

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)

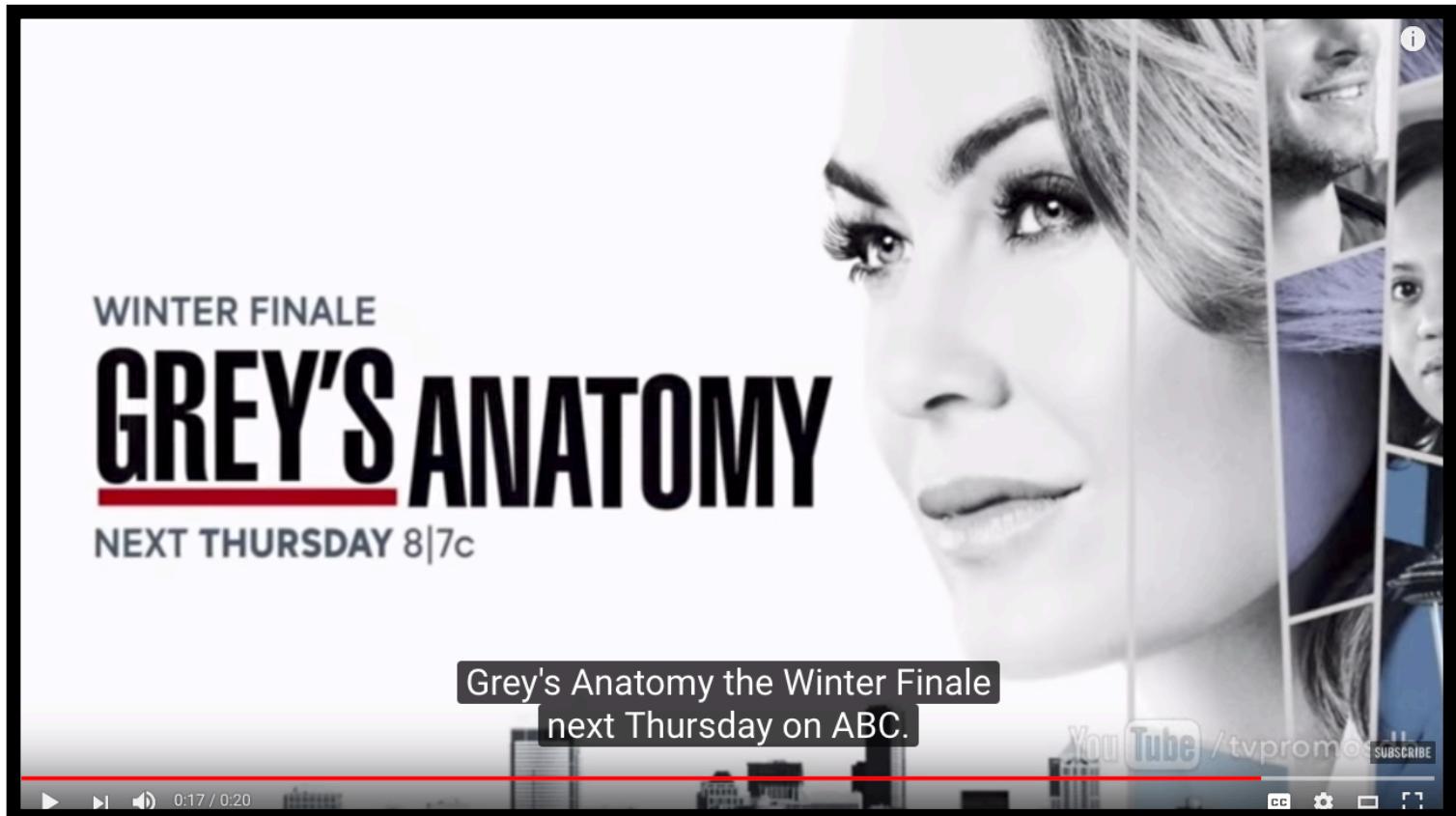
- Graduate-level security research
- Emphasis on embedded security
- Hands-on cryptanalysis with oscilloscopes and electronics
- Physics of computer security and privacy: acoustics, RF, light, etc.



Grey's Anatomy tonight at 8PM

Hospital Cyberattack...

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



Don't Believe Everything You ReadSee

The image is a collage of three newspaper front pages from different US cities. The top left is the 'Los Angeles Times' with a headline about Allstate cutting homeowner rates. The middle is 'The Palm Beach Post' with a story on Iran's missile tests. The right is the 'Chicago Tribune' with a headline about Boeing getting a tanker redo. Each page includes a mix of local and national news, along with political cartoons and other columns.

