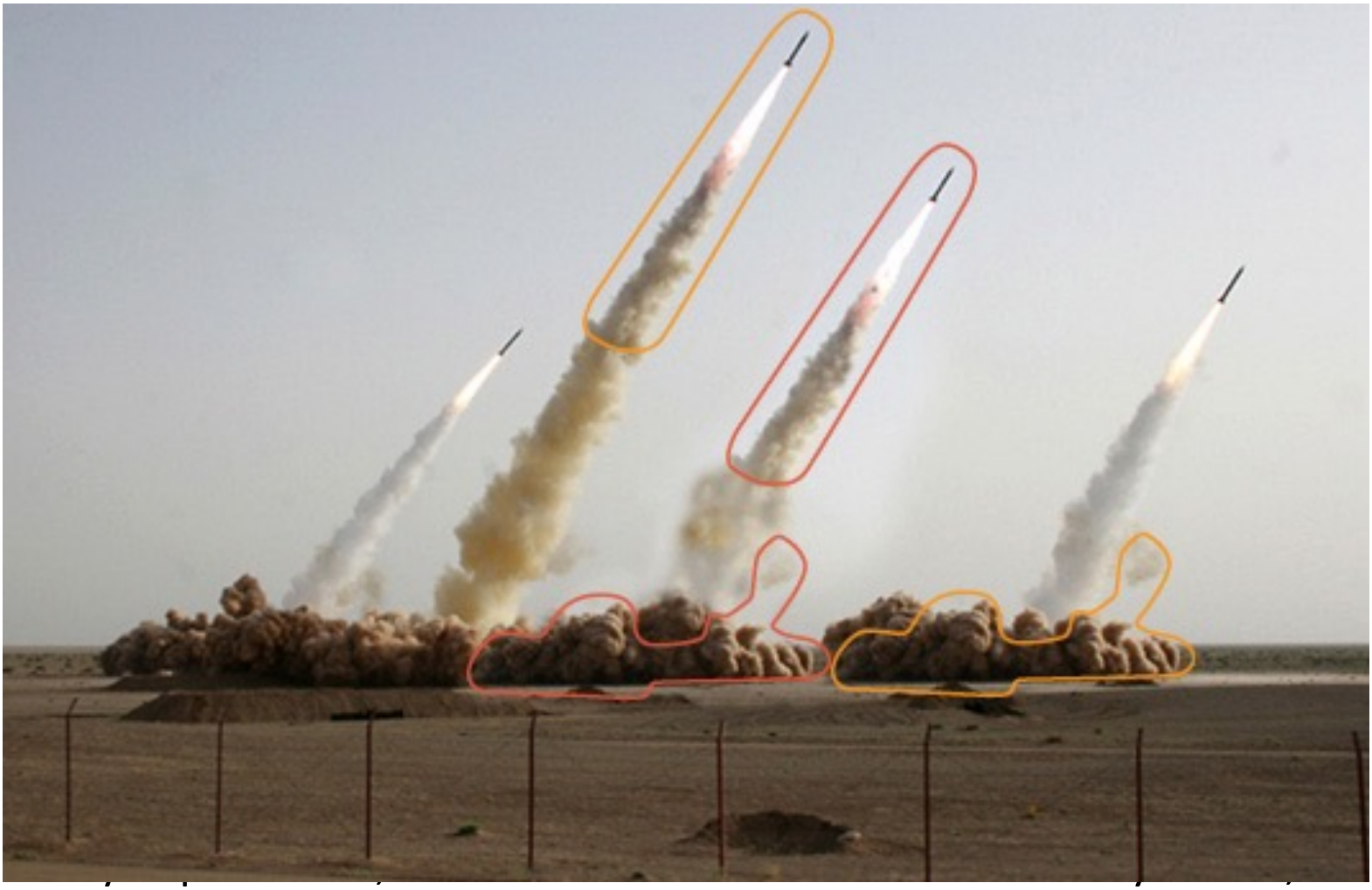
Don’t Believe Everything You ~~Read~~See

Fake?

Real?

(near-by vantage point)

What's wrong with this picture?



