Harassment at

NITROBA
State University

The case

NITROBA
State University

You are a staff member at the Nitroba University Incident Response Team.

Lily Tuckrige is teaching chemistry CHEM109 this summer at NSU.

Tuckrige has been receiving harassing email at her personal email address.

- Tuckrige's personal email is lilytuckrige@yahoo.com
- She thinks that it is from one of the students in her class.

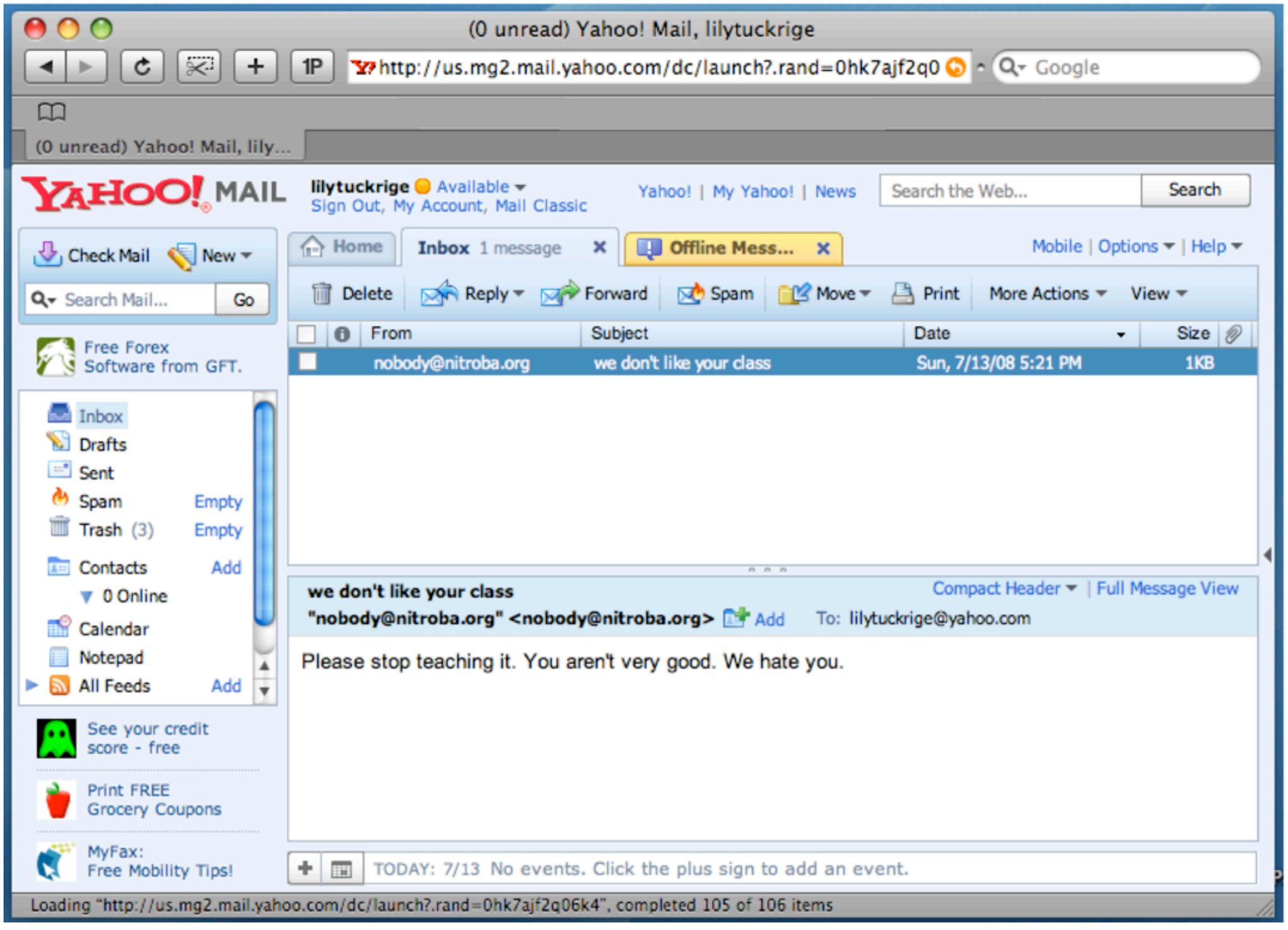
Tuckrige contacted IT support.