TOPICS | **TODAY'S PAGES** | **VIDEOS** | **BEST SELLERS** | **PAGE INDEX** | **GATEWAY**

The New York Times

Wednesday, July 8, 2009 | Last Update: 10:00 PM ET

NYT Archives (since 1881) | Search

Senate Backs Wiretap Bill to Shield Phone Companies

By DAVID E. SANGER AND JAMES M. BORNEMAN
The Senate gave final approval to broadening government spy powers and protecting immunity for the phone companies that took part in secret wiretapping.

U.S. Responds Riddling an Flawed Tanker Counter

By MICHAEL WITKIN
A multimillion-dollar fine from court for senior executive tankers will be imposed in the wake of a report that found flaws in the original process.

6 U.S. Air Attacks on U.S. Post in Turkey

By STEPHEN LEE
Counterterrorism forces in a Turkish military facility outside the United States bombed an American post in Turkey.

MAGAZINE REVIEW

FBI: Snapping Feds

By DAVID M. SHAW

Americans are spending millions on anti-alarming drugs for their cars and dogs. Is it because we're driven crazy?

Travel +
Spying on Bushwhack's Cool Underwear
Some clever art projects to lay foundations for thought. Underwear may be the city's issue.
Or Trees? (84 Miles From)

At Northeast Geysers
Take a quick trip to Nature's tiny fountains at West Virginia's hot-spring springs.

FREE
FREE

Photo: News and Opinion / Politics / National / Science / Business / Entertainment / Sports / Obituaries / Health

Iran Reports Missile Test, Downing Rebuttal

By ROBERT S. SOUTER, with ASSOCIATED PRESS

The White House said the tests, which coincide with tense negotiations over Tehran's nuclear program, would further isolate Iran, showing a photo released by Iran.

Oil May Reverse Surge of Late

By CLAUDIO HALLIGAN, with ASSOCIATED PRESS

The latest oil price rally has investors nervous.

Efficiency vs. G. H. Moniz's Green Climate Goal

By JONATHAN S. CROWLEY and DAVID E. SANGER

Power companies are bristling but not wholly adverse to the Energy Department's more aggressive steps to cut pollution.

Reassessing the Economy

Read or Listen: **How to Buy a Home** (10:00 AM ET)

Earthquakes and Climate Policy (The International Report)

World News

India's Rail Agency to Lay Handing Out Millions

By DAVID E. SANGER

Police officers are hunting last night's culprits after the Central Bank of India made aggressive steps to cut pollution.

India's Rail Agency to Lay Handing Out Millions

By DAVID E. SANGER

India's Rail Agency to Lay Handing Out Millions

On The Web

What Causes So Many Arrests for Young Offenders

City官员 have written stories in New York, Chicago, Boston, Seattle, Atlanta and Minneapolis. Paper City: A Reader's Guide to Whisker-Face Walls Should Encourage Big Overweight Patients?

Deathbed: Low Coverage from Work Valley

REAL ESTATE | **ARTICLES**

See Thatland: a Contemporary Villa

For John and Linda, their new walls describe what last took in a building.

