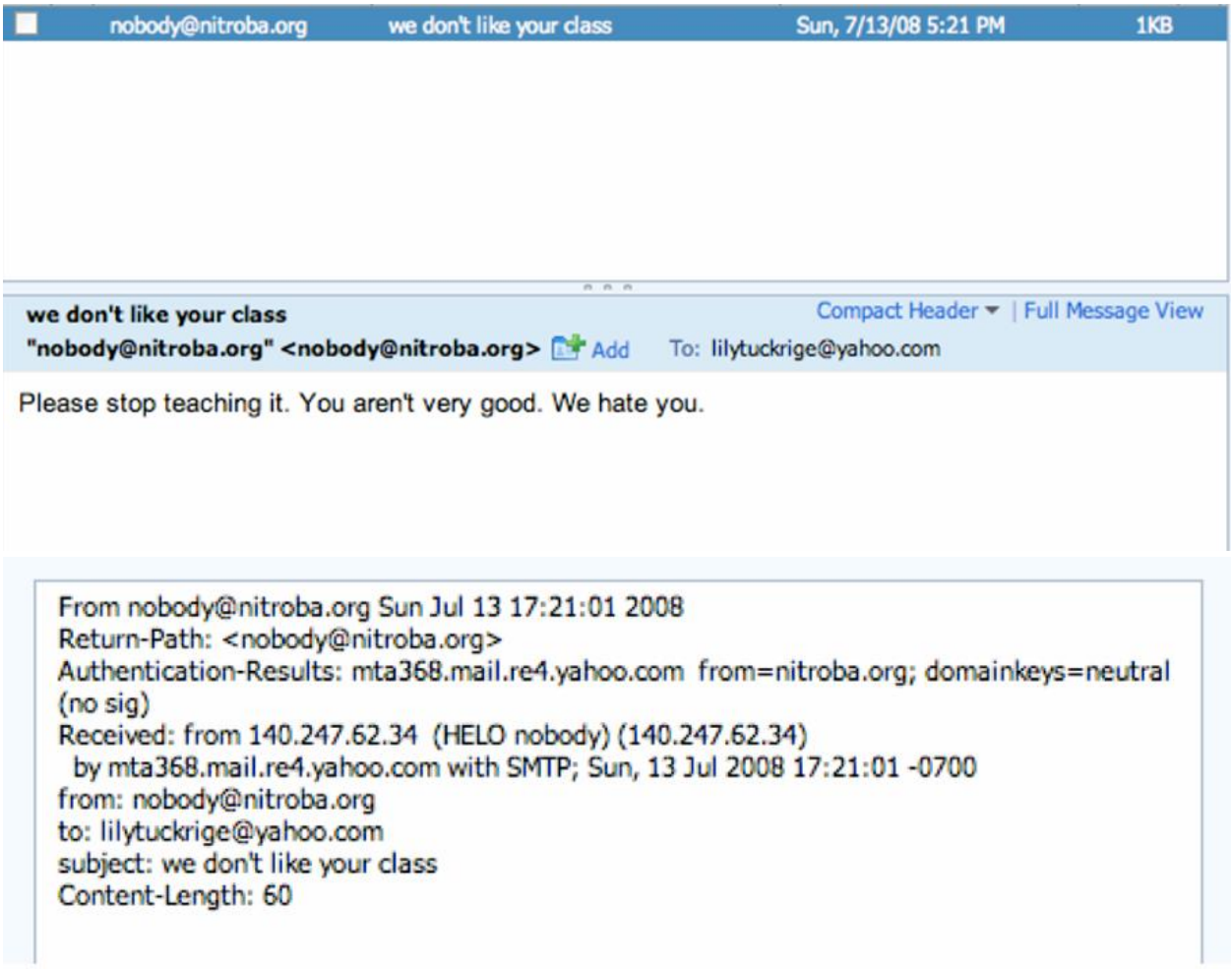
Digital Corpora

Nitroba case:

Lily Tuckrige

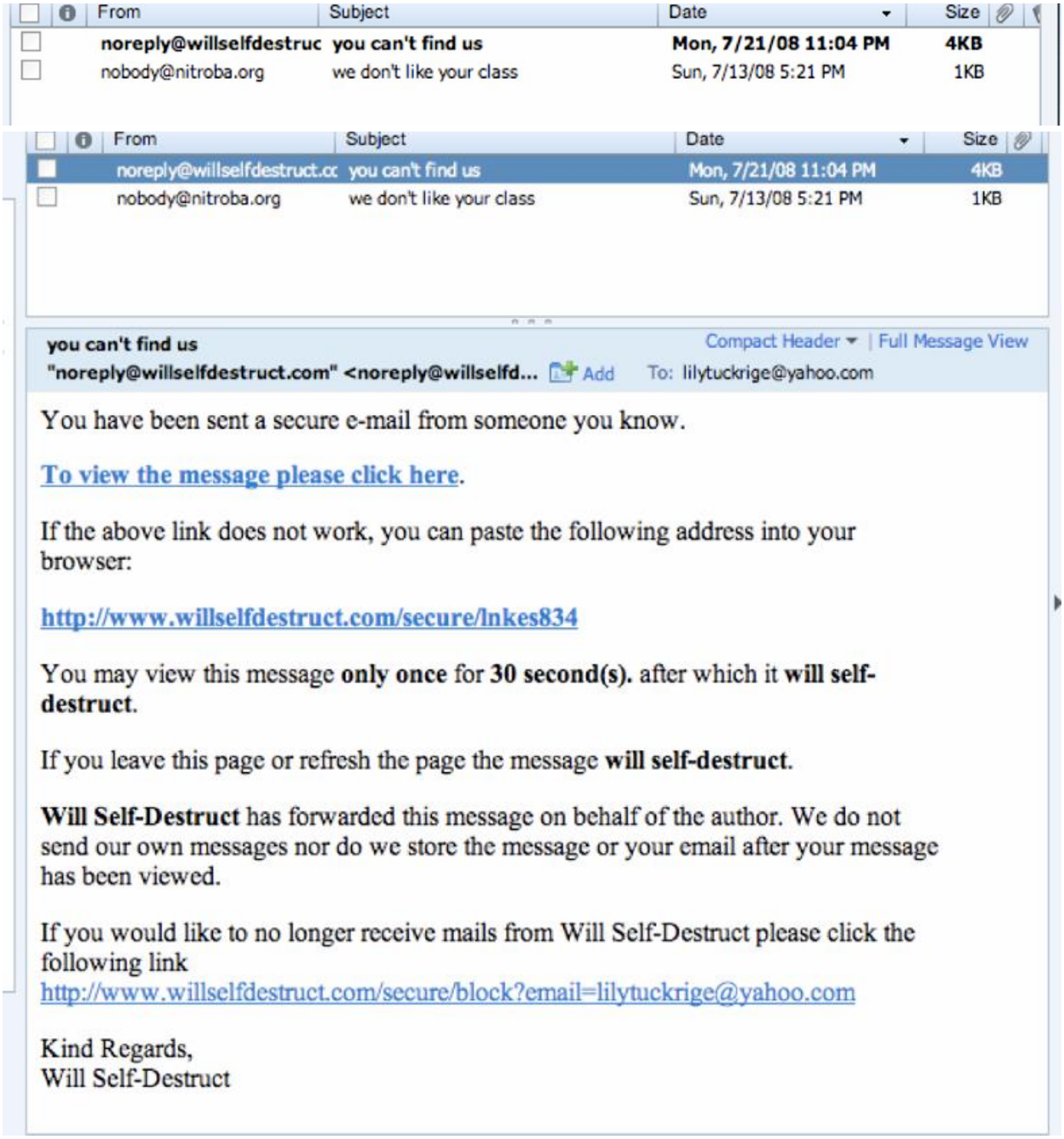
CHEM109 this summer at NSU

lilytuckrige@yahoo.com



host 140.247.62.34

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



From	Subject	Date	Size
noreply@willselfdestruc	**you can't find us**	**Mon, 7/21/08 11:04 PM**	**4KB**
nobody@nitroba.org	we don't like your class	Sun, 7/13/08 5:21 PM	1KB

From	Subject	Date	Size
noreply@willselfdestruct.cc	you can't find us	Mon, 7/21/08 11:04 PM	4KB
nobody@nitroba.org	we don't like your class	Sun, 7/13/08 5:21 PM	1KB

you can't find us

Compact Header | Full Message View

"noreply@willselfdestruct.com" <noreply@willselfd... Add To: lilytuckrige@yahoo.com

You have been sent a secure e-mail from someone you know.

