

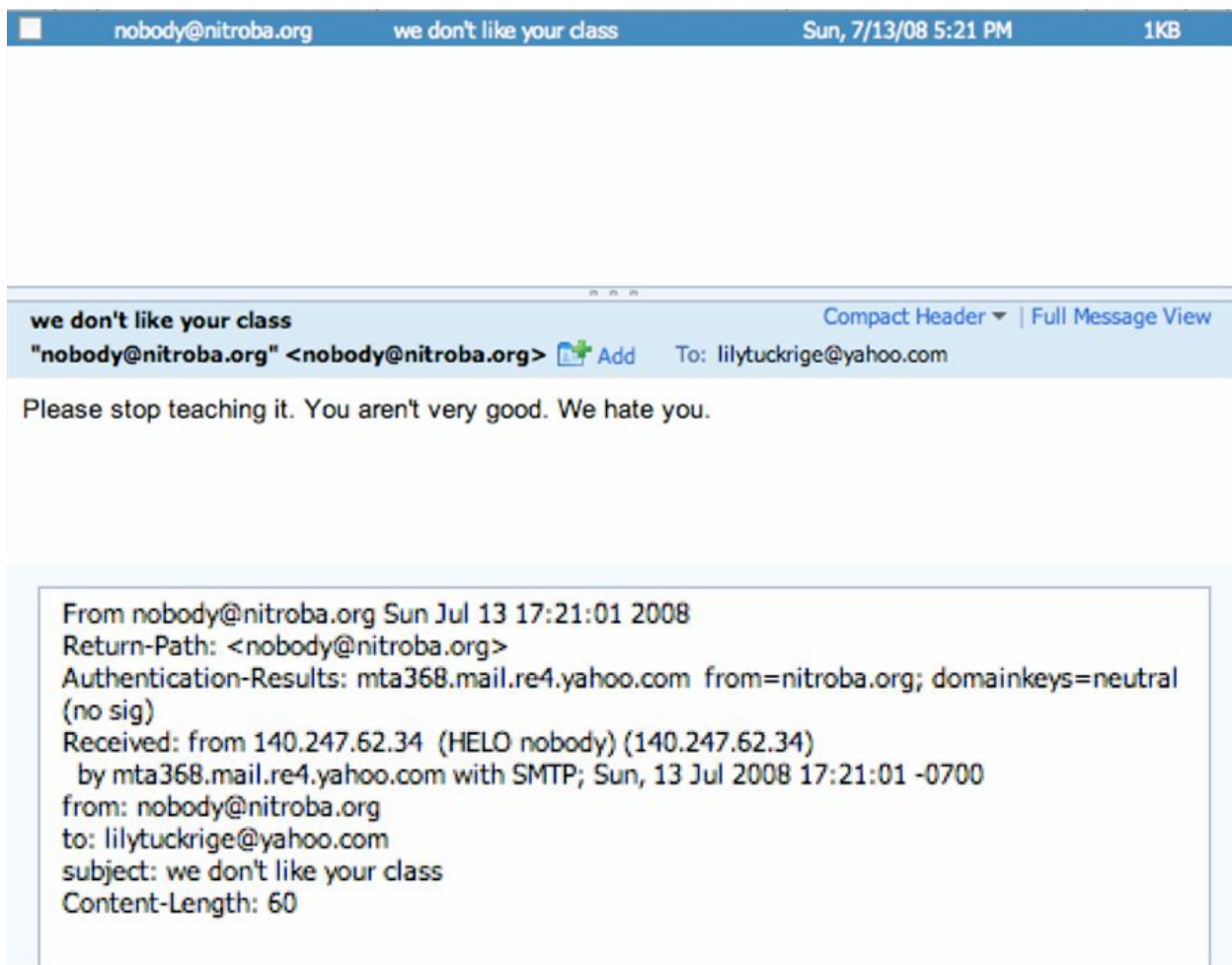
[Digital Corpora](#)

Nitroba case:

Lily Tuckrige

CHEM109 this summer at NSU

[lilytuckrige@yahoo.com](mailto:lilytuckrige@yahoo.com)



host 140.247.62.34

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

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

<input type="checkbox"/>	From	Subject	Date	Size
<input checked="" type="checkbox"/>	noreply@willselfdestruct.com	you can't find us	Mon, 7/21/08 11:04 PM	4KB
<input type="checkbox"/>	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**.