Two million dollars will on a residence never

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

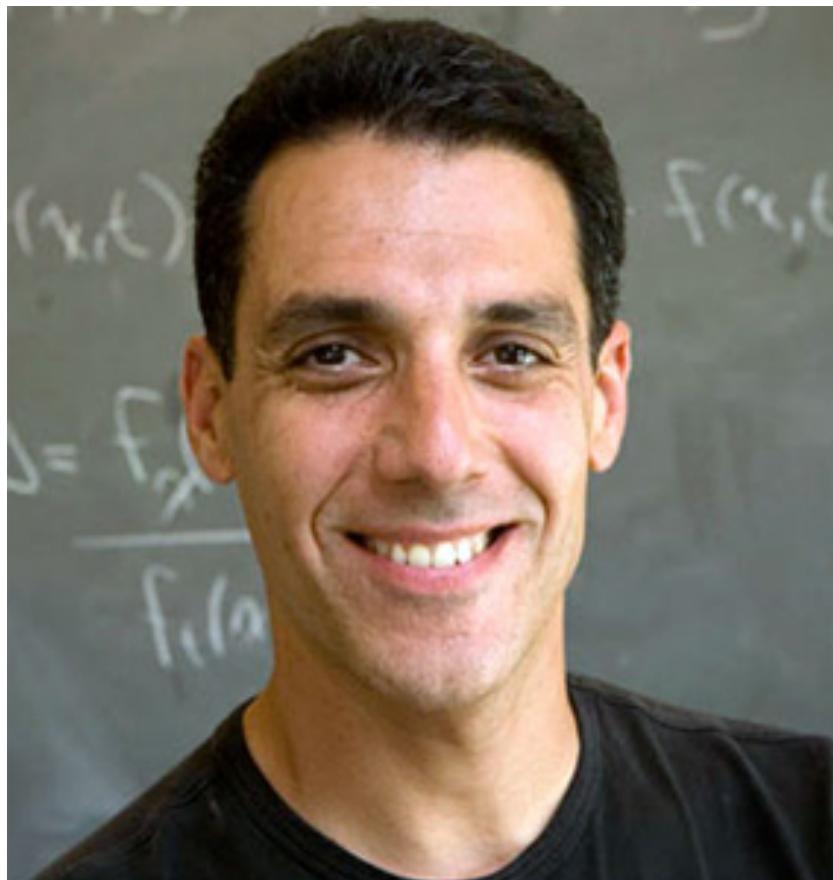


Why Xi Jinping's (Airbrushed) Face Is Plastered All Over China

Want to know more?

Read up on Prof. Hany Farid of Dartmouth College

[http://www.dartmouth.edu/~tedx/
hanyfarid/](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.



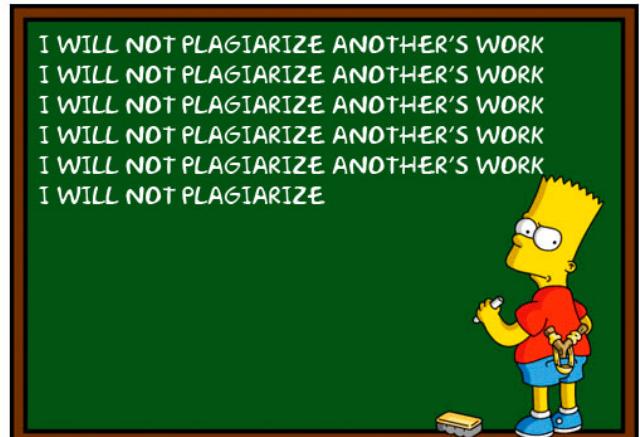
Source code stylometry: Who wrote this code?

- **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.

Rachel and Roger are getting married!

- [General Info](#)
- [Directions](#)
- [Hotel info](#)
- [FAQ](#)
- [Registry info](#)