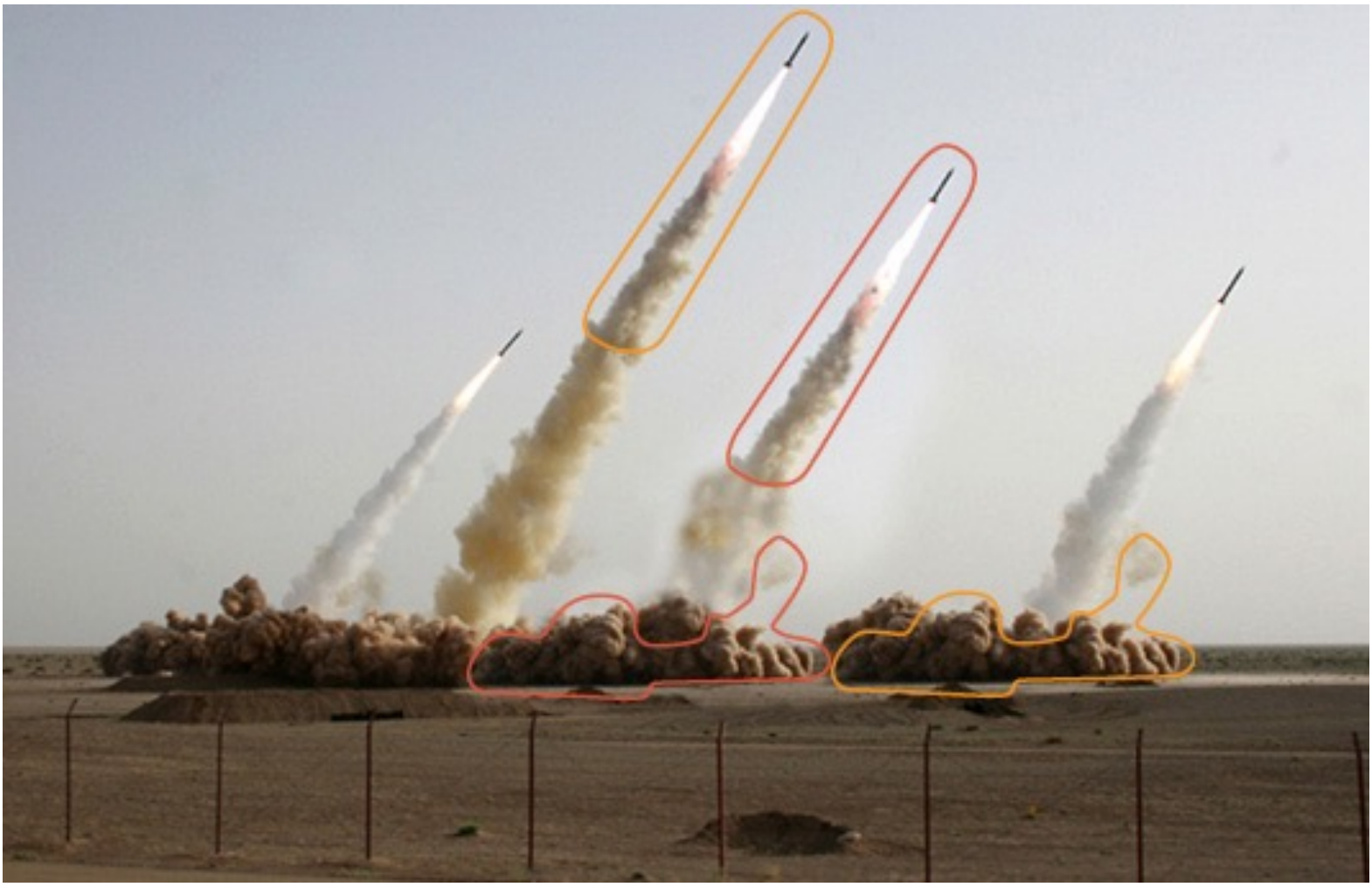
two major sections (encircled in red) appear to closely replicate other sections (encircled in orange). (Illustration by The New York Times; photo via Agence France-Presse)

Latest update at 3 p.m. Eastern Agence France-Presse has retracted the image as "apparently digitally altered." More developments at the bottom of the post.

In an Iranian Image, a Missile Too Many

By MIKE NIZZA AND PATRICK J. LYONS JULY 10, 2008 9:16 AM

the second missile from the right appears to be the sum of two other missiles in the image.



In an Iranian Image, a Missile Too Many

By MIKE NIZZA AND PATRICK J. LYONS JULY 10, 2008 9:16 AM

The Making of an Icon

In the front-page version of Mr. Xi's portrait, the color and saturation were adjusted, hiding gray hairs and skin imperfections and giving the photo the feel of a painting, said Hany Farid, a professor at Dartmouth College and an expert on photo forensics.

Mao Zedong, c. 1950

Xi Jinping, 2017

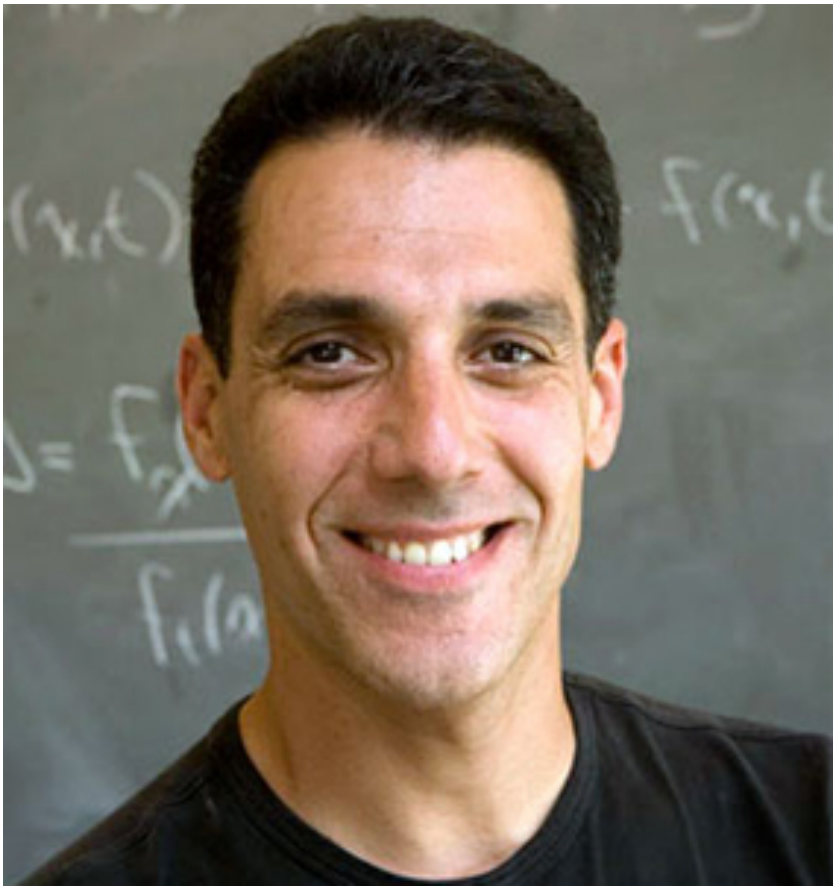
Why Xi Jinping's (Airbrushed) Face Is Plastered All Over China