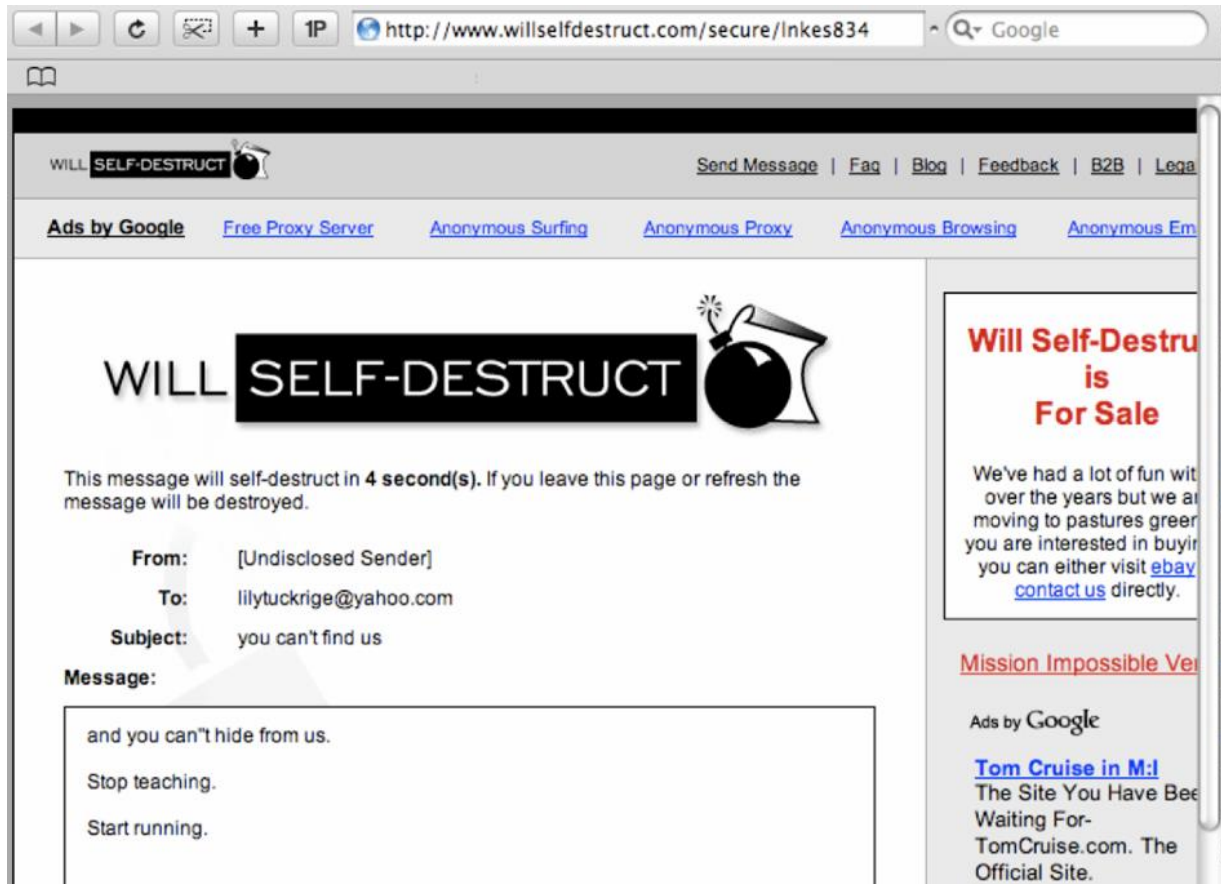
If you leave this page or refresh the page the message **will self-destruct**.