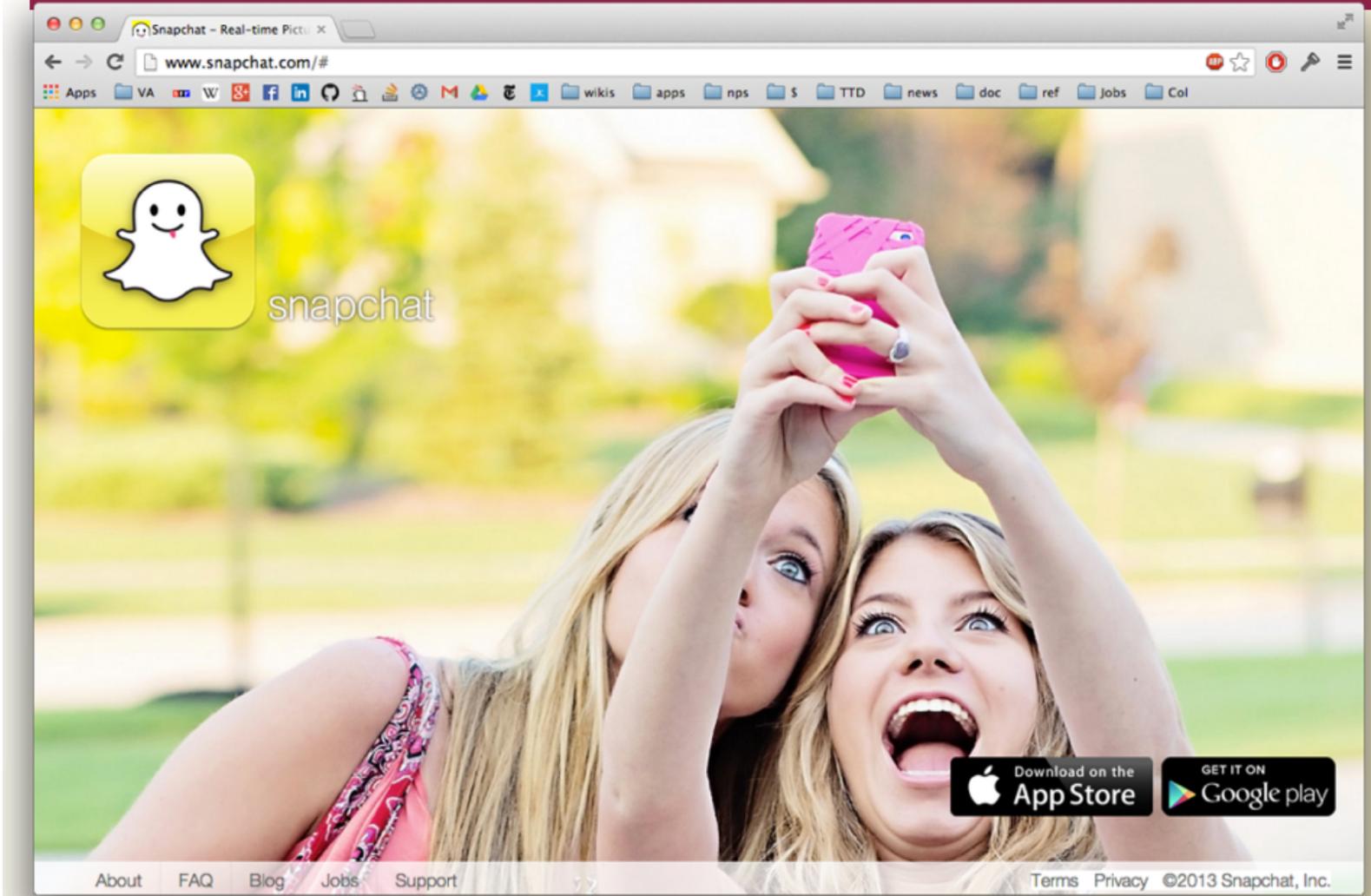


Digital Forensics

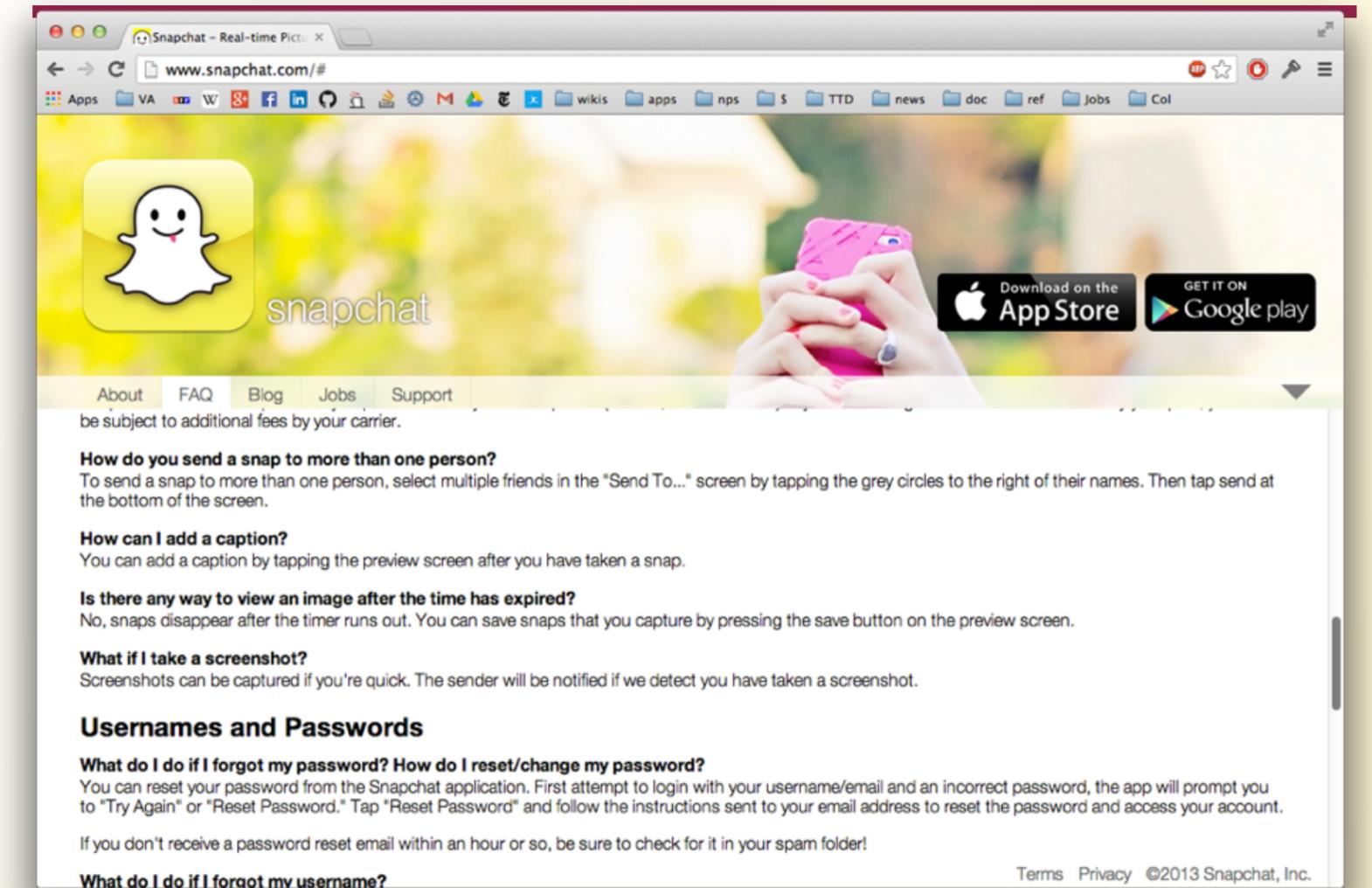
Material from Dr. Simson Garfinkel



Snapchat is a popular app!



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



The screenshot shows the official Snapchat website at www.snapchat.com/. The page features the iconic white ghost logo on a yellow background. Below the logo, the word "snapchat" is written in a lowercase sans-serif font. To the right, there's a photograph of a person's hands holding a pink smartphone. At the top right, there are download links for the App Store and Google Play. A navigation bar at the bottom includes links for About, FAQ, Blog, Jobs, and Support. The main content area contains several frequently asked questions:

- How do you send a snap to more than one person?**
To send a snap to more than one person, select multiple friends in the "Send To..." screen by tapping the grey circles to the right of their names. Then tap send at the bottom of the screen.