By JAVIER C. HERNÁNDEZ and AUDREY CARLSEN NOV. 9, 2017

Want to know more?

Read up on Prof. Hany Farid of Dartmouth College

http://www.dartmouth.edu/~tedx/hanyfarid/



Code Stylometry

“Style expressed in source code can be quantified and characterized.”

[De-anonymizing Programmers via Code Stylometry.

Aylin Caliskan-Islam, Richard Harang, Andrew Liu, Arvind Narayanan, Clare Voss, Fabian Yamaguchi, and Rachel Greenstadt.
Usenix Security Symposium, 2015]

(Prof. Rachel Greenstadt @ Drexel)

Stylistic fingerprints

- Stylometry has been applied to:
  - Fine-art
  - Music
  - Unconventional text
  - Translated text
  - Source code

Source code stylometry

- Everyone learns coding on an individual basis, as a result code in a unique style, which makes de-anonymization possible.

- Software engineering insights
  - programmer style changes while implementing sophisticated functionality
  - differences in coding styles of programmers with different skill sets

- Identify malicious programmers.

Source code stylometry: Who wrote this code?

- **Scenario 1:**

Alice analyzes a library with malicious source code.

Bob has a source code collection with known authors.

Bob will search his collection to find Alice's adversary.

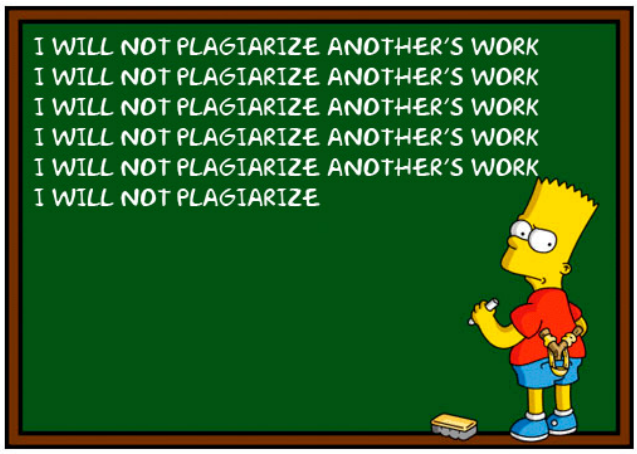
Source code stylometry: Who wrote this code?

- **Scenario 2:**

Alice got an extension for her programming assignment.

Bob, the teacher has everyone else's code.

Bob wants to see if Alice plagiarized.