To view the message please click here.

If the above link does not work, you can paste the following address into your browser:

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

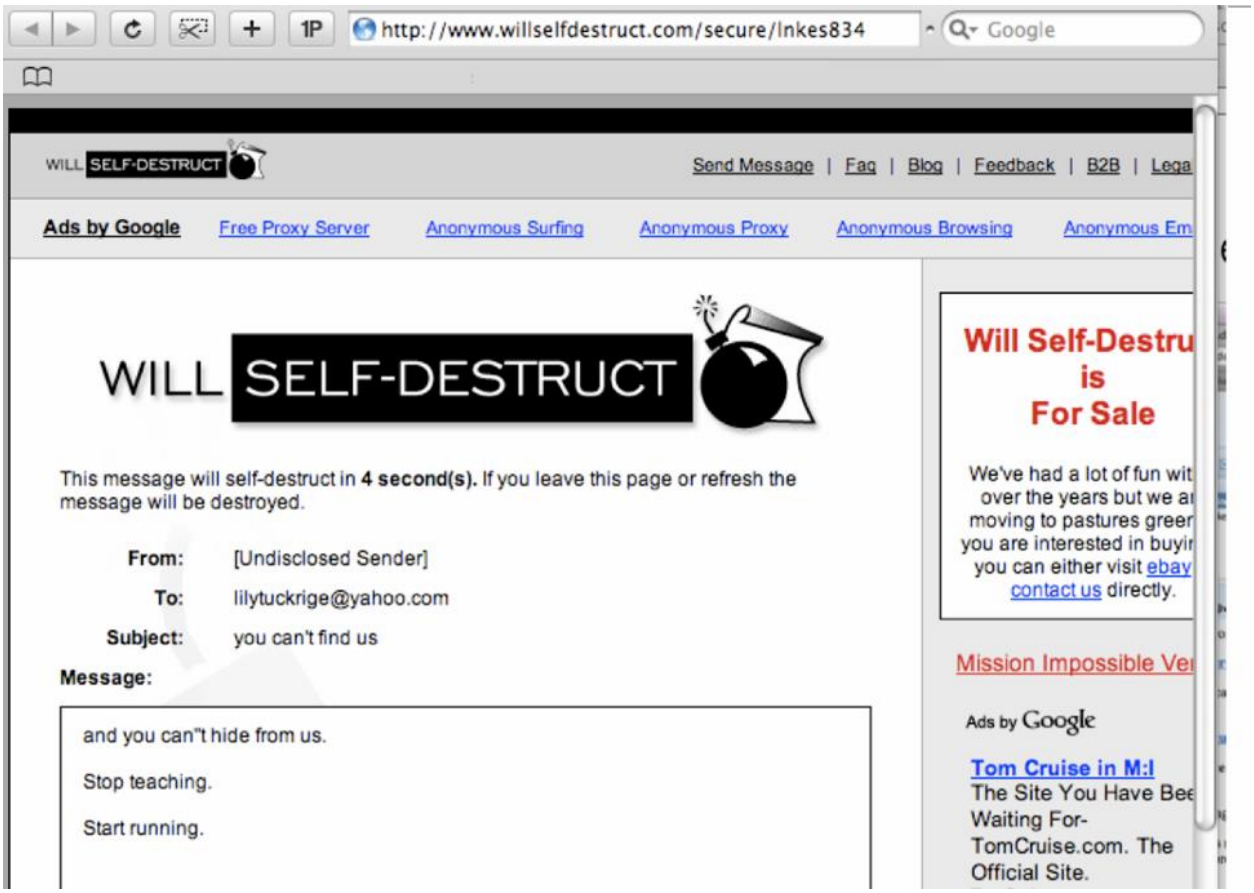
You may view this message **only once** for **30 second(s).** after which it **will self-destruct**.