- How can I add a caption?**
You can add a caption by tapping the preview screen after you have taken a snap.
- Is there any way to view an image after the time has expired?**
No, snaps disappear after the timer runs out. You can save snaps that you capture by pressing the save button on the preview screen.
- What if I take a screenshot?**
Screenshots can be captured if you're quick. The sender will be notified if we detect you have taken a screenshot.

Usernames and Passwords

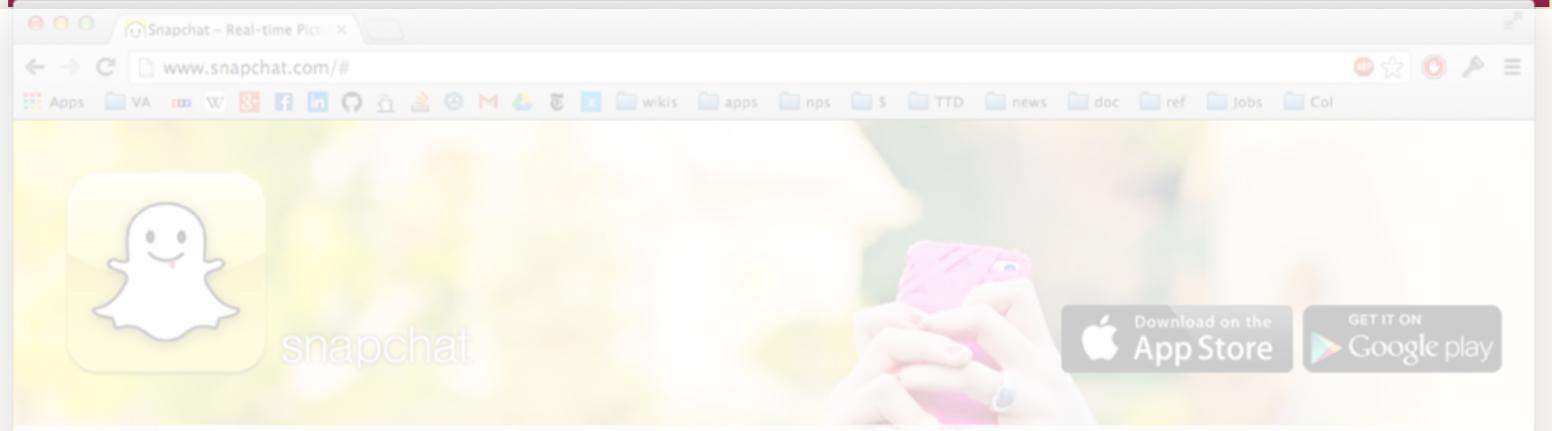
What do I do if I forgot my password? How do I reset/change my password?
You can reset your password from the Snapchat application. First attempt to login with your username/email and an incorrect password, the app will prompt you to "Try Again" or "Reset Password." Tap "Reset Password" and follow the instructions sent to your email address to reset the password and access your account.

