

Harassment at

**NITROBA
State University**

The case

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

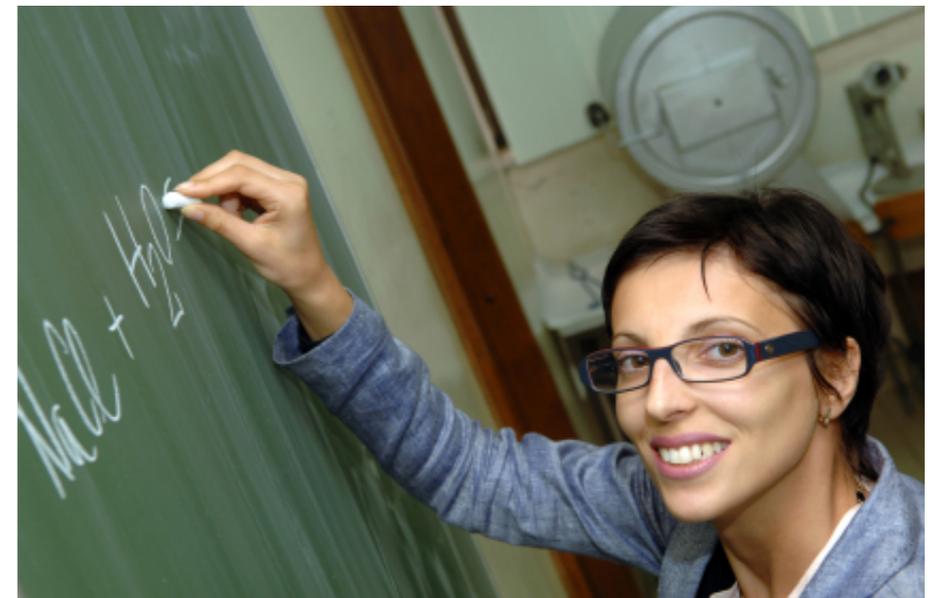
Lily Tuckrige is teaching chemistry CHEM109 this summer at NSU.

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

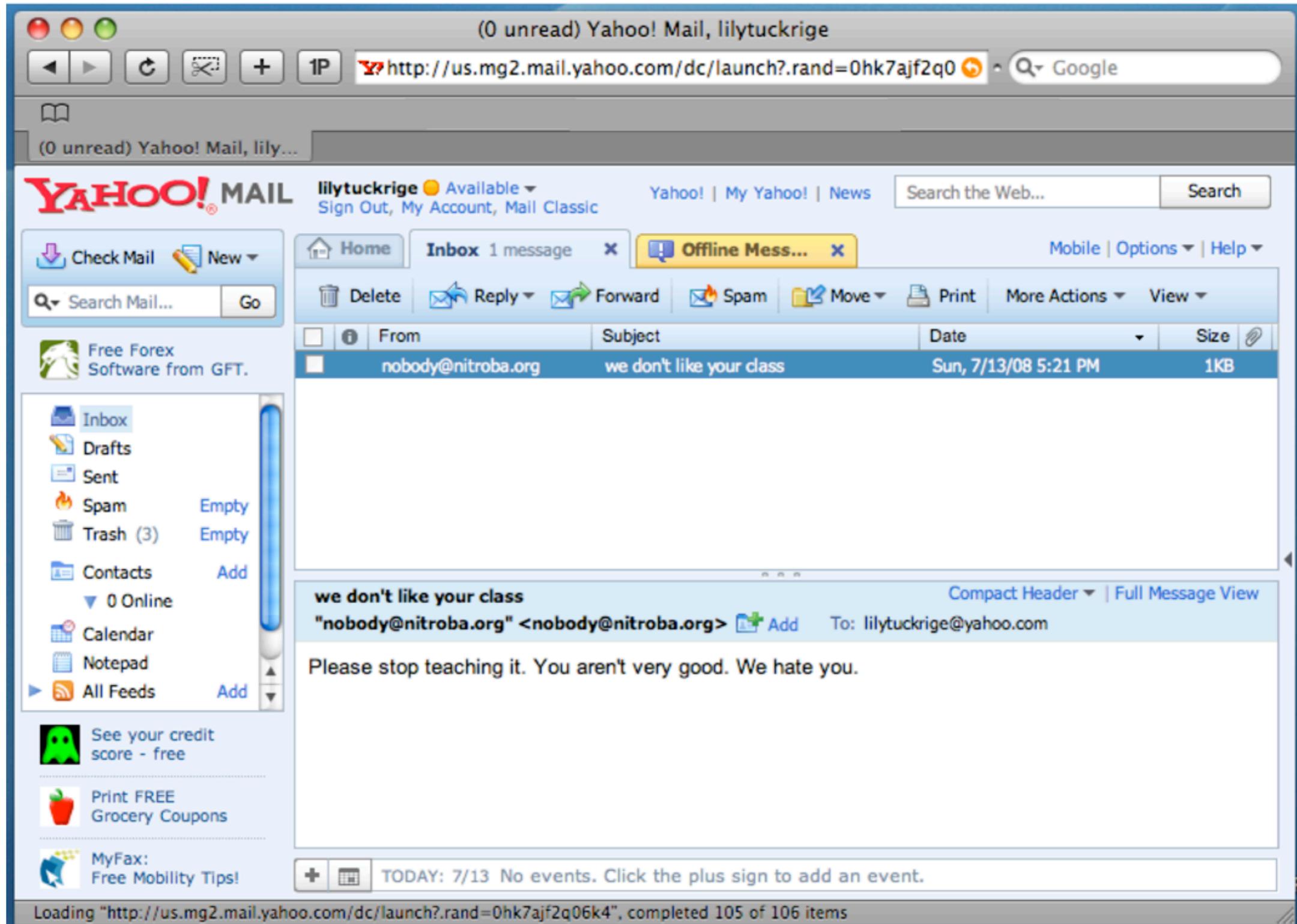
- Tuckrige's personal email is lilytuckrige@yahoo.com
- She thinks that it is from one of the students in her class.