- She sent a screen shot of one of the harassing email messages.
- She wants to know who is doing it.

istockphoto.com

The email message.

NITROBA
State University



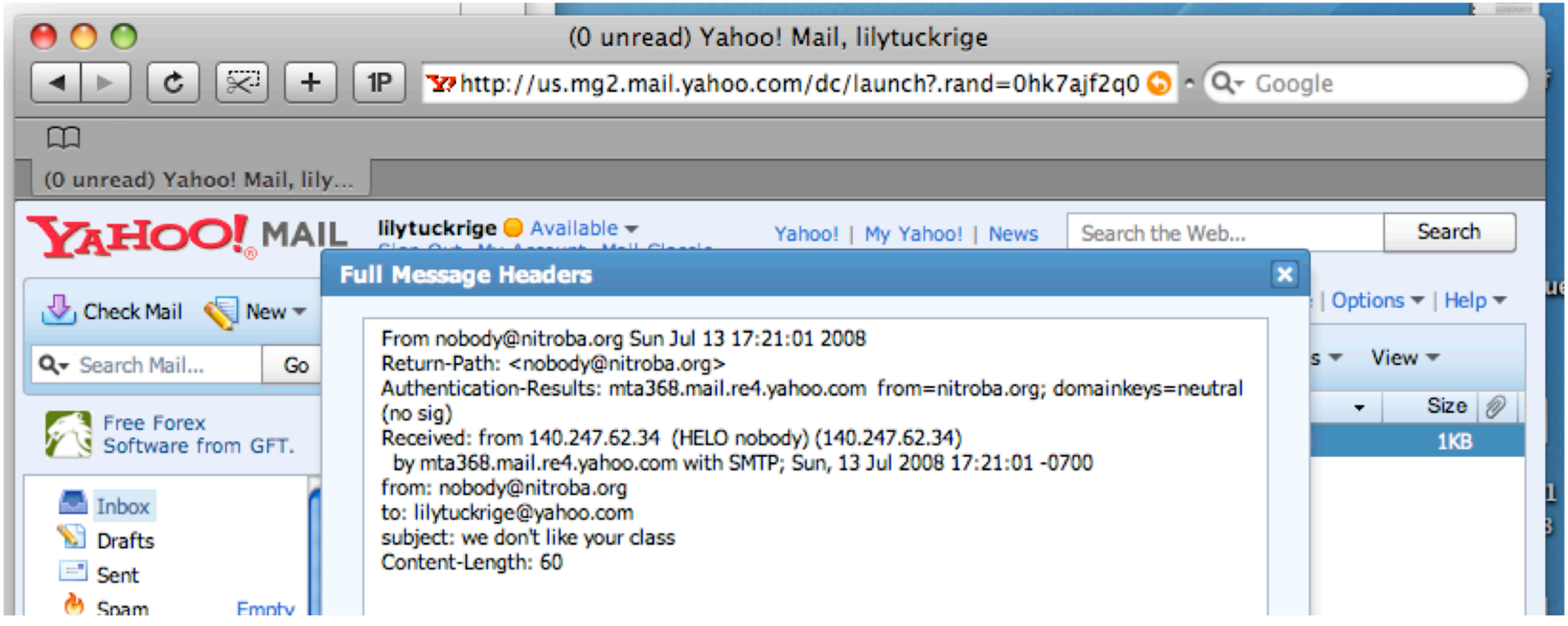
Nitroba's IT wrote back to Lily.

NITROBA
State University

The IT tech told Lily:

- The screen shot wasn't tremendously useful.
- Can you get the full headers?