**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

No.	Time	Source	Destination	Proto	Length	Info
12768.417		192.168.15.4	140.247.62.34	T...	82	34526 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734633743 TSecr=0 SACK_PERM
12768.503		140.247.62.34	192.168.15.4	T...	78	8000 → 34526 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351651998 TSecr=734633743 WS=128
12768.504		192.168.15.4	140.247.62.34	T...	70	34526 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734633744 TSecr=351651998
12797.461		192.168.15.4	140.247.62.34	T...	82	34528 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634033 TSecr=0 SACK_PERM
12797.547		140.247.62.34	192.168.15.4	T...	78	8000 → 34528 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351681047 TSecr=734634033 WS=128
12797.548		192.168.15.4	140.247.62.34	T...	70	34528 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634034 TSecr=351681047
12799.171		192.168.15.4	140.247.62.34	T...	75	34528 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=65612 Len=5 TSval=734634051 TSecr=351681047
12799.258		140.247.62.34	192.168.15.4	T...	70	8000 → 34528 [ACK] Seq=1 Ack=6 Win=5888 Len=0 TSval=351682757 TSecr=734634051
12817.474		192.168.15.4	140.247.62.34	T...	70	34526 → 8000 [FIN, ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634233 TSecr=351651998
12817.560		140.247.62.34	192.168.15.4	T...	70	8000 → 34526 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351701063 TSecr=734634233
12823.804		140.247.62.34	192.168.15.4	T...	70	[TCP Retransmission] 8000 → 34526 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351707308 TSecr=734634233
12823.806		192.168.15.4	140.247.62.34	T...	82	34526 → 8000 [ACK] Seq=2 Ack=2 Win=65612 Len=0 TSval=734634297 TSecr=351707308
12827.113		192.168.15.4	140.247.62.34	T...	82	34544 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634330 TSecr=0 SACK_PERM
12827.198		140.247.62.34	192.168.15.4	T...	78	8000 → 34544 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351710703 TSecr=734634330 WS=128
12827.200		192.168.15.4	140.247.62.34	T...	70	34544 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634331 TSecr=351710703
12853.215		192.168.15.4	140.247.62.34	T...	82	34554 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634590 TSecr=0 SACK_PERM
12853.300		140.247.62.34	192.168.15.4	T...	78	8000 → 34554 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351736809 TSecr=734634590 WS=128

192.168.15.4 as source ip

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

```

File Data: 100 bytes
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "to" = "lilytuckrige@yahoo.com"
  ▶ Form item: "from" = ""
  ▶ Form item: "subject" = "you can't find us"
  ▶ Form item: "message" = "and you can't hide from us.\r\n\r\nStop teaching.\r\n"
  ▶ Form item: "type" = "0"
  ▶ Form item: "ttl" = "30"
  ▶ Form item: "submit.x" = "92"
  ▶ Form item: "submit.y" = "26"

▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "email" = "lilytuckrige@yahoo.com"
  ▶ Form item: "sender" = "the_whole_world_is_watching@nitroba.org"
  ▶ Form item: "subject" = "Your class stinks"
  ▶ Form item: "message" = "Why do you persist in teaching a boring class?\r\n\r\n"
  ▶ Form item: "security_code" = "xkpmkb"
  ▶ Form item: "submit" = "SEND!"

http://www.sendanonymousemail.net/\r\n

```

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

ip.addr == 192.168.15.4 and frame contains "lucky"