Tuckrige contacted IT support.

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



The email message.

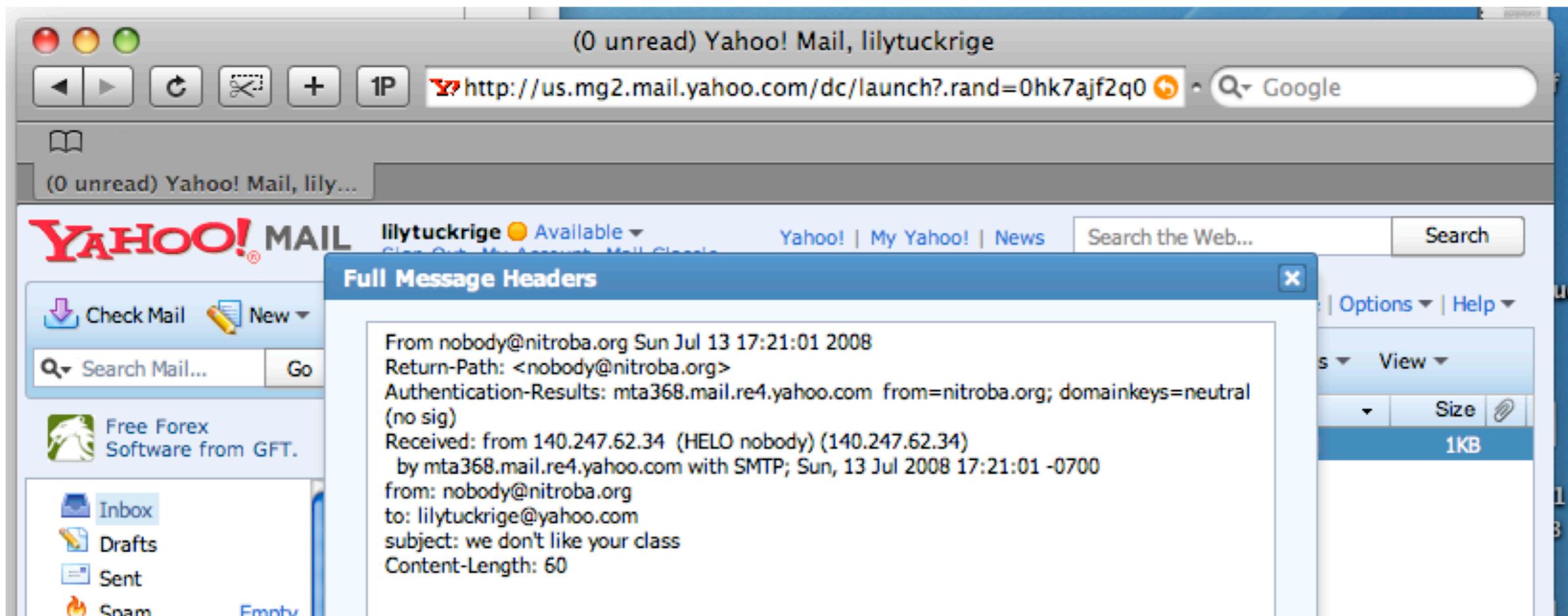


Nitroba's IT wrote back to Lily.

