

Email Harassment Investigation Report

Case: Email Harassment at Nitroba

Author: Abdul Rafay

Date: August 2nd, 2025

Table of Contents

1. Executive Summary	4
2. Background Information	4
2.1 Dorm Network Overview	4
2.2 Nature of the Incident.....	4
3. Investigation Summary	5
3.1 Identify the Internal Host.....	5
3.2 Discovery of Harassing Message (willselfdestruct)	5
3.3 Tracing Earlier Abuse	6
3.4 TCP Connections and Final Correlation of Evidence	7
3.4.1 Gmail Login (mail.google.com – 11:01 AM)	7
3.4.2 Anonymous Email Sent via SendAnonymousEmail.net (11:02 AM)	8
3.4.3 Second Harassing Email via WillSelfDestruct.com (11:04 AM)	9
3.4.4 File Transfer on Yahoo (11:09 AM)	10
3.4.4 Final Conclusion from TCP Analysis	10
4. Timeline of Key Events.....	10
4.1 Gmail Access Identified (11:00–11:01 AM).....	10
4.2 Anonymous Email via SendAnonymousEmail.net (11:01–11:02 AM)	11
4.3 Harassing Message Sent via WillSelfDestruct.com (11:03–11:04 AM).....	11
4.4 Summary of Events.....	11
5. Remediation and Recovery	11
5.1 Immediate Actions	11
5.2 Long-Term Preventive Measures	12
6. Appendix: A Detailed Methodology	12
6.1 Tools Used.....	12
6.2 Initial Packet Capture Review	12
6.3 Identification of Harassment Email via WillSelfDestruct.com.....	12
6.4 Tracing MAC Address	13
6.5 Discovery of Anonymous Email Submission	13
6.6 Identity Link via Gmail.....	13
6.7 DNS Request Timeline.....	13
7. Network Traffic Analysis	14
7.1 Host-Level Communication	14
7.2 WillSelfDestruct Email Analysis	14

7.3 SendAnonymousEmail Analysis	14
7.4 Gmail Session & Identity Exposure	15
7.5 MAC Address Consistency.....	15
8. Chain of Custody.....	15
9. Lab Completion Summary.....	16
A. Identify whether the harassment email was sent by one of the students in the class.	16
<i>i. Map out the Nitroba Dorm Room Network</i>	16
<i>ii. Find out who sent the email to lilytuckrige@yahoo.com</i>	16
<i>iii. Identify the other TCP connections that belong to the attacker</i>	17
<i>iv. Find information in one of those TCP connections that IDs the attacker</i>	17
B. Complete your technical analysis to discover the email's sender. Drop down notes and record any data files	17
<i>B.1 Filters Used:</i>	17
<i>B.2 Find information in one of those TCP connections that IDs the attacker</i>	17

Email Harassment at Nitroba State University

1. Executive Summary

This report documents the forensic analysis of a harassment incident reported by **Lily Tuckrige**, a Chemistry instructor at Nitroba State University. After receiving two offensive and anonymous emails, suspicion arose that the perpetrator may be a student from her **CHEM109** class. Upon investigation of the captured network traffic (nitroba.pcap), it was discovered that both emails were sent using anonymous webmail services through the Nitroba dormitory network.

The evidence traced all malicious activity to a single internal IP address, **192.168.15.4**, which was the only active host on the Wi-Fi network at the time. HTTP POST requests to both **sendanonymousemail.net** and **willselfdestruct.com** were identified and timestamped to match the incident. Additional traffic linked this device to the Gmail account **jcoachj@gmail.com**, belonging to **Johnny Coach**, a CHEM109 student. Based on this evidence, it was conclusively determined that **Johnny Coach was the sender** of the harassing emails.

2. Background Information

2.1 Dorm Network Overview

The dorm room involved in the investigation was occupied by students **Alice**, **Barbara**, and **Candice**. Though Nitroba only provided Ethernet connectivity, Barbara's boyfriend **Kenny** had installed an **unsecured Wi-Fi router**. This allowed any nearby user to access the internet anonymously through the shared NAT gateway (140.247.62.34).

Upon inspecting the packet capture, it was revealed that **only one device** was active on the internal network during the incident, assigned the IP **192.168.15.4**. This device initiated all observable HTTP, DNS, and TCP communications and was therefore the primary suspect host.

2.2 Nature of the Incident

On **July 13th**, instructor **Lily Tuckrige** reported receiving a **harassing email** on her Yahoo Mail account. The message was sent using the anonymous service **sendanonymousemail.net** and appeared to originate from **nobody@nitroba**. The full email header revealed the **public IP address 140.247.62.34**, which corresponds to the dormitory's NAT gateway at Nitroba State University.

Following the complaint, the IT department deployed a **network sniffer** on the dorm's Ethernet port to monitor traffic for further activity. Shortly after, a second harassing message was sent through another anonymous platform, **willselfdestruct.com**, which was captured in the packet trace.