Lily sent back a screen shot with the headers:



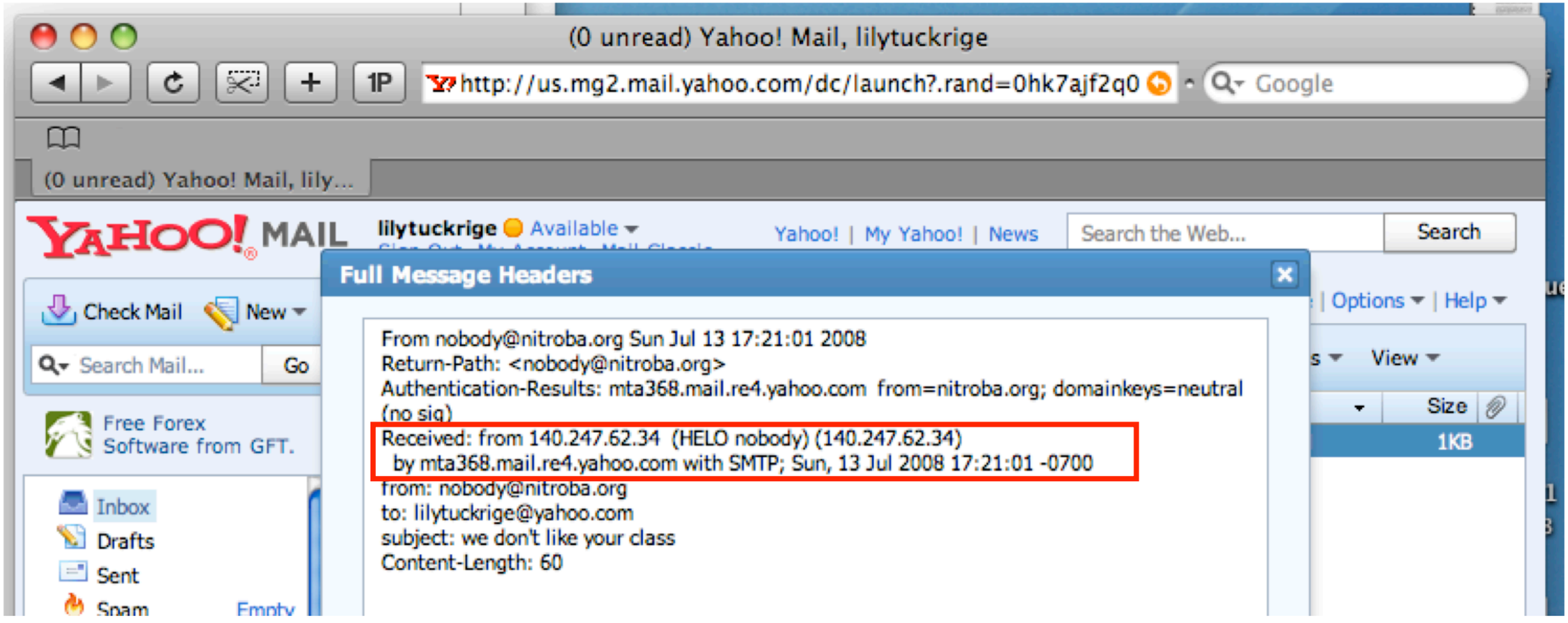
Nitroba's IT wrote back to Lily.

NITROBA
State University

The IT tech told Lily:

- The screen shot wasn't tremendously useful.
- Can you get the full headers?

Lily sent back a screen shot with the headers:



The IP address points to a nitroba dorm room.


```
$ host 140.247.62.34
34.62.247.140.in-addr.arpa domain name pointer G24.student.nitroba.org
$
```

The Dorm Room

NITROBA
State University

Three women share the room:

- Alice
- Barbara
- Candice

Nitroba provides 10mbps Ethernet in every room but no Wi-Fi.