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:

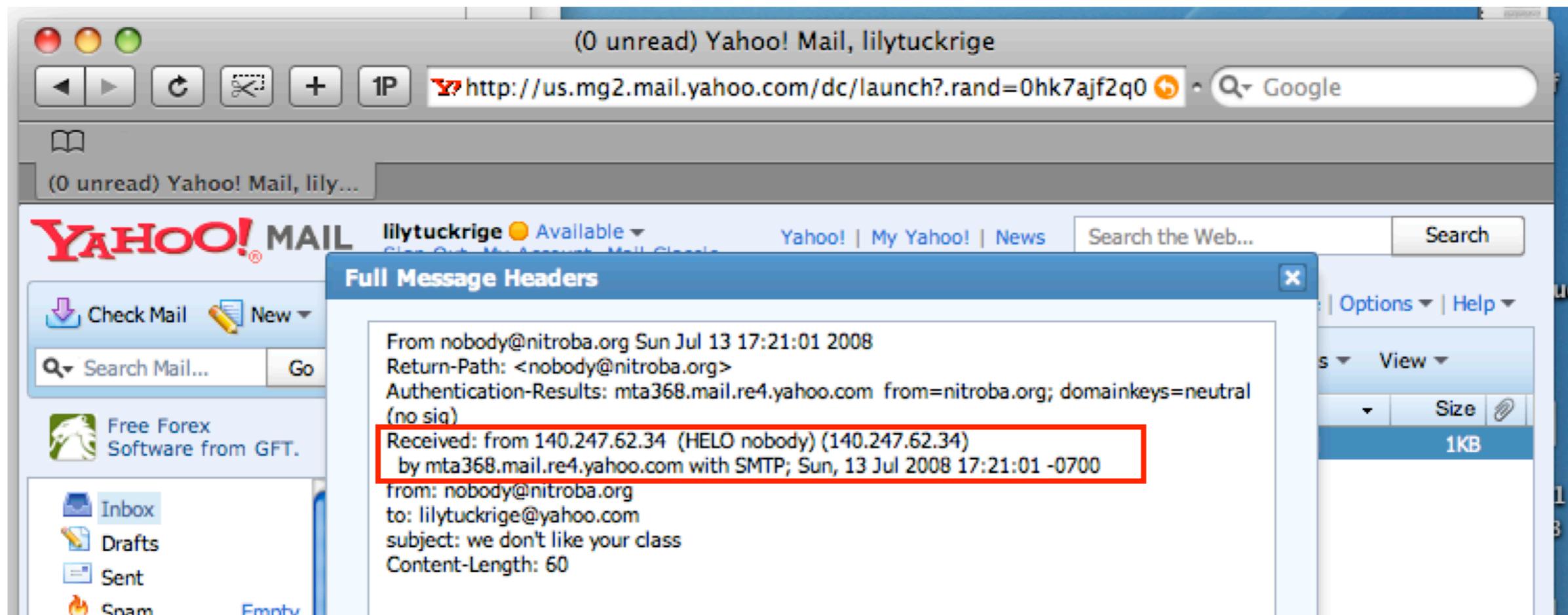


Nitroba's IT wrote back to Lily.

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.