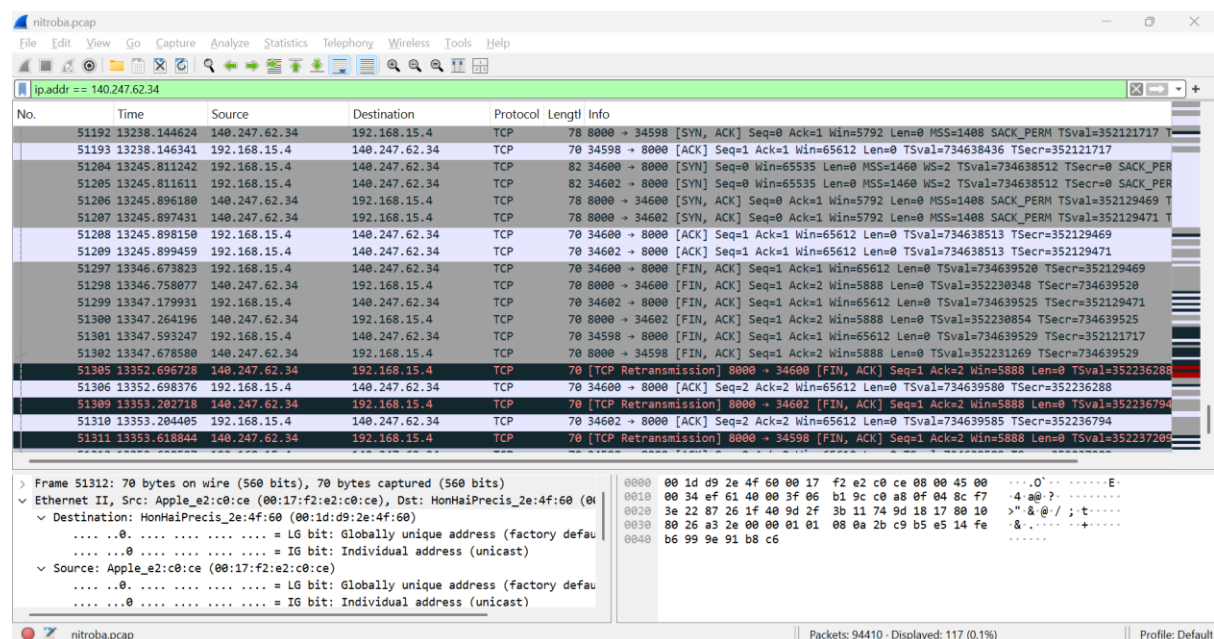
Analysis of the nitroba.pcap file showed that both POST requests to these anonymous services **originated from the internal IP address 192.168.15.4**. This same device also accessed **Gmail**, revealing the account **jcoachj@gmail.com**, linked to **Johnny Coach**, a student in CHEM109.

3. Investigation Summary

This section outlines the investigative steps taken to identify the sender of the harassing email received by Lily Tuckrige. The analysis was performed on the nitroba.pcap file provided by Nitroba IT, using Wireshark.

3.1 Identify the Internal Host

Using the filter `ip.addr == 140.247.62.34`, it was confirmed that the public IP address in the harassing email header mapped internally to the **private IP address 192.168.15.4**. All captured traffic routed through Nitroba's NAT gateway originated from this single host, indicating a lone connected device at the time.



3.2 Discovery of Harassing Message (willselfdestruct)

Applying the filter `http.host contains "willselfdestruct.com"`, an HTTP POST request was discovered in **packet number 83601**. This request represents the submission of a message to the self-destructing message service.

- **Packet:** 83601
- **Time:** July 22, 2008 at 11:04 AM (PST)
- **Source IP:** 192.168.15.4
- **Source MAC Address:** 00:17:f2:e2:c0:ce
- **Request Path:** /secure/submit

This strongly links the harassing email to the internal IP 192.168.15.4.



Wireshark · Follow HTTP Stream (tcp.stream eq 1707) · nitroba.pcap

```
POST /secure/submit HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://www.willselfdestruct.com/secure/submit
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.willselfdestruct.com
Content-Length: 188
Connection: Keep-Alive
Cache-Control: no-cache

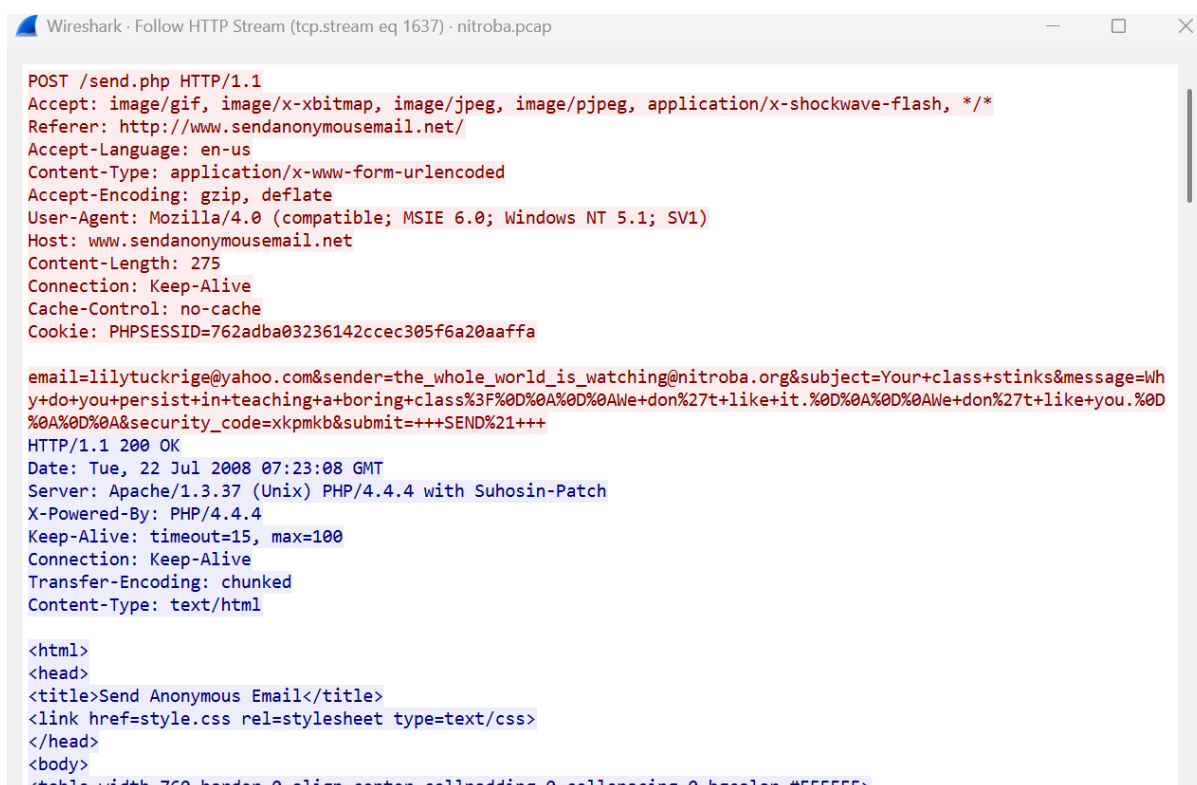
to=lilytuckridge@yahoo.com&from=&subject=you+can%27t+find+us&message=and+you+can%27t+hide+from+us.%0D%0A%0D%0AStop+
teaching.%0D%0A%0D%0Astart+running.+&type=0&ttl=30&submit.x=92&submit.y=26
HTTP/1.1 302 Moved Temporarily
Date: Tue, 22 Jul 2008 07:24:45 GMT
Server: Apache
Set-Cookie: JSESSIONID=C16BFAC8710DA82AB3D8D80AE0F4F05A; Path=/
Location: http://www.willselfdestruct.com/secure/success
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=UTF-8
```