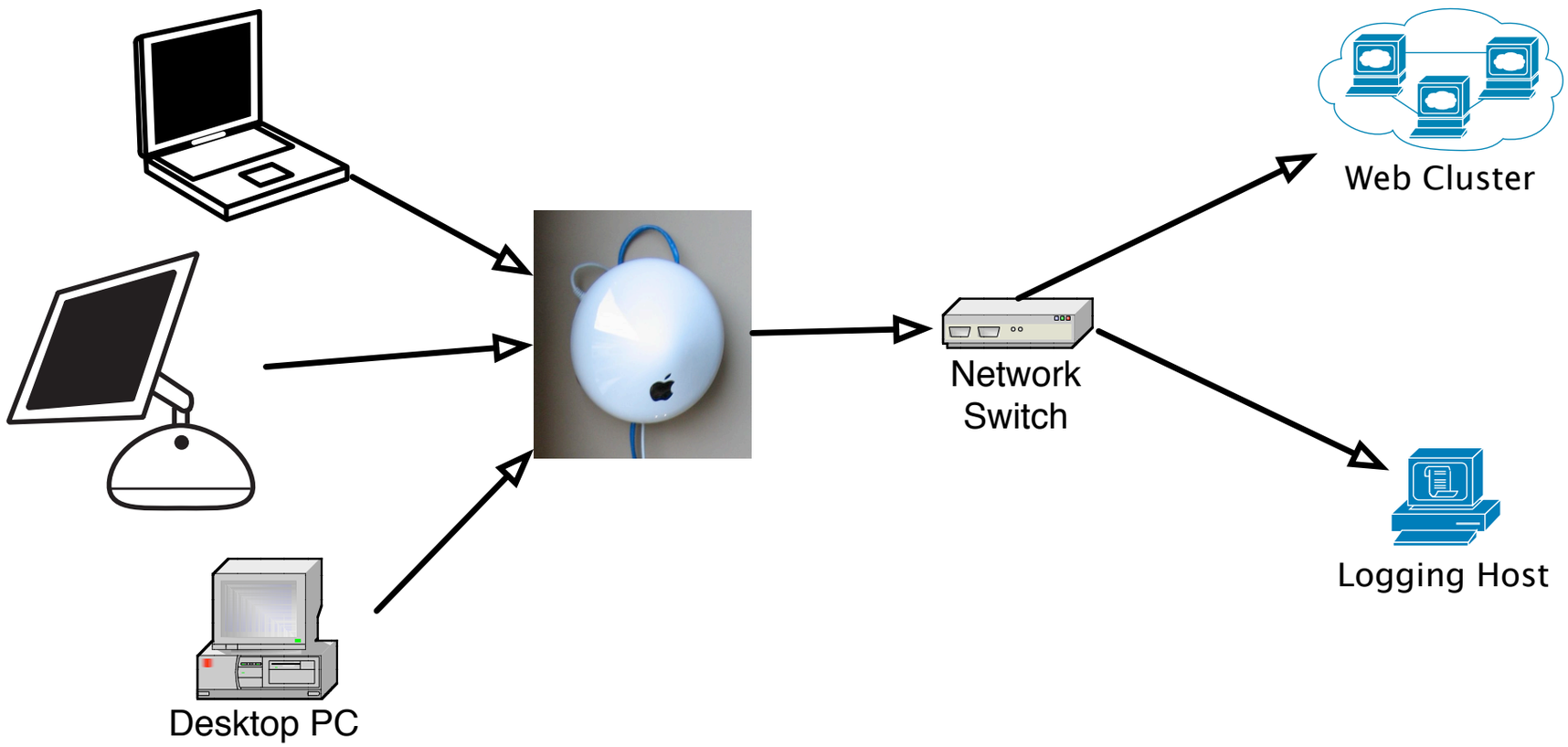
Barbara's boyfriend Kenny installed a Wi-Fi router in the room.