If you leave this page or refresh the page the message **will self-destruct**.

Will Self-Destruct has forwarded this message on behalf of the author. We do not send our own messages nor do we store the message or your email after your message has been viewed.

If you would like to no longer receive mails from Will Self-Destruct please click the following link
http://www.willselfdestruct.com/secure/block?email=lilytuckrige@yahoo.com

Kind Regards,
Will Self-Destruct



Amy Smith

Burt Greedom

Tuck Gorge

Ava Book

Johnny Coach

Jeremy Ledvkin

Nancy Colburne

Tamara Perkins

Esther Pringle

Asar Misrad

Jenny Kant

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.

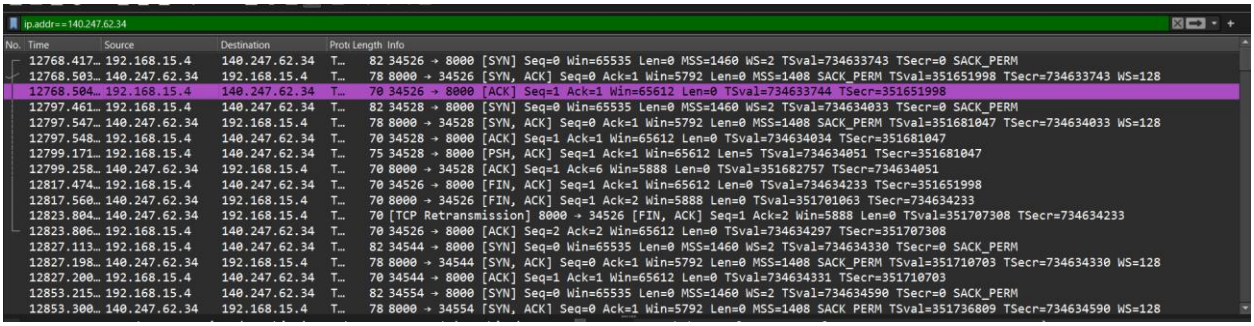
3. Identify the other TCP connections that below to the attacker