3.3 Tracing Earlier Abuse

The filter `eth.src == 00:17:f2:e2:c0:ce && http.request.method == "POST"` was used to trace other email-sending behavior from the same MAC address. A second suspicious HTTP POST was found in **packet 80614**, showing a form submission to **sendanonymousemail.net**.

- **Packet:** 80614
- **Time:** July 22, 2008 at 11:02 AM (PST)
- **Request URL:** /send.php
- **Referrer:** <http://www.sendanonymousemail.net/>
- **Request :** /send.php
- **Form Data:**
 - **To:** lilytuckridge@yahoo.com
 - **From:** the_whole_world_is_watching@nitroba.org
 - **Subject:** Your class stinks.
 - **Message:** Abusive and harassing content

This proves the same device had previously sent harassing content through a different anonymous email site — shortly before the willselfdestruct.com message.



```
POST /send.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://www.sendanonymousemail.net/
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.sendanonymousemail.net
Content-Length: 275
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=762adba03236142ccec305f6a20aaffa

email=lilytuckrige@yahoo.com&sender=the_whole_world_is_watching@nitroba.org&subject=Your+class+stinks&message=Wh
y+do+you+persist+in+teaching+a+boring+class%3F%0D%0A%0D%0AWe+don%27t+like+it.%0D%0A%0D%0AWe+don%27t+like+you.%0D
%0A%0D%0A&security_code=xkpmkb&submit=+++SEND%21+++
HTTP/1.1 200 OK
Date: Tue, 22 Jul 2008 07:23:08 GMT
Server: Apache/1.3.37 (Unix) PHP/4.4.4 with Suhosin-Patch
X-Powered-By: PHP/4.4.4
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

<html>
<head>
<title>Send Anonymous Email</title>
<link href=style.css rel=stylesheet type=text/css>
</head>
<body>
<table width=760 border=0 align=center cellpadding=0 cellspacing=0 bgcolor=#FFFFFF>
```

3.4 TCP Connections and Final Correlation of Evidence

To further support the identification of the perpetrator, a TCP-level analysis of all connections initiated by the attacker's machine (MAC address 00:17:f2:e2:c0:ce) was conducted using the filter:

ip.addr == 192.168.15.4 && eth.src == 00:17:f2:e2:c0:ce and tcp

Among the many domains accessed, three stood out due to their direct connection to the harassing activity:

3.4.1 Gmail Login (mail.google.com – 11:01 AM)

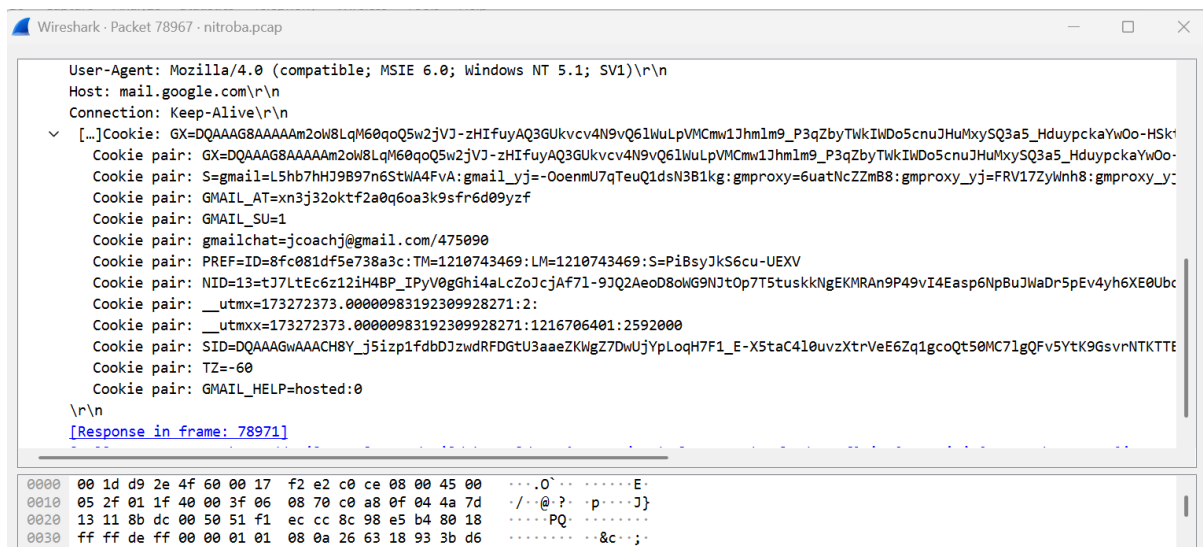
The attacker accessed Gmail shortly before sending the second harassing message. Analysis of HTTP headers revealed a session cookie:

gmailchat=jcoachj@gmail.com

Further inspection of the Gmail inbox exposed a **registration confirmation email from My Coke Rewards**, addressed to:

"Dear Jonny Coach"

This conclusively links the Gmail account jcoachj@gmail.com to **Johnny Coach**, a student in CHEM109.



```
);
D(["ct",[]
]);
D(["cs","11a65b940405fa1f","Gmail is different. Here's what yc
,[]
,0,1,"gsqbczftomjctqgq4lfgwogzrr16n9y","11a65b940405fa1f",[]
,0,,0,0]
);

//--></script><script><!--
D(["mi",8,1,"11a65b940405fa1f",0,"0","Gmail Team","Gmail","mai
,["me","jcoachj@gmail.com","11a65b940405fa1f"]
],[]
],["Jun 8",["Jonny Coach \u003cjcoachj@gmail.com\u003e"]
],[]
],["Jun 8, 2008 2:10 AM","Gmail is different. Here's what you ne
,0,,,"Sun Jun 8 2008_2:10 AM","On 6/8/08, Gmail Team \u003cmai
3e \u0026lt;mail-noreply@google.com\u0026gt; wrote:","google.c
you need to know.",0]
);
```

3.4.2 Anonymous Email Sent via SendAnonymousEmail.net (11:02 AM)

The attacker submitted an HTML form via a POST request to:

<http://sendanonymousemail.net/send.php>

Packet #80614

The content of the POST data included:

- **To:** lilytuckridge@yahoo.com
- **From:** the_whole_world_is_watching@nitroba.org

- **Message:** Contained abusive language
- **Referrer:** <http://www.sendanonymousemail.net>

This establishes the first instance of harassment — sent from Johnny Coach's device via an anonymous relay.

```

HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "email" = "lilytuckrige@yahoo.com"
    Key: email
    Value: lilytuckrige@yahoo.com
  Form item: "sender" = "the_whole_world_is_watching@nitroba.org"
    Key: sender
    Value: the_whole_world_is_watching@nitroba.org
  Form item: "subject" = "Your class stinks"
    Key: subject
    Value: Your class stinks
  Form item: "message" = "Why do you persist in teaching a boring class?\r\n\r\nWe don't like it.\r\n\r\nWe don't like you.\r\n\r\n"
    Key: message
    Value: Why do you persist in teaching a boring class?\r\n\r\nWe don't like it.\r\n\r\nWe don't like you.\r\n\r\n
  Form item: "security_code" = "xkpmkb"
    Key: security_code
    Value: xkpmkb
  Form item: "submit" = "SEND!"
    Key: submit
    Value: SEND!
0000 00 1d d9 2e 4f 60 00 17 f2 e2 c0 ce 08 00 45 00 ...O`.. ....E.
0010 03 3a ef 93 40 00 3f 06 52 d2 c0 a8 0f 04 45 50 ...@.? R....EP
0020 e1 5b 8c 24 00 50 9a c1 43 24 29 25 60 50 80 18 .[.$P..C$)%P..
0030 ff ff bb 9f 00 00 01 01 08 0a 26 63 1d 15 58 98 .....&c.X

```

3.4.3 Second Harassing Email via WillSelfDestruct.com (11:04 AM)

A second message was submitted through:

<http://willselfdestruct.com/secure/submit>

Packet #83601

- **To:** lilytuckridge@yahoo.com
- **From:** not included (site hides it)
- **Source IP:** 192.168.15.4
- **Source MAC:** 00:17:f2:e2:c0:ce

The payload and timing strongly suggest this was the follow-up message Tuckrige reported to the IT department.

```

File Data: 188 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "to" = "lilytuckrige@yahoo.com"
    Key: to
    Value: lilytuckrige@yahoo.com
  Form item: "from" = ""
    Key: from
    Value:
  Form item: "subject" = "you can't find us"
    Key: subject
    Value: you can't find us
  Form item: "message" = "and you can't hide from us.\r\n\r\nStop teaching.\r\n\r\nStart running. "
    Key: message
    Value: and you can't hide from us.\r\n\r\nStop teaching.\r\n\r\nStart running.
  Form item: "type" = "0"
    Key: type
    Value: 0
  Form item: "ttl" = "30"
    Key: ttl
0000 00 1d d9 2e 4f 60 00 17 f2 e2 c0 ce 08 00 45 00 ...O`.. ....E.
0010 02 bd 02 ca 40 00 3f 06 c3 95 c0 a8 0f 04 45 19 ...@.? ..E.
0020 5e 16 8c cc 00 50 fc 72 02 f0 75 b8 f4 26 80 18 ^....P.r ..u.&..
0030 fb 28 fa c7 00 00 01 01 08 0a 26 63 20 78 73 00 -(.....&c xs