Source code stylometry

Iran confirms death sentence for 'porn site' web programmer

No technical difference between security-enhancing and privacy-infringing…

Available tools

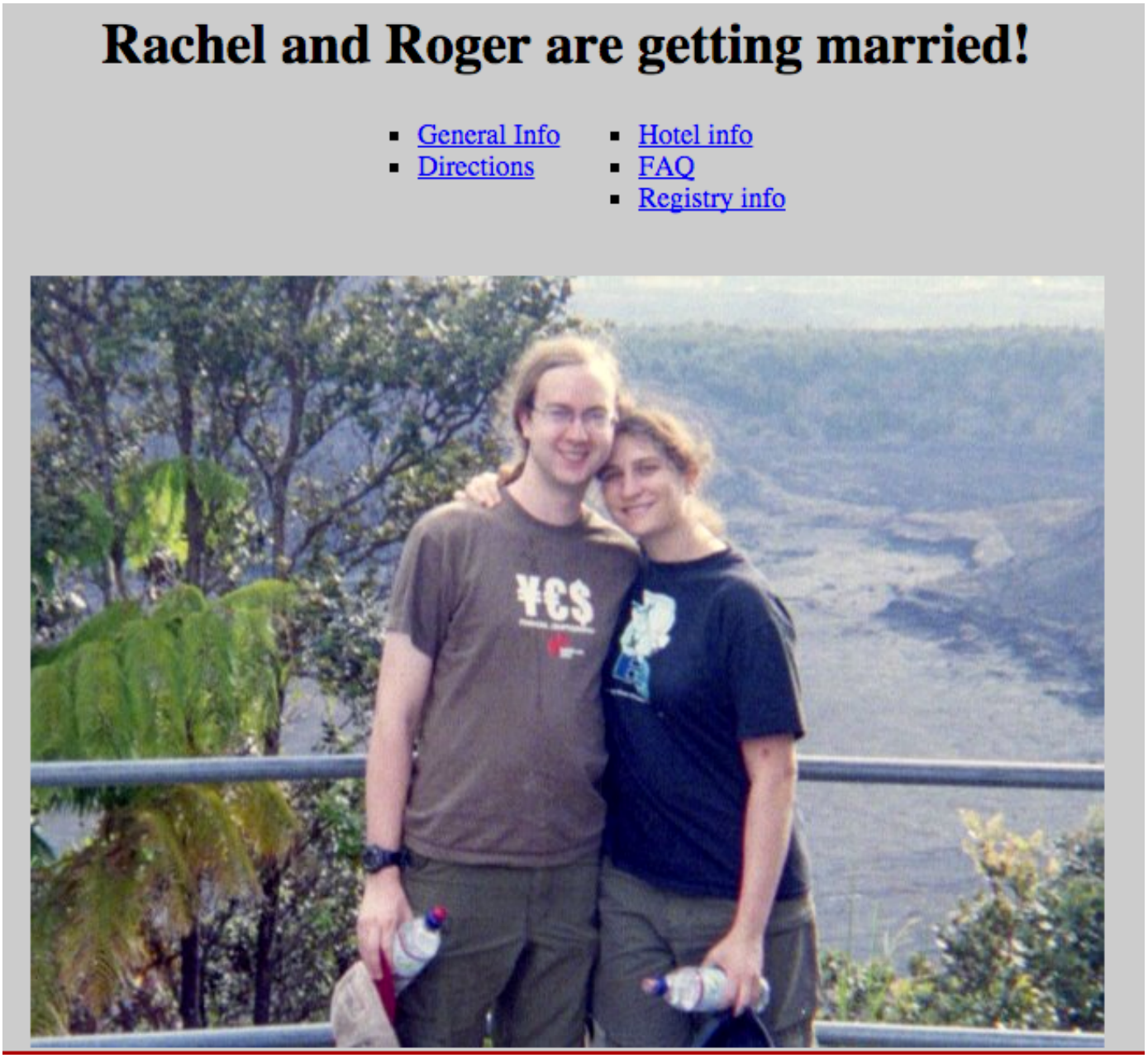
- Source code authorship attribution
  - https://github.com/calaylin/CodeStylometry

- Jstylo
  - prose authorship attribution framework

- Anonymouth
  - writing anonymization

Code Stylometry

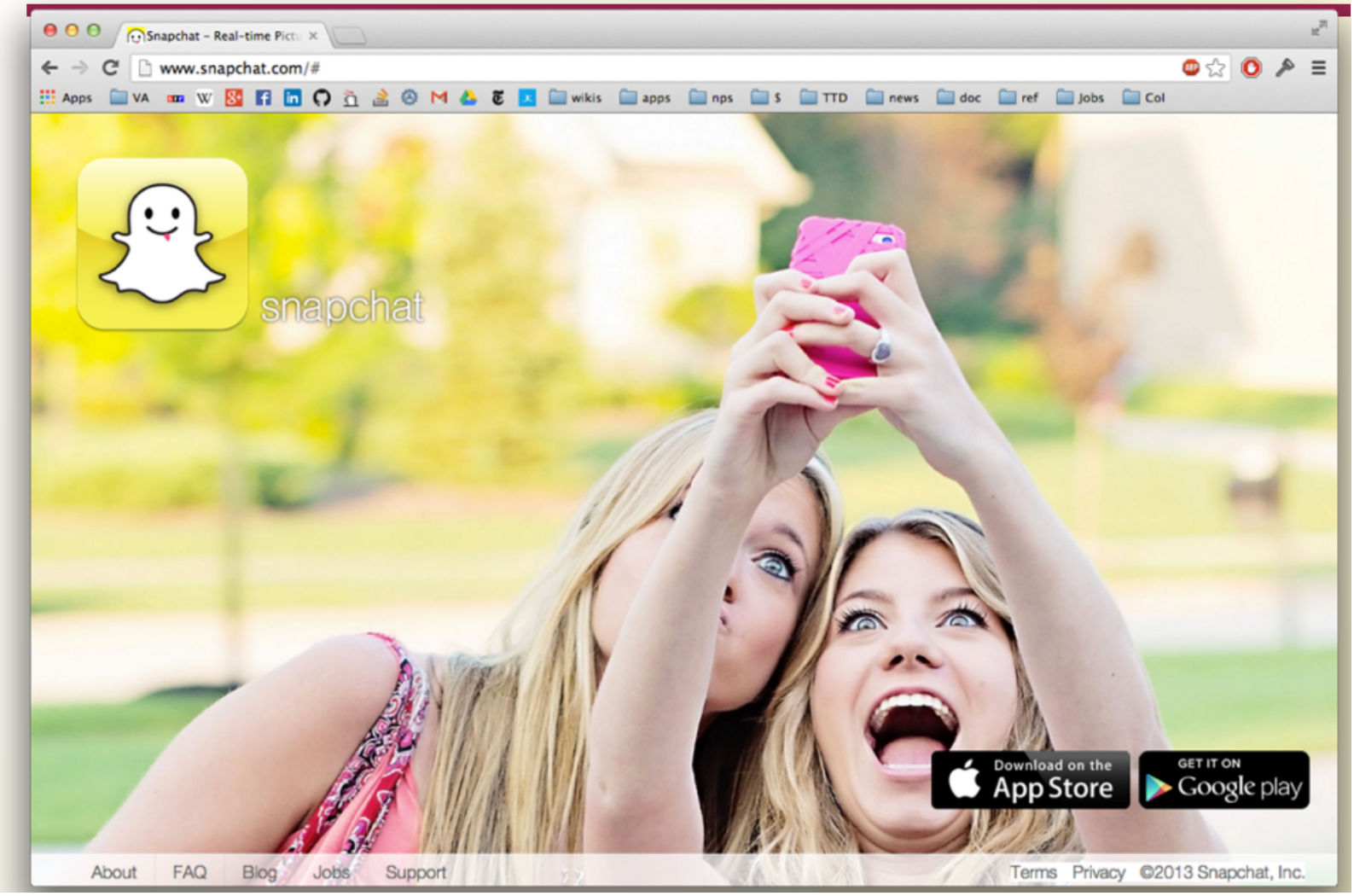
Closely “related” to anonymity.