4. Find information in one of those TCP connections that IDs the attacker

---

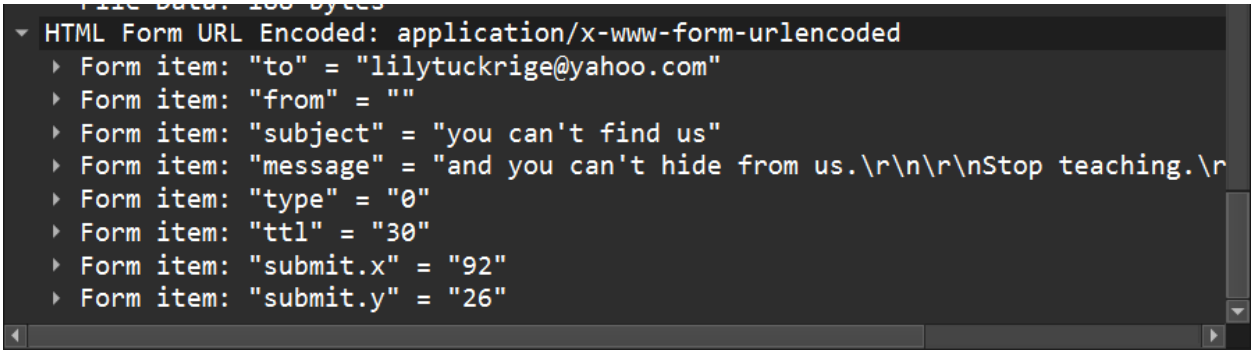
1

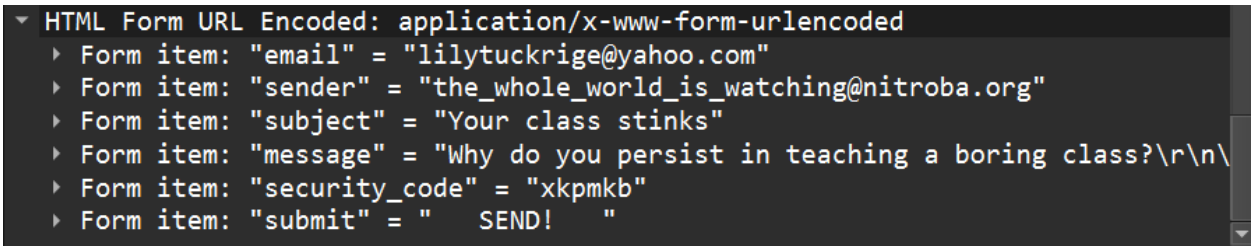
Checking 140.247.62.34

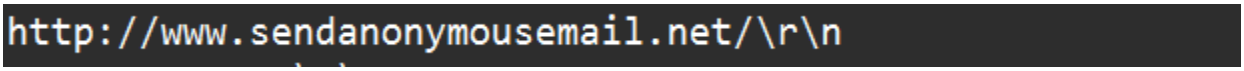


192.168.15.4 as source ip

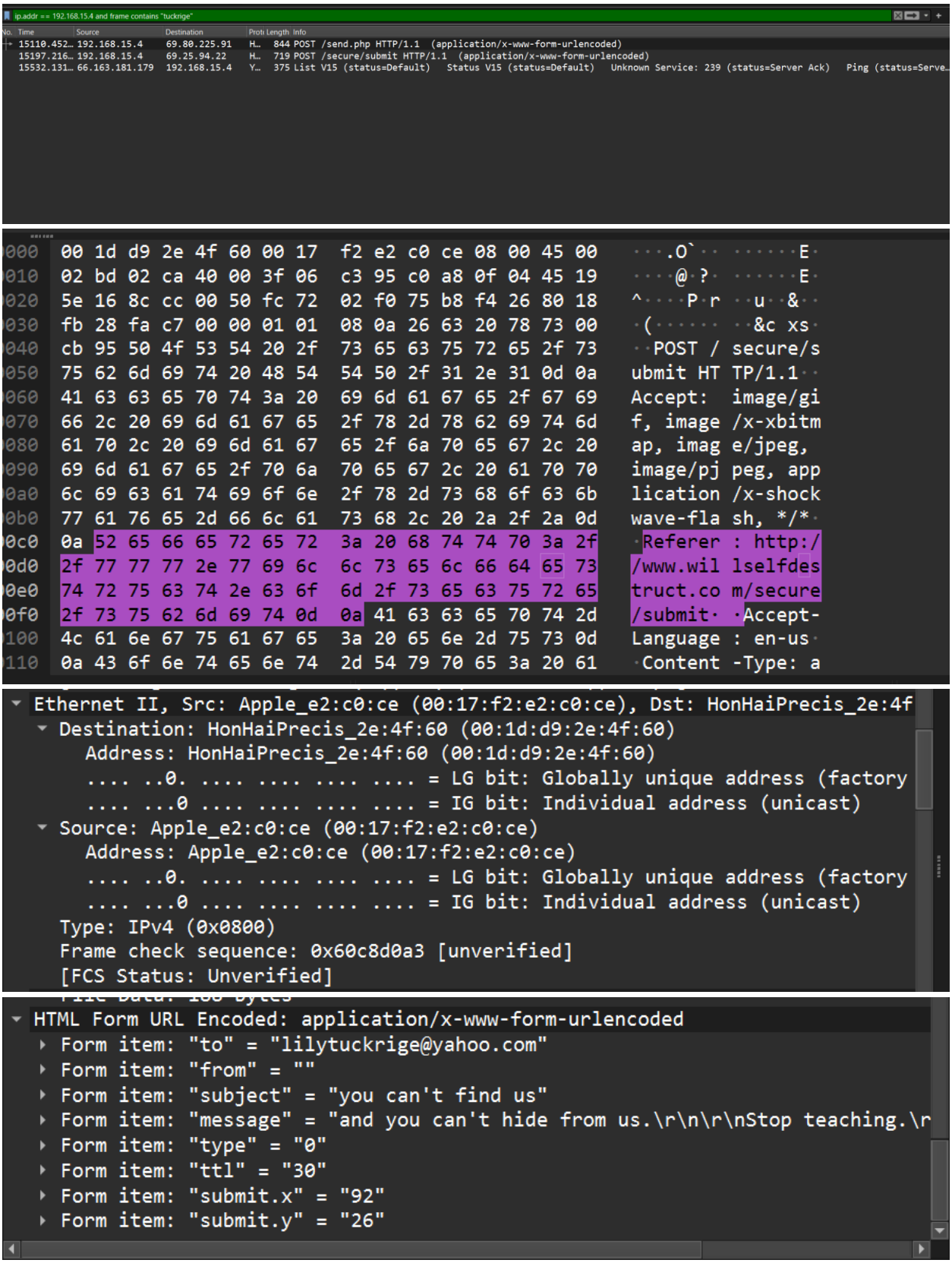
Let's use again the filter capabilities of Wireshark : frame contains "tuckrige"