The logo for Nitroba State University, featuring the text "NITROBA" on the top line and "State University" on the bottom line, set against a background that transitions from pink on the left to orange on the right.

```
$ host 140.247.62.34
```

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

```
$
```

The Dorm Room

Three women share the room:

- Alice
- Barbara
- Candice

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

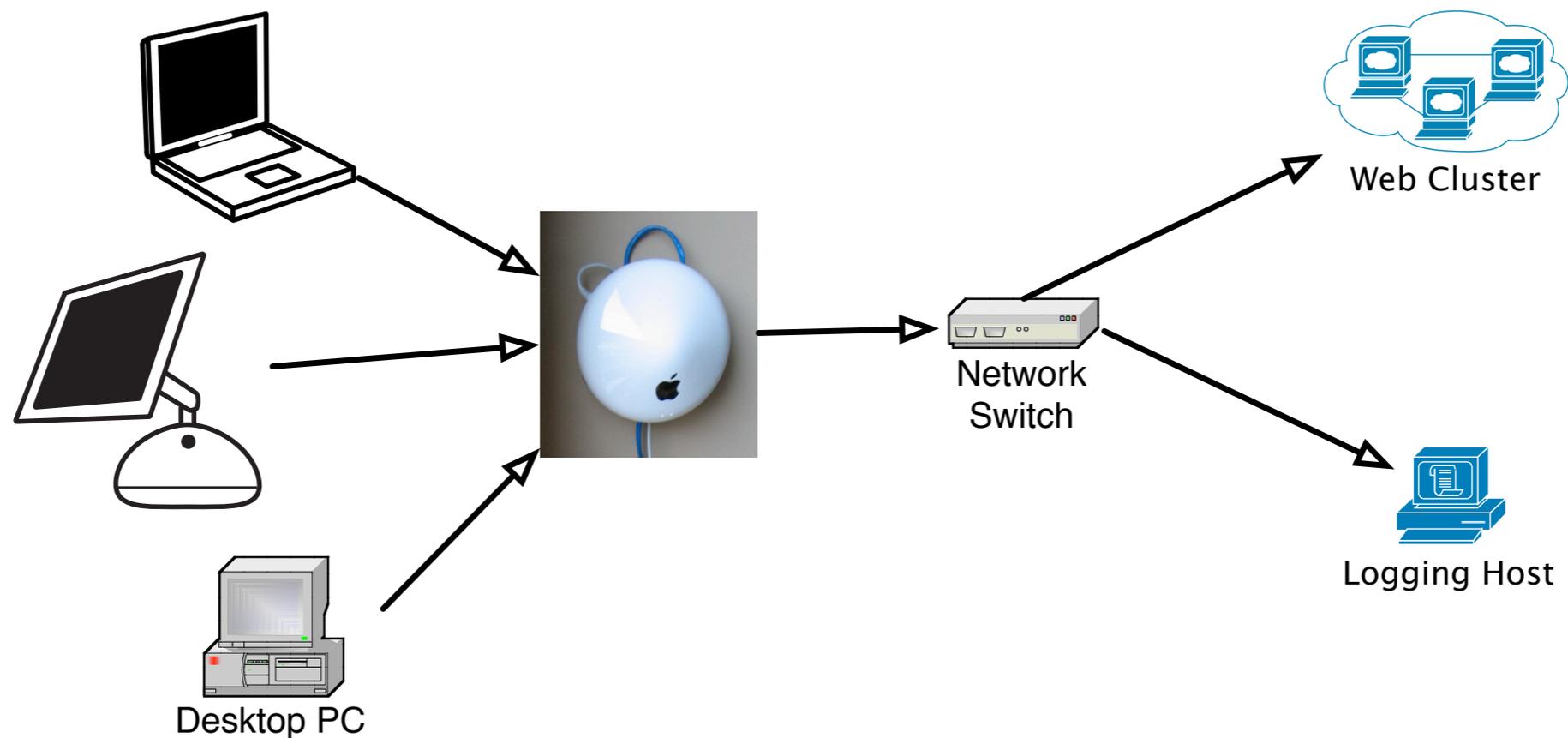
Barbara's boyfriend Kenny installed a Wi-Fi router in the room.

There is no password on the router.