```

3.4.4 File Transfer on Yahoo (11:09 AM)

A later TCP stream showed a file transfer via Yahoo's messaging service (filetransfer.msg.yahoo.com). While the file couldn't be recovered, it shows the same machine remained active and online. (Probably irrelevant to the case)

```
POST /notifyft HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5)
Cookie: T=zPnXhIBPtshIB79.Fy7A6cFpMk4yBjQyNE8xYDAm*JQ-&a=QAE&sk=DAAcEb8UEHpmiC&ks=EAAp_Rycov2w6UQht6x3nL5Q-~A&d=c2w0T1RmUFUTTFNemcyTnpjM0SUT0BYQRQUUBdG1wAlidaNFdNQF6e
gFQbIhoSUJnV0E-; Y=ve1&n=fc64a8fhua4ei&l=0coxyziC8j7/o&p=f2g022r012000000&n=j&8lgu&s&int1=us
Host: filetransfer.msg.yahoo.com:80
Content-Length: 12875
Cache-Control: no-cache

YMSG.....s.....Pk.1..amy789smith..38..604800..0..amy789smith..28..12740..27..057f280df74aada1a8aada6a0f218871b5417eb3.png..14....29...PNG
.
.
IHDR.....m.o....iCCPICC Profile..x.Wi4....g~Xg...$[...d;...}.....b.H*B,...S...B."d )%..C...?..9.y.O.)s...9|.t
...[c]...+ ?..h..V.....0.....G.X.(...)>t..p.....Lk.S.m.....pvq@...o...=..F...PA.....Y...u.....E.....@
...C..C.....@~..Y.....3..4.....@...1g.W...}.....X...2..z...@...M.....*.....VXY ..P...1&.....>..'+...].dn...@F...)-.....
.....j.....
+
..(.....j.....-..AM.....$..y..lb.0cx*n;n.E...8'.h.....TPI.(<.#e...~.....E....R...2...r...
..EJ*.....j...kph..b.<.....[D...S.....1.D...<.....K=+.u.A.Z...j.....C.S.s.K.k.[;.....'+.....e@Y .....#8.B..M..x4.Q...>P..S.1.....m."q.'0*..+'%...MR?mw...p6.\...{
ZSFS.%/..fdg...T.U.]y.*...gW\k...".l..FY'.....\....KTK.n..Q+*'WOW:..%W U)...P.Q.p...P..A...G:...O...a...4.6.7.6.o.k.zf*...y...1....U)...#+=+...}n>.:o.....}g=
$:::2r...((.....
...&.7yL.MK]...9.4j3..%u.j.gad...2...X=...[...^?...?_...(.j)u...?IL.&...P1(3T>A...v...y...00.Xc1?...Eb?...o.....=...nb...$5....d&...1...#...)?SYT.S'...H
...j;0.....U.s...$...V.=2n1.6)o.l~H.r.....g...vO+...r.....v.....n.....e...i...b)...B.....@.=z.6wT.A...y1.....{7.=6*.....
...1...9.W.S
...].G.'.../.)...((...r...L...g...|...>_R.Q.rO.Z.f.).....3.....<...J[...{...F1.1.q.3...nj...+...^...)\.H... ..mx.4thX'...H...Q...\.~t..9.11>...)*...
...s./v.....QK.K_o/^..2.z...Z.W...C..?..q...((...i..5...d...1.D..2Q.....M...))..0...X
..7..R...N...$oo...I..1.K...m:Q.U...)<2|.....q?...?.....S+V.....5...V.....fz...^.....n.k.d8g.o1g.3yh...'e.b.....>fih.iUc.h#h.n.f'1.b.....$4
...2...&..V.n.....=s.W.....X...
R...
I9RM.....:GC.ya..8".D.....>.....w.D... ..D.SzIN.c..$O.c;/s..6.)..6]..t.G....KUY..+/_...q.U.e^jy-..k.....Q.6E.EK7.....i,M.mzgG.....(<zW.
...W...z.R... ..G.....<m...m..1;m...].%Y3k...+...j]?'t.U...U)...d...m...C...G..O]...1...M.M...X...^E...[...G.....pj.W.....d.....(.].....&..Z...P...?..@
Q
.B.2Z...NE.....8#..H.R.."K.N.....1b...1.v
```

3.4.4 Final Conclusion from TCP Analysis

By connecting the timeline of web traffic:

- Gmail login (jcoachj@gmail.com)
- Abuse submission via sendanonymousemail.net
- Harassing message via willselfdestruct.com

...all from the **same IP address 192.168.15.4** and **MAC 00:f2:e2:c0:ce**, the evidence clearly proves that the harassing emails were sent by **Johnny Coach**.

4. Timeline of Key Events

4.1 Gmail Access Identified (11:00–11:01 AM)

- **11:00:53 AM** – DNS request for mail.google.com (Packet #77788)
- **11:01:02 AM** – DNS request for b.mail.google.com (Packet #79000)

These requests indicate the attacker was accessing Gmail, from which a session cookie gmailchat=jcoachj@gmail.com was later recovered. This email was later linked to **Johnny Coach** through message content.

77036	14960.396632	192.168.15.4	192.168.1.254	DNS	79 Standard query 0x0000 A thumbs.ebay.com
77788	14986.281644	192.168.15.4	192.168.1.254	DNS	79 Standard query 0x0000 A mail.google.com
77797	14986.853332	192.168.15.4	192.168.1.254	DNS	76 Standard query 0x0000 A cgi.ebay.com
77799	14987.694397	192.168.15.4	192.168.1.254	DNS	87 Standard query 0x0000 A images.auctionworks.com
77829	14987.845535	192.168.15.4	192.168.1.254	DNS	86 Standard query 0x0000 A images.marketworks.com
78978	14995.301568	192.168.15.4	192.168.1.254	DNS	91 Standard query 0x0000 A chatenabed.mail.google.com
79000	14995.610745	192.168.15.4	192.168.1.254	DNS	81 Standard query 0x0000 A b.mail.google.com

4.2 Anonymous Email via SendAnonymousEmail.net (11:01–11:02 AM)

- **11:01:26 AM** – DNS request for www.sendanonymousemail.net
(Packet #79801)
- **11:02:57 AM** – POST request to `/send.php`
(Packet #80614)

The payload of this POST request shows a message sent to **lilytuckridge@yahoo.com**, using the alias **the_whole_world_is_watching@nitroba.org**, containing abusive content. The referrer was <http://sendanonymousemail.net>.