There is no password on the router.

photo credit: epa.gov

To find out what's going on, Nitroba's IT sets up a packet sniffer

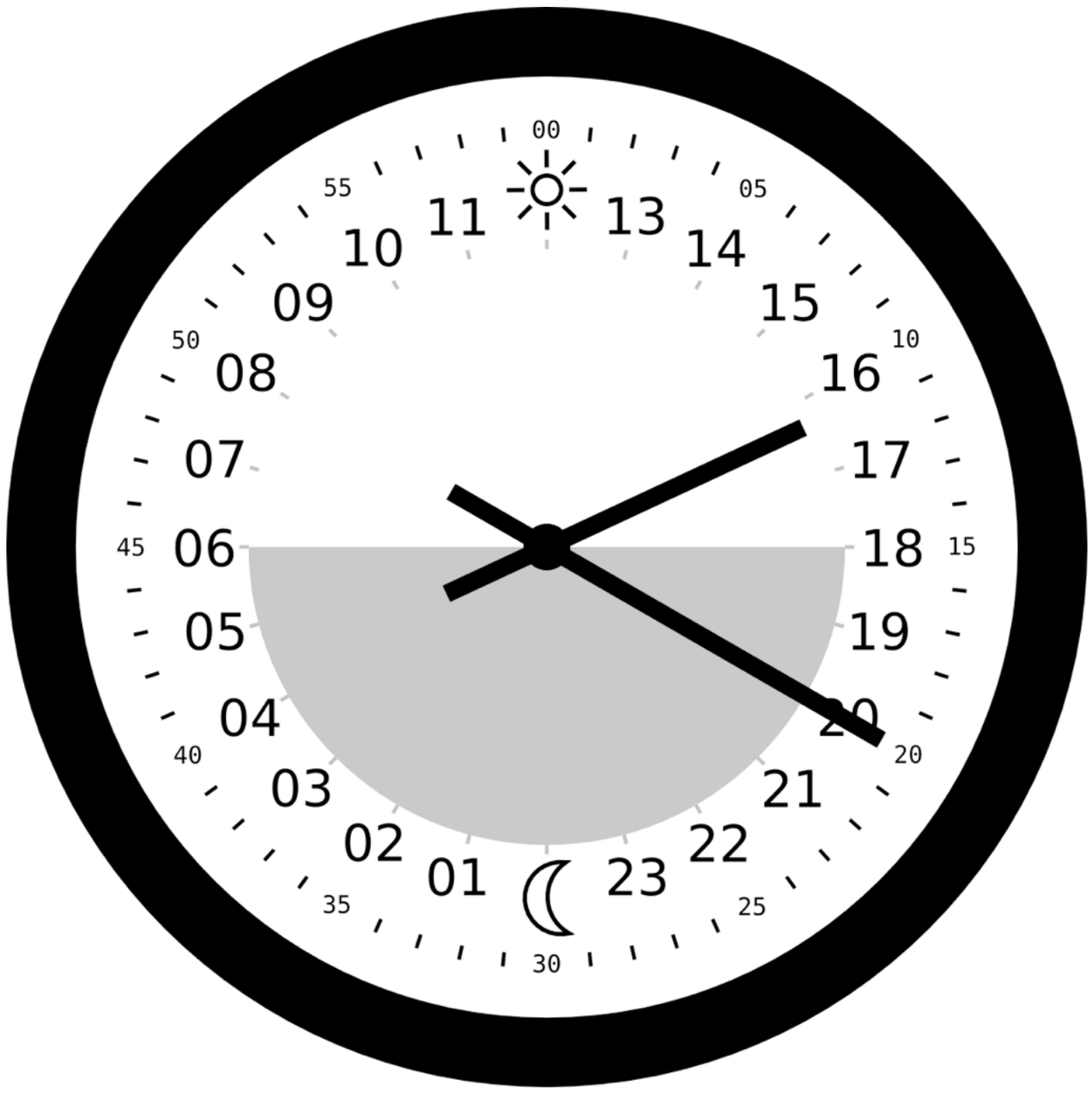
NITROBA
State University



Who is sending the harassing mail?