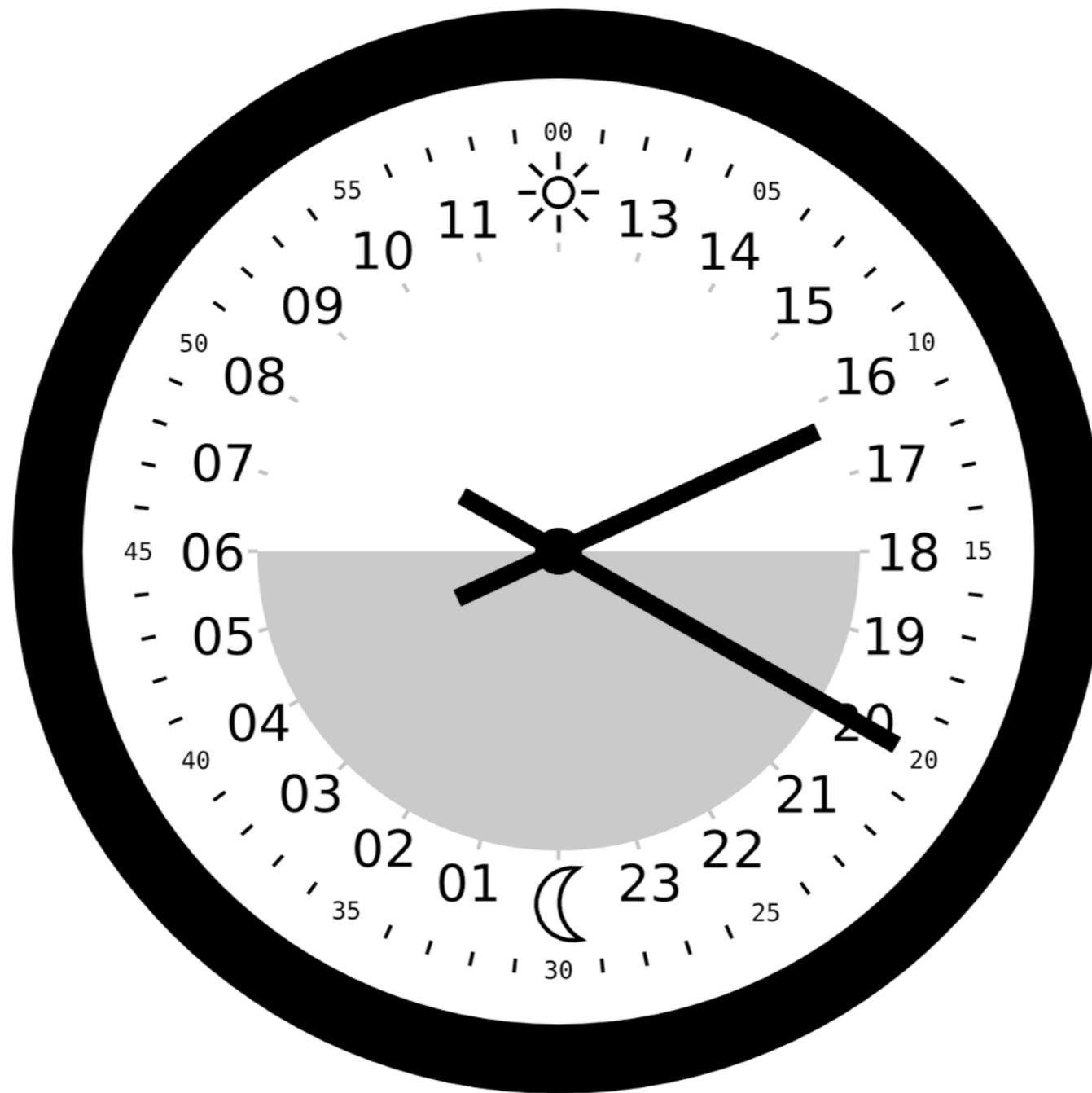
photo credit: epa.gov

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