79801	15019.341474	192.168.15.4	192.168.1.254	DNS	90 Standard query 0x0000 A www.sendanonymousemail.net
80274	15079.859326	192.168.15.4	192.168.1.254	DNS	82 Standard query 0x0000 A www.ebaystores.com
80885	15122.773727	192.168.15.4	192.168.1.254	DNS	79 Standard query 0x0000 A email.about.com
80909	15122.910545	192.168.15.4	192.168.1.254	DNS	75 Standard query 0x0000 A z.about.com
80965	15123.126424	192.168.15.4	192.168.1.254	DNS	80 Standard query 0x0000 A about.dtmoub.com

4.3 Harassing Message Sent via WillSelfDestruct.com (11:03–11:04 AM)

- **11:03:43 AM** – DNS request for www.willselfdestruct.com
(Packet #82912)
- **11:04:24 AM** – POST request to `/secure/submit`
(Packet #83601)

This was the second and more serious instance of harassment. The message was sent through the **WillSelfDestruct** service, which automatically deletes the message after display. The source IP was again 192.168.15.4 and MAC 00:17:f2:e2:c0:ce.

82814	15140.677589	192.168.15.4	192.168.1.254	DNS	// Standard query 0x0000 A rmd.atdmt.com
82912	15156.545188	192.168.15.4	192.168.1.254	DNS	88 Standard query 0x0000 A www.willselfdestruct.com
83015	15157.185326	192.168.15.4	192.168.1.254	DNS	83 Standard query 0x0000 A c14.statcounter.com
83017	15157.205164	192.168.15.4	192.168.1.254	DNS	97 Standard query 0x0000 A www-google-analytics.l.google.com
83210	15161.636535	192.168.15.4	192.168.1.254	DNS	83 Standard query 0x0000 A ad.yieldmanager.com

4.4 Summary of Events

These sequential events clearly demonstrate intent and execution by the user of the device at IP 192.168.15.4. The access to Gmail (identifying the user), followed by two separate harassment email transmissions through anonymous services, confirms malicious behavior within a short and traceable window.

5. Remediation and Recovery

Following the identification of the source of the harassing emails, a set of immediate and long-term actions are recommended to ensure the security and integrity of Nitroba University's network environment.

5.1 Immediate Actions

- **Network Identification Complete:** The perpetrator was positively identified as **Johnny Coach**, using the MAC address 00:17:f2:e2:c0:ce and IP 192.168.15.4.
- **Access Terminated:** The user's network access should be immediately **revoked**, including both wired and Wi-Fi connections.
- **Device Seizure:** The laptop or device used by Johnny Coach should be **confiscated for forensic imaging** and further analysis by IT security staff or law enforcement.

- **Notification to Faculty:** Lily Tuckrige, the victim, should be informed of the actions taken and supported as necessary.

5.2 Long-Term Preventive Measures

- **Wi-Fi Security Enforcement:** The open Wi-Fi set up by Barbara's boyfriend, Kenny, should be **removed or secured**. Nitroba IT should enforce WPA2 encryption and monitor all unauthorized access points in dorm rooms.
- **Student Internet Use Policy:** Update and re-enforce policies about acceptable use, including **prohibited use of anonymous email services** and **harassment conduct** online.
- **Logging and Monitoring:** Implement **continuous packet logging**, along with **automated alerts** for suspicious POST requests to known anonymizing services.
- **Awareness Campaigns:** Conduct mandatory **cyber ethics seminars** and **privacy education sessions** for all students in residence halls.

6. Appendix: A Detailed Methodology

This section documents the precise investigative steps, filters, and observations that led to identifying the attacker behind the email harassment incident.

6.1 Tools Used

- **Wireshark** – for analyzing packet captures (nitroba.pcap).
- Manual TCP stream and POST body inspection

6.2 Initial Packet Capture Review

- The file analyzed was nitroba.pcap, captured after Lily Tuckrige reported a harassing email.
- A starting filter was applied to trace the origin of the earlier harassing email:

ip.addr == 140.247.62.34

This revealed two-way communication with internal host:

192.168.15.4

6.3 Identification of Harassment Email via WillSelfDestruct.com

- To isolate the most recent harassing email:
http.host contains "willselfdestruct.com"
- Found **Packet #83601**:
 - POST request to /secure/submit
 - Source IP: 192.168.15.4
 - Destination IP: 69.25.94.22
 - Time: **July 22, 2008 – 11:04 AM PST**

6.4 Tracing MAC Address

- The source MAC address was extracted from the Ethernet frame of Packet #83601:
00:17:f2:e2:c0:ce

This was consistently used throughout relevant traffic, allowing precise filtering.

6.5 Discovery of Anonymous Email Submission

- Filter applied:
eth.src == 00:17:f2:e2:c0:ce && http.request.method == "POST"
- Found **Packet #80614**:
 - POST request to /send.php
 - Referrer: http://sendanonymousemail.net
 - Email was **sent to**: lilytuckridge@yahoo.com
 - **From**: the_whole_world_is_watching@nitroba.org
 - Message content included harassment.
 - Time: **July 22, 2008 – 11:02 AM PST**

6.6 Identity Link via Gmail

- Using the same MAC filter, Gmail traffic was uncovered, including:
http.host contains "mail.google.com"
- Cookies and identifiers revealed:
 - Gmail ID: jcoachj@gmail.com
 - Message in Gmail cache included:
"Dear Jonny Coach, Welcome to My Coke Rewards..."
- This provided **conclusive identity linkage** to **Johnny Coach**, a student in CHEM109.