The source IP is 192.168.15.4, and the destination IP is 69.80.225.91

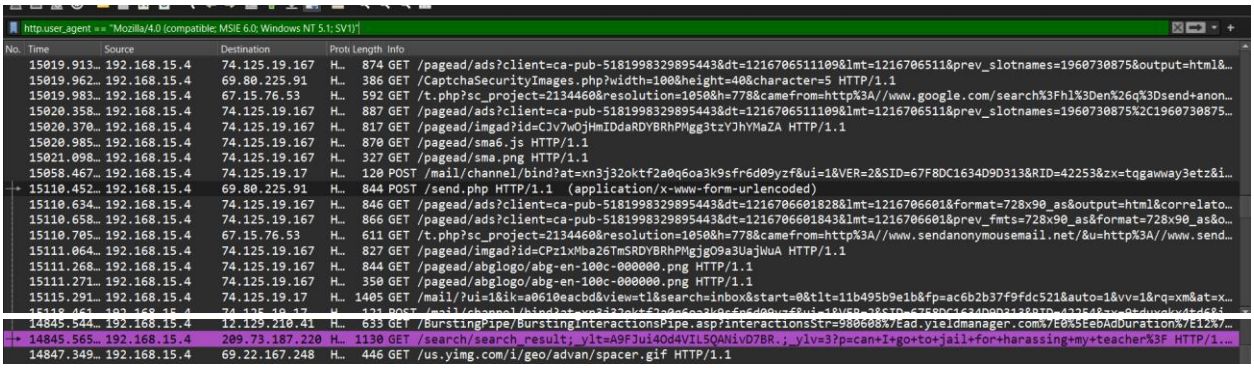


The source IP is 192.168.15.4, and the destination IP is 69.25.94.22

IP	MAC	Hardware
192.168.15.4 (source)	**00:17:f2:e2:c0:ce**	**Apple**
140.247.62.34 (destination)	**00:1f:d9:2e:4f:60**	**HonHaiPr**

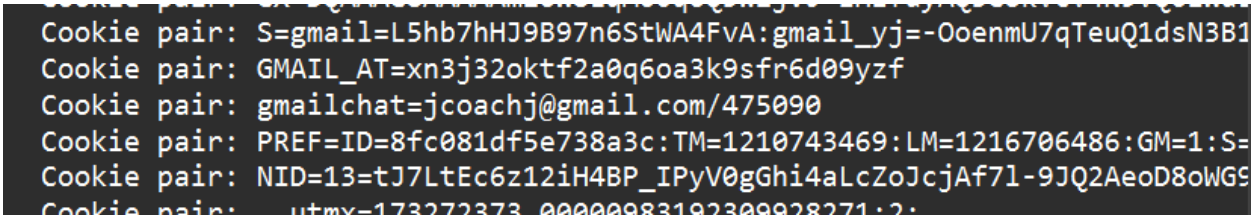
After checking packets

User-agent Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)



I check for accounts by names

So I found google acount and mail acount



jcoachj@gmail.com

that was Johnny Coach