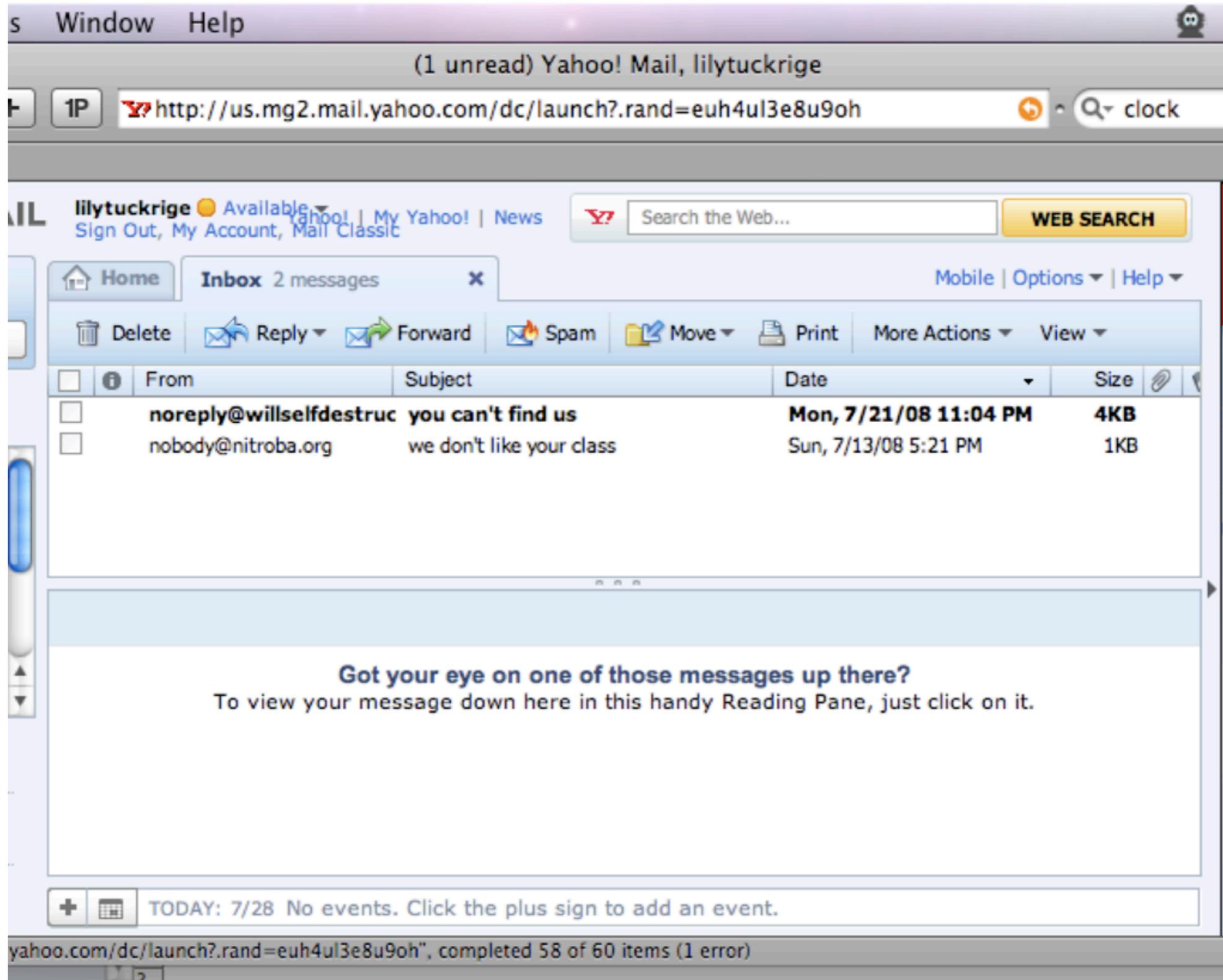


Who is sending the harassing mail?