No.	Time	Source	Destination	Prot	Length	Info
15110.452	192.168.15.4	69.80.225.91	H..	844	POST /send.php HTTP/1.1 (application/x-www-form-urlencoded)	
15197.216	192.168.15.4	69.25.94.22	H..	719	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)	
15532.131	66.163.181.179	192.168.15.4	Y..	375	List V15 (status=Default) Status V15 (status=Default) Unknown Service: 239 (status=Server Ack) Ping (status=Serve..	

```

000  00 1d d9 2e 4f 60 00 17 f2 e2 c0 ce 08 00 45 00  ...O`...E
010  02 bd 02 ca 40 00 3f 06 c3 95 c0 a8 0f 04 45 19  ...@.?...E
020  5e 16 8c cc 00 50 fc 72 02 f0 75 b8 f4 26 80 18  ^...P.r..u.&..
030  fb 28 fa c7 00 00 01 01 08 0a 26 63 20 78 73 00  .(.....&c xs
040  cb 95 50 4f 53 54 20 2f 73 65 63 75 72 65 2f 73  .POST / secure/s
050  75 62 6d 69 74 20 48 54 54 50 2f 31 2e 31 0d 0a  ubmit HT TP/1.1
060  41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 67 69  Accept: image/gi
070  66 2c 20 69 6d 61 67 65 2f 78 2d 78 62 69 74 6d  f, image /x-xbitm
080  61 70 2c 20 69 6d 61 67 65 2f 6a 70 65 67 2c 20  ap, imag e/jpeg,
090  69 6d 61 67 65 2f 70 6a 70 65 67 2c 20 61 70 70  image/pj peg, app
0a0  6c 69 63 61 74 69 6f 6e 2f 78 2d 73 68 6f 63 6b  lication /x-shock
0b0  77 61 76 65 2d 66 6c 61 73 68 2c 20 2a 2f 2a 0d  wave-fla sh, */*
0c0  0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f  .Referer : http:/
0d0  2f 77 77 77 2e 77 69 6c 6c 73 65 6c 66 64 65 73  /www.wil lselfdes
0e0  74 72 75 63 74 2e 63 6f 6d 2f 73 65 63 75 72 65  truct.co m/secure
0f0  2f 73 75 62 6d 69 74 0d 0a 41 63 63 65 70 74 2d  /submit. Accept-
100  4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 0d  Language : en-us
110  0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61  .Content -Type: a

```

▼ Ethernet II, Src: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis\_2e:4f:60

- ▼ Destination: HonHaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)  
Address: HonHaiPrecis\_2e:4f:60 (00:1d:d9:2e:4f:60)  
.... ..0. .... = LG bit: Globally unique address (factory)
- .... ..0. .... = IG bit: Individual address (unicast)
- ▼ Source: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce)  
Address: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce)  
.... ..0. .... = LG bit: Globally unique address (factory)
- .... ..0. .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)  
Frame check sequence: 0x60c8d0a3 [unverified]  
[FCS Status: Unverified]  
File Data: 100 bytes

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- ▶ Form item: "to" = "lilytuckrige@yahoo.com"
- ▶ Form item: "from" = ""
- ▶ Form item: "subject" = "you can't find us"
- ▶ Form item: "message" = "and you can't hide from us.\r\n\r\nStop teaching.\r\n"
- ▶ Form item: "type" = "0"
- ▶ Form item: "ttl" = "30"
- ▶ Form item: "submit.x" = "92"
- ▶ Form item: "submit.y" = "26"

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)