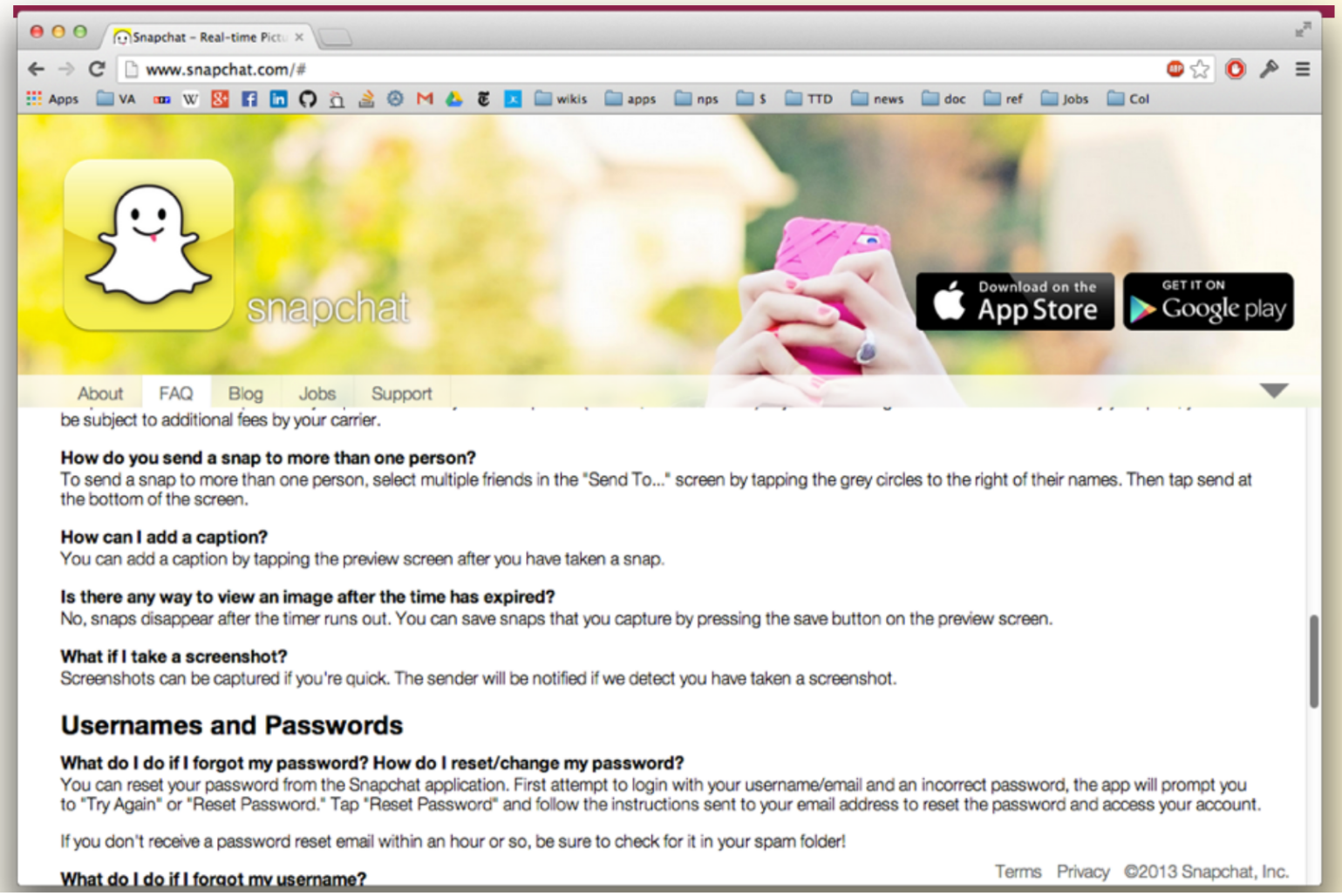
Digital Forensics

Material from Dr. Simson Garfinkel

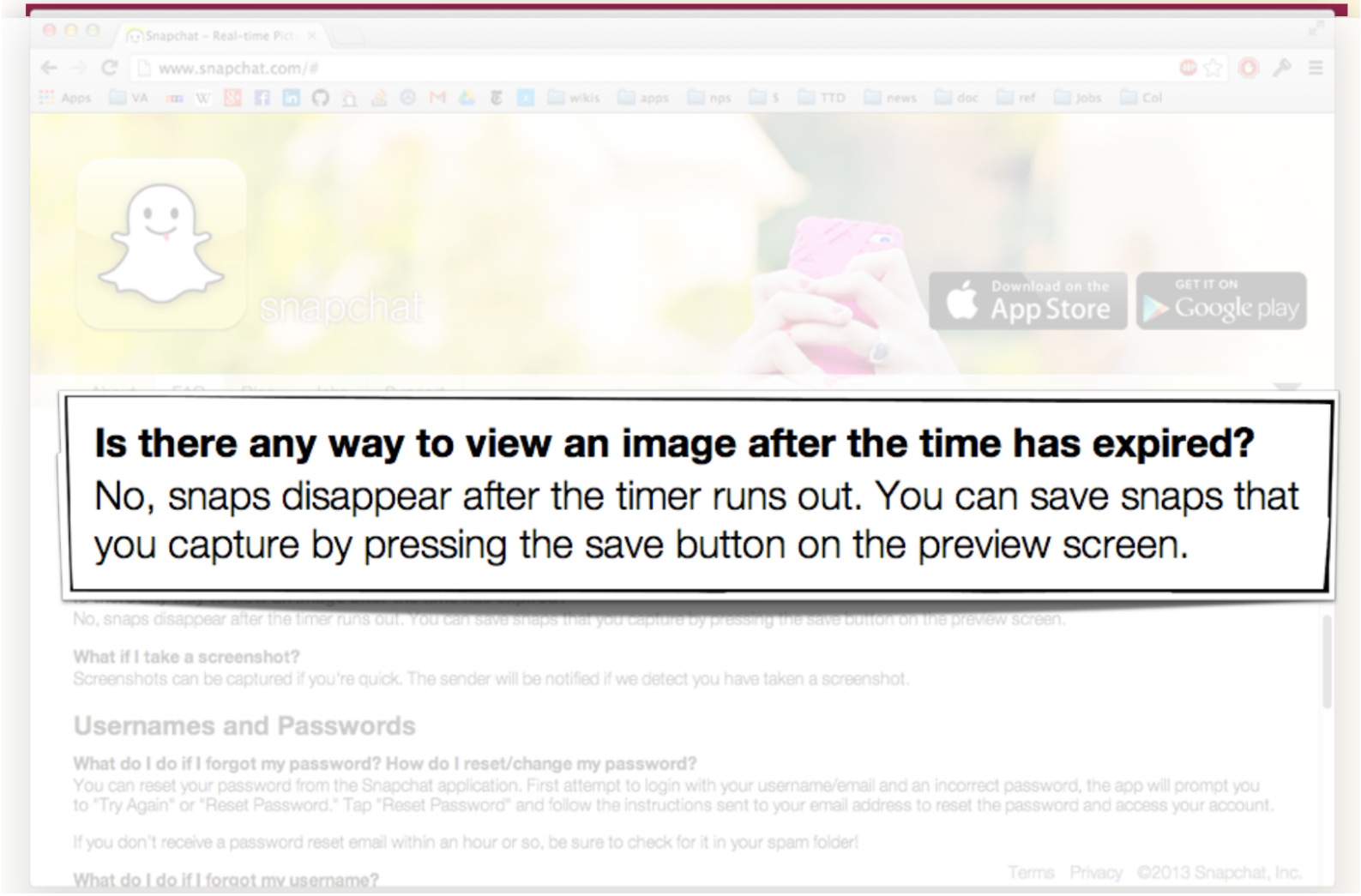
Snapchat is a popular app!



Snapchat promised users that expired images could not be viewed unless “saved.”



Snapchat promised users that expired images could not be viewed unless “saved.”



OMG! — Expired images not actually deleted. They were just hidden from view.

slate | Follow @slate 588K followers | LO

NEWS & POLITICS | TECH | BUSINESS | ARTS | LIFE | HEALTH & SCIENCE | SPORTS | DOUBLE X | PODCASTS

OMG, "Deleted" Snapchat Sexts Can Actually Be Recovered

By Will Oremus | Posted Thursday, May 9, 2013, at 3:56 PM

Share 59 | Like 133 | Tweet 84 | EMAIL | PRINT | COMMENT 46

Snapchat's users shouldn't be shocked to find that their images can be recovered even after they "self-destruct"—but they will be anyway.
Sylvie Bouchard/Shutterstock.com

The premise of Snapchat is simple: Send a photo or short video to a friend, and it will self-destruct after 10 seconds. That way, it won't wind up on the Internet and ruin anyone's reputation, friendships, or career.

Needless to say, that has made it a wildly popular choice for sexting. But Snapchat's appeal goes far beyond that. In an age in which "privacy" and "technology" have become almost antonymous, it has been billed as the anti-Facebook—a communications tool that deletes your data rather than preserving, analyzing, and trading on it. In short, it's supposed to make messaging fun again.