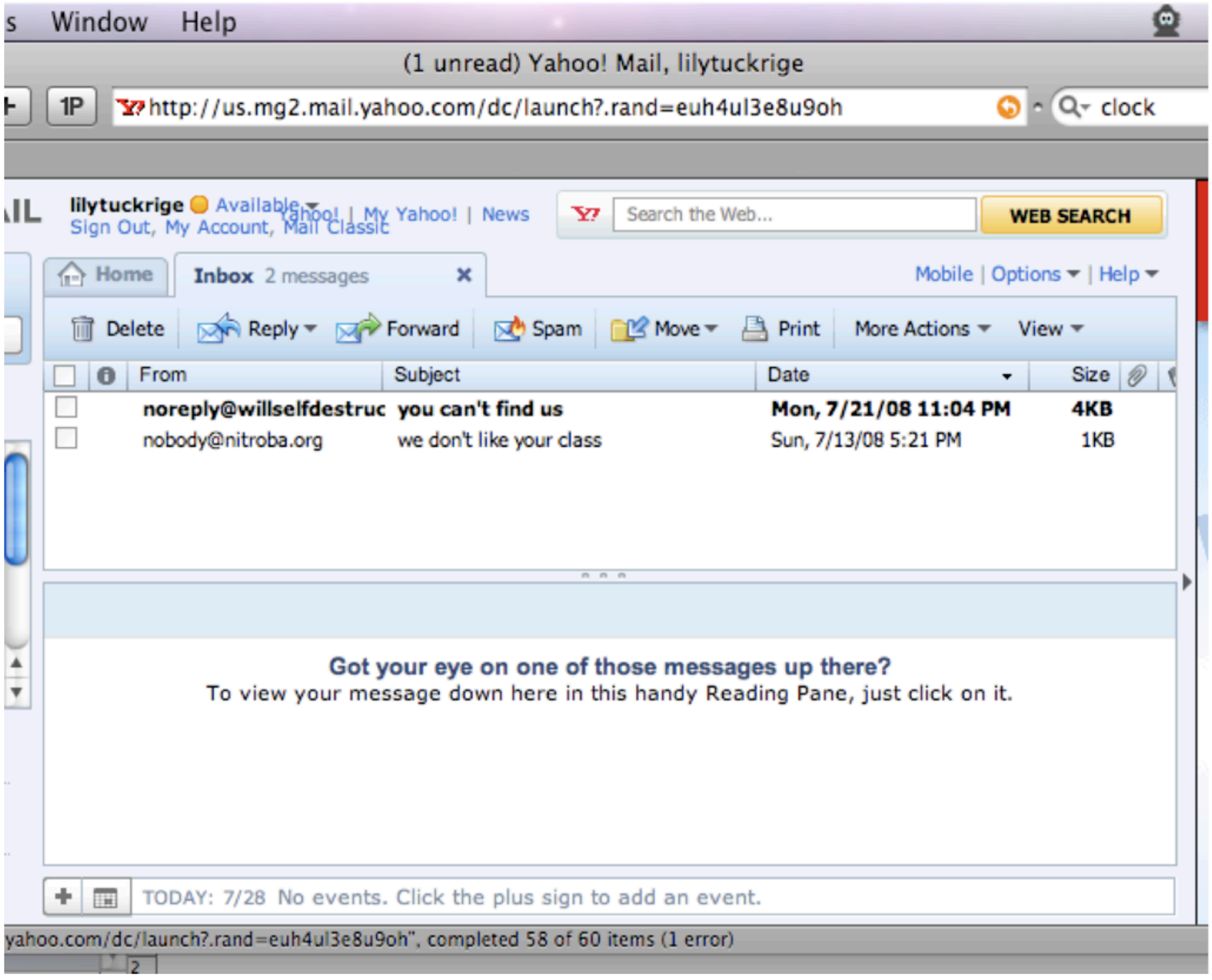
Now we wait

NITROBA
State University