If you don't receive a password reset email within an hour or so, be sure to check for it in your spam folder!

What do I do if I forgot my username?

Terms Privacy ©2013 Snapchat, Inc.

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



Is there any way to view an image after the time has expired?

No, snaps disappear after the timer runs out. You can save snaps that you capture by pressing the save button on the preview screen.

No, snaps disappear after the timer runs out. You can save snaps that you capture by pressing the save button on the preview screen.

What if I take a screenshot?

Screenshots can be captured if you're quick. The sender will be notified if we detect you have taken a screenshot.

Usernames and Passwords

What do I do if I forgot my password? How do I reset/change my password?

You can reset your password from the Snapchat application. First attempt to login with your username/email and an incorrect password, the app will prompt you to "Try Again" or "Reset Password." Tap "Reset Password" and follow the instructions sent to your email address to reset the password and access your account.

If you don't receive a password reset email within an hour or so, be sure to check for it in your spam folder!

What do I do if I forgot my username?

[Terms](#) [Privacy](#) ©2013 Snapchat, Inc.

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

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 synonymous, 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



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.

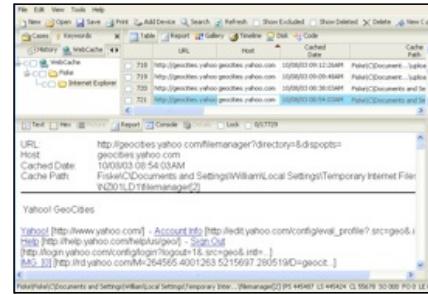
TV digital forensics:

- 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



Result:

—DF is a difficult process that looks easy

EnCase



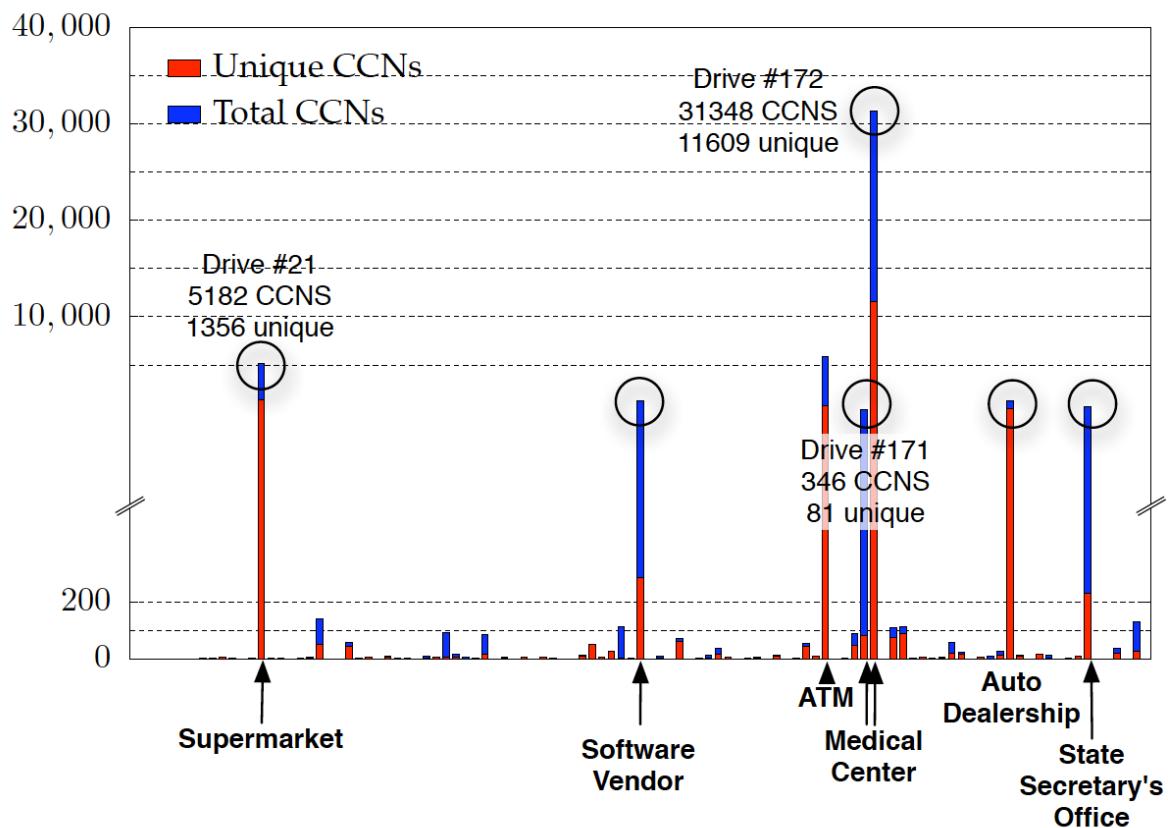
Digital media triage: Deciding where to start