No.	Time	Source	Destination	Proto	Length	Info
15019.913...	192.168.15.4	74.125.19.167	H..	874	GET	/pagead/ads?client=ca-pub-5181998329895443&dt=1216706511109&mt=1216706511&prev_slotnames=1960730875&output=html&...
15019.962...	192.168.15.4	69.80.225.91	H..	386	GET	/CaptchaSecurityImages.php?width=100&height=40&character=5 HTTP/1.1
15019.983...	192.168.15.4	67.15.76.53	H..	592	GET	/t.php?sc_project=2134460&resolution=1050&h=778&camefrom=http%3A//www.google.com/search%3Fhl%3Den%26%3Dsend+anon...
15020.388...	192.168.15.4	74.125.19.167	H..	887	GET	/pagead/ads?client=ca-pub-5181998329895443&dt=1216706511109&mt=1216706511&prev_slotnames=1960730875&2C1960730875...
15020.370...	192.168.15.4	74.125.19.167	H..	817	GET	/pagead/imgad?id=Cjv7w0jHmIDdaRDYBRhPMgg9tzYjhYMaZA HTTP/1.1
15020.985...	192.168.15.4	74.125.19.167	H..	870	GET	/pagead/sma6.js HTTP/1.1
15021.098...	192.168.15.4	74.125.19.167	H..	327	GET	/pagead/sma6.png HTTP/1.1
15058.467...	192.168.15.4	74.125.19.17	H..	120	POST	/mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D90313&RID=42253&zx=tqagaway3etz&i...
15110.452...	192.168.15.4	69.80.225.91	H..	844	POST	/send.php HTTP/1.1 (application/x-www-form-urlencoded)
15110.634...	192.168.15.4	74.125.19.167	H..	846	GET	/pagead/ads?client=ca-pub-5181998329895443&dt=1216706601828&mt=1216706601&format=728x90_as&output=html&correlato...
15110.658...	192.168.15.4	74.125.19.167	H..	866	GET	/pagead/ads?client=ca-pub-5181998329895443&dt=1216706601843&mt=1216706601&prev_fm=728x90_as&format=728x90_as&o...
15110.705...	192.168.15.4	67.15.76.53	H..	611	GET	/t.php?sc_project=2134460&resolution=1050&h=778&camefrom=http%3A//www.sendanonymousemail.net/&u=http%3A//www.send...
15111.064...	192.168.15.4	74.125.19.167	H..	827	GET	/pagead/imgad?id=CPz1xMba26TmSRDYBRhPMgg9Oa3UajWuA HTTP/1.1
15111.268...	192.168.15.4	74.125.19.167	H..	844	GET	/pagead/abglogo/abg-en-100c-000000.png HTTP/1.1
15111.271...	192.168.15.4	74.125.19.167	H..	350	GET	/pagead/abglogo/abg-en-100c-000000.png HTTP/1.1
15115.291...	192.168.15.4	74.125.19.17	H..	1405	GET	/mail/?ui=1&ik=0610eacbd&view=tl&search=inbox&start=0&ttl=11b495b9e1b&fp=ac6b2b37f9f9dc521&auto=1&vv=1&rq=xm&at=x...
15118.461...	192.168.15.4	74.125.19.17	H..	121	POST	/mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=10V80-3F5TD-67F8DC1634D90313&RID=42253&zx=tqagaway3etz&i...
14845.544...	192.168.15.4	12.129.210.41	H..	633	GET	/BurstingPipe/BurstingInteractionsPipe.aspx?interactionsStr=980608&Ead.yieldmanager.com/7E0K5EabAdDuration%7E12%7...
14845.565...	192.168.15.4	209.73.187.220	H..	1130	GET	/search/search_result; ylt=A9FJui40d4VIL5QANivD7BR.; ylv=3?pscan+I+go+to+jail+for+harassing+my+teacher%3F HTTP/1.1
14847.349...	192.168.15.4	69.22.167.248	H..	446	GET	/us.yimg.com/i/geo/advan/spacer.gif HTTP/1.1

I check for accounts by names

So I found google account and mail account

```

Cookie pair: S=gmail=L5hb7hHJ9B97n6StWA4FvA:gmail_yj=-OoenmU7qTeuQ1dsN3B1
Cookie pair: GMAIL_AT=xn3j32oktf2a0q6oa3k9sfr6d09yzf
Cookie pair: gmailchat=jcoachj@gmail.com/475090
Cookie pair: PREF=ID=8fc081df5e738a3c:TM=1210743469:LM=1216706486:GM=1:S=
Cookie pair: NID=13=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf7l-9JQ2AeoD8oWGS
Cookie pair: utmy=173272373-00000083192300028271-2:

```

[jcoachj@gmail.com](mailto:jcoachj@gmail.com)

that was Johnny Coach