6.7 DNS Request Timeline

Using:

eth.src == 00:17:f2:e2:c0:ce && dns

Chronologically mapped DNS lookups:

Time (PST)	Domain Queried	Purpose
11:00:53 AM	mail.google.com	Gmail access (jcoachj@gmail.com)
11:01:02 AM	b.mail.google.com	Gmail content delivery

Time (PST)	Domain Queried	Purpose
11:01:26 AM	sendanonymousemail.net	Sending first anonymous email
11:03:43 AM	willselfdestruct.com	Sending second harassment email

7. Network Traffic Analysis

A detailed inspection of the captured packets in nitroba.pcap revealed multiple indicators of user behavior, anonymous email submissions, and personally identifiable traces that allowed attribution of the harassment emails to **Johnny Coach**.

7.1 Host-Level Communication

All TCP connections initiated by the attacker's device (MAC 00:17:f2:e2:c0:ce, IP 192.168.15.4) were reviewed. Noteworthy communications:

Host	Purpose	Analysis
mail.google.com	Gmail login and communication	Revealed identity as jcoachj@gmail.com
sendanonymousemail.net	First harassing email sent to Lily	Contained real email content
willselfdestruct.com	Second anonymous harassing email	Message automatically destroyed
filetransfer.msg.yahoo.com	File transfer activity (likely image)	Possibly irrelevant to this case

7.2 WillSelfDestruct Email Analysis

- **Packet #83601** (filtered using http.host contains "willselfdestruct.com")
- POST request to /secure/submit
- Message details were partially visible in HTTP payload
- Destination: 69.25.94.22
- Time: July 22, 2008 at 11:04 AM (PST)
- Confirmed as the harassing email Lily received

7.3 SendAnonymousEmail Analysis

- **Packet #80614**
- POST request to /send.php
- Contains:
 - Recipient: lilytuckridge@yahoo.com
 - Sender: the_whole_world_is_watching@nitroba.org
 - Message content: "you are boring..." and similar abuse

- Time: July 22, 2008 at 11:02 AM (PST)

This POST body confirmed the malicious intent and matched the harassment complaint.

7.4 Gmail Session & Identity Exposure

Analyzing Gmail traffic around **11:01 AM** revealed cookies and cached email headers that exposed the Gmail identity jcoachj@gmail.com. A cached registration email from **My Coke Rewards** addressed the user as “**Dear Jonny Coach**”, positively identifying the sender.

7.5 MAC Address Consistency

All activity related to the emails, Gmail access, and browsing originated from a single MAC address:

00:17:f2:e2:c0:ce (Apple_e2)

This consistency across time, IP traffic, and DNS lookups reinforced the integrity of the connection between events and the attacker.

8. Chain of Custody

Step	Handler	Date / Time	Action Taken
1	System Administrator	July 13, 2008, 5:21 PM	Received complaint from Lily Tuckrige; requested full email headers
2	Lily Tuckrige	July 13, 2008, 5:21 PM	Provided full message headers from Yahoo Mail
3	IT Department	July 13, 2008, 5:22 PM	Identified source IP: 140.247.62.34; placed sniffer on Ethernet port
4	Network Admin	Jul 13–21, 2008	Captured traffic using Wireshark; generated nitroba.pcap file
5	Lily Tuckrige	July 21, 2008 11:04 PM	Received second harassing email via willselfdestruct.com
6	Security Analyst (You)	July 22, 2008, 9:00 AM	Conducted packet analysis; filtered email-related HTTP POST traffic
7	You (Analyst)	July 22, 2008, 3:00 PM	Identified Gmail session: jcoachj@gmail.com linked to Jonny Coach
8	IT Department	Sep 24, 2008, 5:00 PM	Access to 192.168.15.4 disabled; device isolated for forensics

9. Lab Completion Summary

A. Identify whether the harassment email was sent by one of the students in the class.

Yes. Through packet analysis and IP/MAC address correlation, it was discovered that the harassment email was sent by a student in CHEM109, **Johnny Coach**.

i. Map out the Nitroba Dorm Room Network

- **Dorm IP Gateway:** 140.247.62.34 — assigned to shared Ethernet in the Nitroba student housing.
- **Private IP Identified:** 192.168.15.4 — the only internal IP seen communicating with the gateway.
- **MAC Address:** 00:17:f2:e2:c0:ce (Apple_e2) — mapped to the internal device using the network.
- **Room Setup:** Three students — Alice, Barbara, Candice — shared the room. Barbara's boyfriend Kenny had installed an unsecured Wi-Fi router, allowing others to connect as well