But the app's security has never been ironclad. As the media have repeatedly warned parents, and parents in turn warned their kids, message recipients can still save a compromising image by taking a quick screenshot. But Snapchat tries to mitigate the risk somewhat by automatically notifying the sender when that happens. If someone screenshots you, it's a virtual slap in the face. If they don't, you can assume you're in the clear.

Except that apparently you can't. KSL-TV in Utah reports that an Orem-based firm called Decipher Forensics has figured out a way to recover supposedly deleted images from the recipient's phone. The process isn't simple: 24-year-old Decipher forensics examiner Richard Hickman told the network that it takes him about six hours, on average, to image the phone's data. So far he can only do it with Android devices, though he's working on doing the same for iOS. But his firm is now offering to perform the recovery procedure for anyone who wants it, from parents

rm -rf

- rm is not forever
- delete vs. mark
- Solid state drives, flash memory

Digital Forensics “research” traditionally focused on training, collection & extraction

Preparation: policy, training & tools

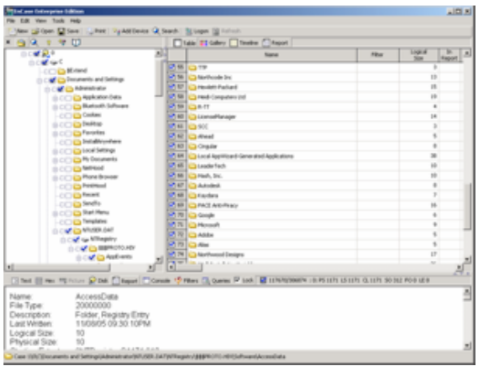
Collect & preserve evidence

Extract preserved data

Training the force

CyberCorps®
Defending America's Cyberspace

Collection Techniques



Reverse engineering

Extracting digital evidence was simple five years ago

"Imaging tools" extracted data without modification.

"Write Blocker" prevents accidental overwriting.

Original device stored in evidence locker.

Forensic copy ("disk image") stored on a storage array.

Today much of the work is with cell phones. Every one is different.

Operating system:

- Android? iPhone? Blackberry? Feature Phone?

Access to the data:

- PIN lock?
- Encrypted Storage?
- Stored locally or in the cloud?

Applications:

- Built-in? Downloaded from “App Store”?
- Custom-written?
- Self-destruct / remote wipe?
- Malware?

Human Language: English? Korean? Chinese?

Phone forensics

Hanssen

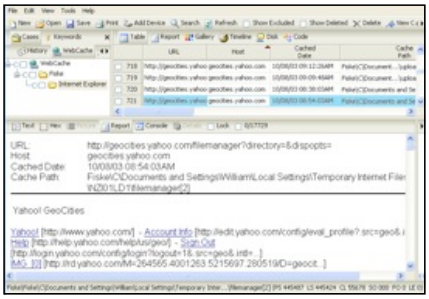
The “CSI Effect” creates unrealistic expectations.

TV digital forensics:

- Every investigator is trained on every tool.
- Correlation is easy and instantaneous.
- There are no false positives.
- Overwritten data can be recovered.
- Encrypted data can usually be cracked.
- It is impossible to delete anything.

The reality:

- Overwritten data *cannot* be recovered
- Encrypted data usually can't be decrypted
- Forensics rarely answers questions or establishes guilt
- Tools crash a lot



EnCase

Result:

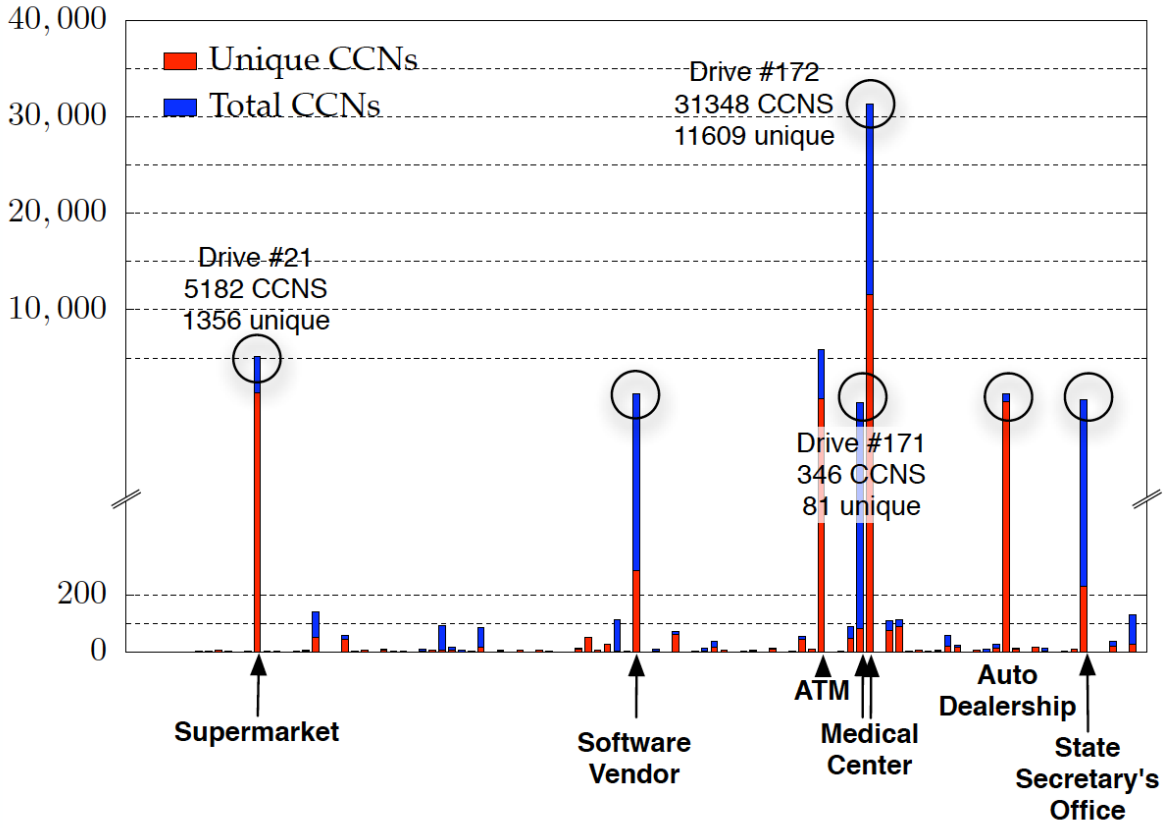
—DF is a difficult process that looks easy