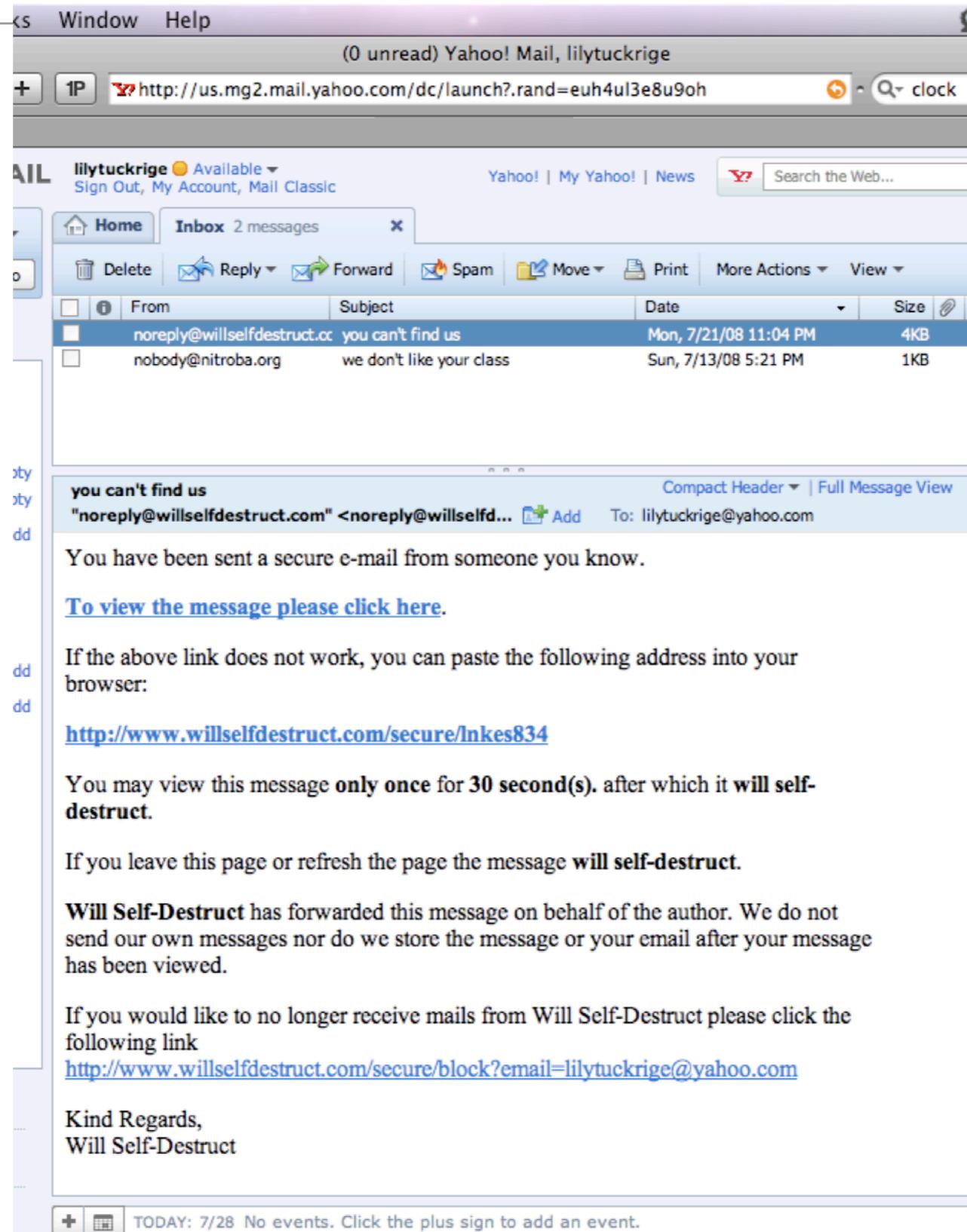
Now we wait



The guy attacked!



And here is the message:



No, here is the message

FREE secure anonymous E-mail to a friend, client or colleague: WillSelfDestruct

http://www.willselfdestruct.com/secure/lnkes834

WILL SELF-DESTRUCT

Send Message | [Faq](#) | [Blog](#) | [Feedback](#) | [B2B](#) | [Legal](#)

[Ads by Google](#) | [Free Proxy Server](#) | [Anonymous Surfing](#) | [Anonymous Proxy](#) | [Anonymous Browsing](#) | [Anonymous Em](#)

WILL SELF-DESTRUCT

This message will self-destruct in **4 second(s)**. If you leave this page or refresh the message will be destroyed.

From: [Undisclosed Sender]
To: lilytuckrige@yahoo.com
Subject: you can't find us

Message:

and you can't hide from us.
Stop teaching.
Start running.

Will Self-Destruct is For Sale

We've had a lot of fun with over the years but we are moving to pastures greener you are interested in buying you can either visit [ebay](#) [contact us](#) directly.

[Mission Impossible Ver...](#)

Ads by Google

[Tom Cruise in M:!](#)
The Site You Have Been Waiting For- TomCruise.com. The Official Site.
[TomCruise.com](#)

[Free Trial - Mass Ema](#)
99.9% Highest Inbox Deliverability. Test Drive our Mass Emailer Free!
[www.iContact.com](#)

[Gambling Anonymou](#)
Licensed, Individualized Treatment & Financial Aid. Get Treated Today

Loading "http://www.willselfdestruct.com/secure/lnkes834", completed 12 of 26 items

And there goes the message:



So who did it?

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:

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 belong to the attacker
4. Find information in one of those TCP connections that identifies the attacker.