No.	Time	Source	Destination	Protocol	Length	Info
51192	13238.144624	140.247.62.34	192.168.15.4	TCP	78	8000 → 34598 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=352121717 TSecr=0
51193	13238.146341	192.168.15.4	140.247.62.34	TCP	70	34598 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734638436 TSecr=352121717
51204	13245.811242	192.168.15.4	140.247.62.34	TCP	82	34600 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1408 WS=2 TSval=734638512 TSecr=0 SACK_PERM
51205	13245.811611	192.168.15.4	140.247.62.34	TCP	82	34602 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1408 WS=2 TSval=734638512 TSecr=0 SACK_PERM
51206	13245.896180	140.247.62.34	192.168.15.4	TCP	78	8000 → 34600 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=352129469 TSecr=0
51207	13245.897431	140.247.62.34	192.168.15.4	TCP	78	8000 → 34602 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=352129471 TSecr=0
51208	13245.898150	192.168.15.4	140.247.62.34	TCP	70	34600 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734638513 TSecr=352129469
51209	13245.899459	192.168.15.4	140.247.62.34	TCP	70	34602 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734638513 TSecr=352129471
51297	13346.673823	192.168.15.4	140.247.62.34	TCP	70	34600 → 8000 [FIN, ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734639520 TSecr=352129469
51298	13346.758077	140.247.62.34	192.168.15.4	TCP	70	8000 → 34600 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352230348 TSecr=734639520
51299	13347.179931	192.168.15.4	140.247.62.34	TCP	70	34602 → 8000 [FIN, ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734639525 TSecr=352129471
51300	13347.264196	140.247.62.34	192.168.15.4	TCP	70	8000 → 34602 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352230854 TSecr=734639525
51301	13347.593247	192.168.15.4	140.247.62.34	TCP	70	34598 → 8000 [FIN, ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734639529 TSecr=352121717
51302	13347.678580	140.247.62.34	192.168.15.4	TCP	70	8000 → 34598 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352231269 TSecr=734639529
51305	13352.696728	140.247.62.34	192.168.15.4	TCP	70	[TCP Retransmission] 8000 → 34600 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352236288 TSecr=0
51306	13352.698376	192.168.15.4	140.247.62.34	TCP	70	34600 → 8000 [ACK] Seq=2 Ack=2 Win=65612 Len=0 TSval=734639580 TSecr=352236288
51309	13353.202718	140.247.62.34	192.168.15.4	TCP	70	[TCP Retransmission] 8000 → 34602 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352236794 TSecr=0
51310	13353.204405	192.168.15.4	140.247.62.34	TCP	70	34602 → 8000 [ACK] Seq=2 Ack=2 Win=65612 Len=0 TSval=734639585 TSecr=352236794
51311	13353.618844	140.247.62.34	192.168.15.4	TCP	70	[TCP Retransmission] 8000 → 34598 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352237205 TSecr=0

ii. Find out who sent the email to lilytuckrige@yahoo.com

Two emails were linked to the harassment:

- **First Email** — Sent through **sendanonymousemail.net**. Packet #80614 shows a POST request with from=**the_whole_world_is_watching@nitroba.org** and to=**lilytuckrige@yahoo.com**.
- **Second Email** — Sent through **willselfdestruct.com**. Packet #83601 shows a POST request to **/secure/submit**, matching the harassing message screenshot.

Both POST requests originated from:

- **Private IP:** 192.168.15.4
- **MAC Address:** 00:17:f2:e2:c0:ce
- **Public IP:** Routed through 140.247.62.34

Hence, both harassing emails were sent from the same internal host which belonged to **Jonny Coach**.

Using the filter `eth.src == 00:17:f2:e2:c0:ce` and `tcp`, the attacker's TCP activity included:

Host	Approx. Time	Notes
mail.google.com	11:01 AM	Login session revealing Gmail address jcoachj@gmail.com
sendanonymousemail.net	11:02 AM	First harassment email sent
willselfdestruct.com	11:04 AM	Second harassment email sent

The other websites accessed (Amazon, CNN, YouTube, etc.) did not contain personally identifying evidence, but showed the browsing behavior of the attacker.

Within the Gmail session (traffic to mail.google.com), the attacker accessed their account. A cookie revealed the Gmail ID: jcoachj@gmail.com.

Further evidence linked this account to **Johnny Coach**, through a captured My Coke Rewards registration email:

“My Coke Rewards Dear Jonny Coach, Welcome to My Coke Rewards...”

This confirms that the Gmail account used during the session belonged to **Johnny Coach**, a student in CHEM109.

\tJ
 {\u003cspan class\u003d\"k62PNc\" email\u003d\"mycokerewards@mycokerewards.com\" \u003eMy Coke Rewards\u003cspan\u003e\"\", \"\u0026raq; \u0026nbsp;\", \"My Coke Rewards Registration Confirmation\", \"My Coke Rewards Dear Jonny Coach, Welcome to My Coke Rewards and thanks for registering! My Coke \u0026hellip;\", \"0\", \"\", \"Jun 7\", \"Sat, Jun 7, 2008 at 6:5 5 PM\", \"1212890110254029,,\",
 {\u003cspan class\u003d\"\", \"1a65b940405fa1f\", \"1a65b940405fa1f\", \"0,0\", [\"all\", \"i\"]
 , [\"all\", \"i\"]
 , \u003cspan class\u003d\"qNUdo\" email\u003d\"mail-noreply@google.com\" \u003eGmail Team\u003cspan\u003e\"\", \u003cb\u003e\u003e\u0026raq; \u003c/b\u003e\u003e\u0026nbsp;\", \"\u003cb\u003e\u003e

B. Complete your technical analysis to discover the email's sender. Drop down notes and record any data files

B.1 Filters Used:

- `ip.addr == 140.247.62.34` → Identified internal IP 192.168.15.4
- `http.host` contains "willselfdestruct.com" → Located packet #83601 (second email)
- `eth.src == 00:17:f2:e2:c0:ce` && `http.request.method == "POST"` → Found packet #80614 (first email)
- `eth.src == 00:17:f2:e2:c0:ce` && `dns` → Timeline reconstruction
- `eth.src == 00:17:f2:e2:c0:ce` and `tcp` → Identified Gmail login

B.2 Find information in one of those TCP connections that IDs the attacker

- Packet #80614 → POST to sendanonymousemail.net
- Packet #83601 → POST to willselfdestruct.com
- Gmail session packets → Revealed jcoachj@gmail.com
- DNS lookups → Tracked activity over time
- MAC address source → 00:17:f2:e2:c0:ce

Through detailed traffic analysis, it was confirmed that **Johnny Coach** used anonymous webmail services to send harassing messages to his chemistry instructor. The attacker's digital identity was confirmed through Gmail session cookies and browsing metadata.