Digital media triage: Deciding where to start

Imagine you encounter a large number of computers, USB drives, etc.

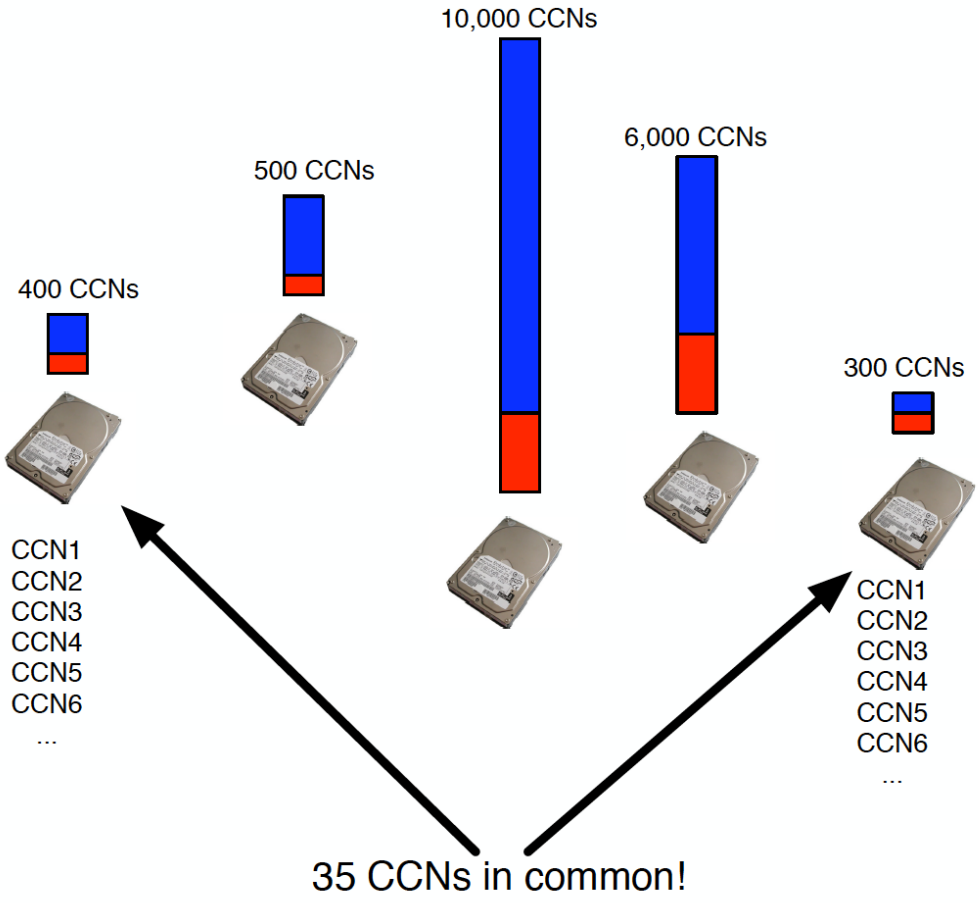
Where do you start?

Most drives had just a few, but some had a lot of credit card numbers.



"Design Principles for Software that is Simultaneously Secure and Usable," Garfinkel, MIT PhD Thesis, 2005

What would it mean if two drives had a lot of credit card numbers in common?



FARHAD MANJOO SCIENCE 11.08.01 12:00 PM

HIDDEN MESSAGES: ANY THERE THERE?

STANFORD, California — Niels Provos, a computer science graduate student at the University of Michigan, took the dais at a Stanford University lecture hall Wednesday evening with what seemed a comforting message: After analyzing a couple million graphics files posted on the Internet, he has found no evidence that any of the pictures contained hidden communications sent by anyone, let alone agents of Osama bin Laden.