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



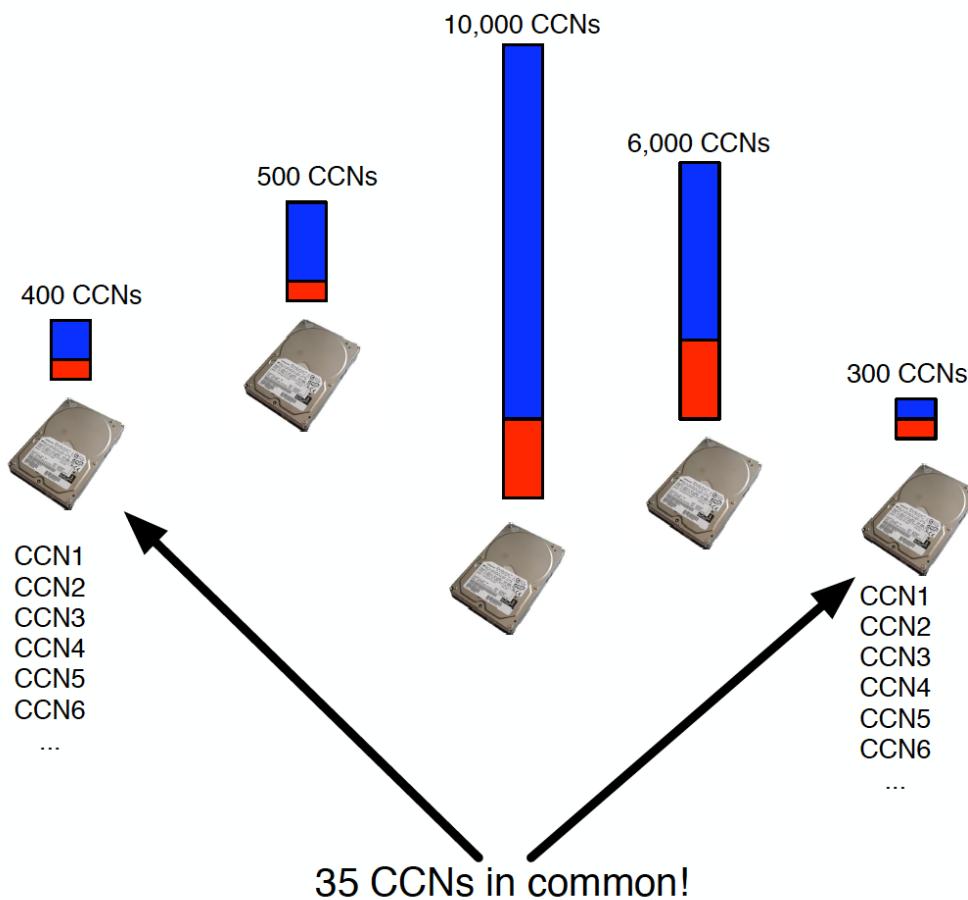
Where do you start?

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?



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.