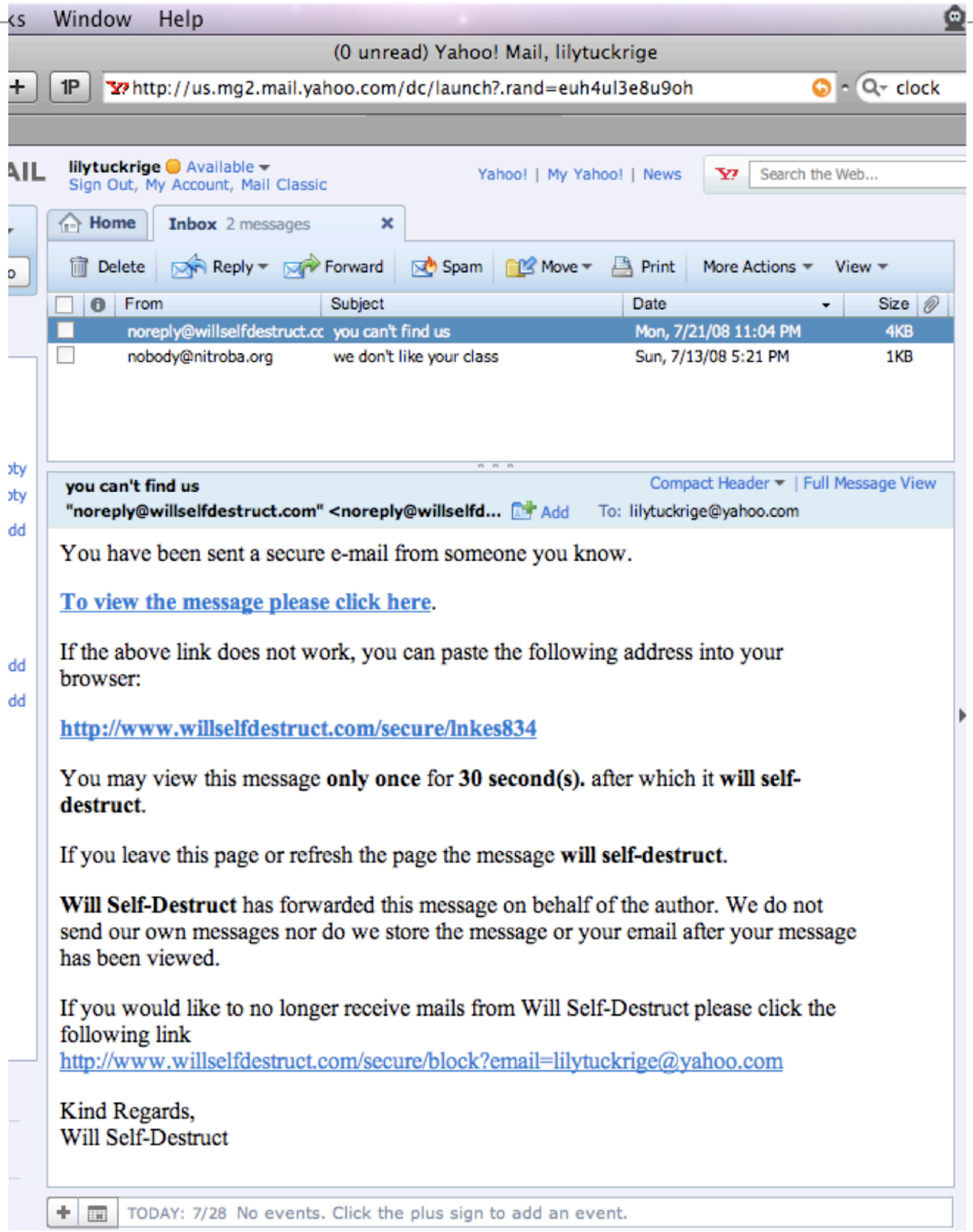
The guy attacked!

NITROBA
State University



And here is the message:

NITROBA
State University

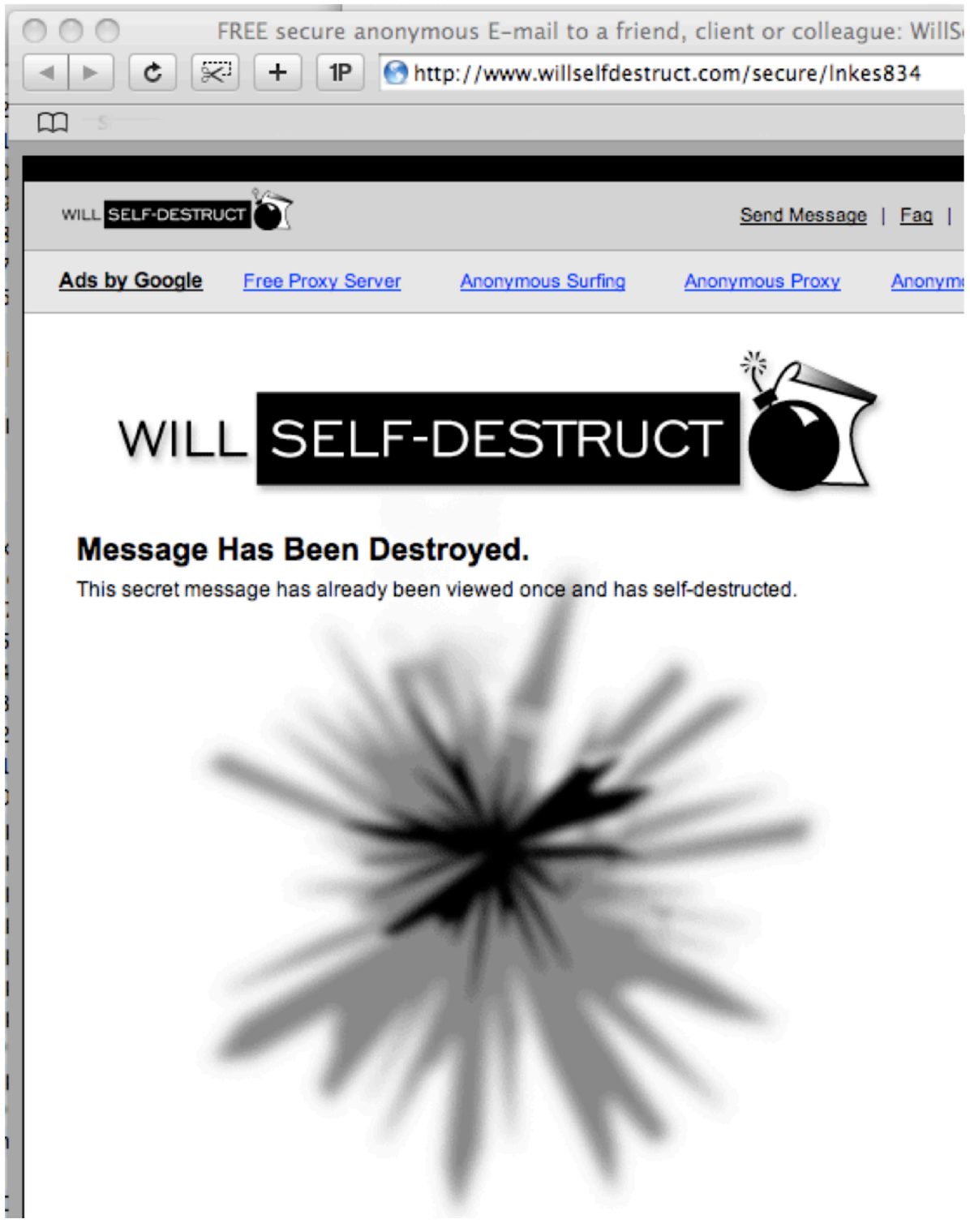


No, here is the message

NITROBA
State University

And there goes the message:

NITROBA
State University



So who did it?

NITROBA
State University

```
Chemistry 109 class list:

Teacher: Lily Tuckrige

Students:
     Amy Smith
     Burt Greedom
     Tuck Gorge
     Ava Book
     Johnny Coach
     Jeremy Ledvkin
     Nancy Colburne
     Tamara Perkins
     Esther Pringle
     Asar Misrad
     Jenny Kant
```

How to solve this problem:

NITROBA
State University

1. Map out the Nitroba dorm room network.
2. Find who sent email to lilytuckrige@yahoo.com
   - Look for a TCP flow that includes the hostile message
   - Find information that can tie that message to a particular web browser.
3. Identify the other TCP connections that below to the attacker
4. Find information in one of those TCP connections that IDs the attacker.