

Digital Forensics Homework

Johnny Coach is the one that who sent the email.

Using the NetworkMiner we can see that the email is sent from the IP adress 192.168.15.4 from an Apple iOS device.

Hosts (747)Files (4301)Images (2349)Messages (2)Credentials (810)Sessions (2108)DNS (2560)Parameters (99012)KeywordsAnomalies

Filter keyword: ☐ Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
83601	192.168.15.4 (Apple_iOS)	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.co...]		lilytuckrige@yahoo.com	you can't find us	Http	2008-07-22 06:00
80614	192.168.15.4 (Apple_iOS)	69.80.225.91 [www.sendanonymousemail.net]	lilytuckrige@yahoo.com		Your class stinks	Http	2008-07-22 06:00

Attribute	Value
email	lilytuckrige@yahoo.com
sender	the_whole_world_is_watching@nitr
subject	Your class stinks
message	Why do you persist in teaching a bc
security code	xknmkh

Windows-1252 Western European (Windows)

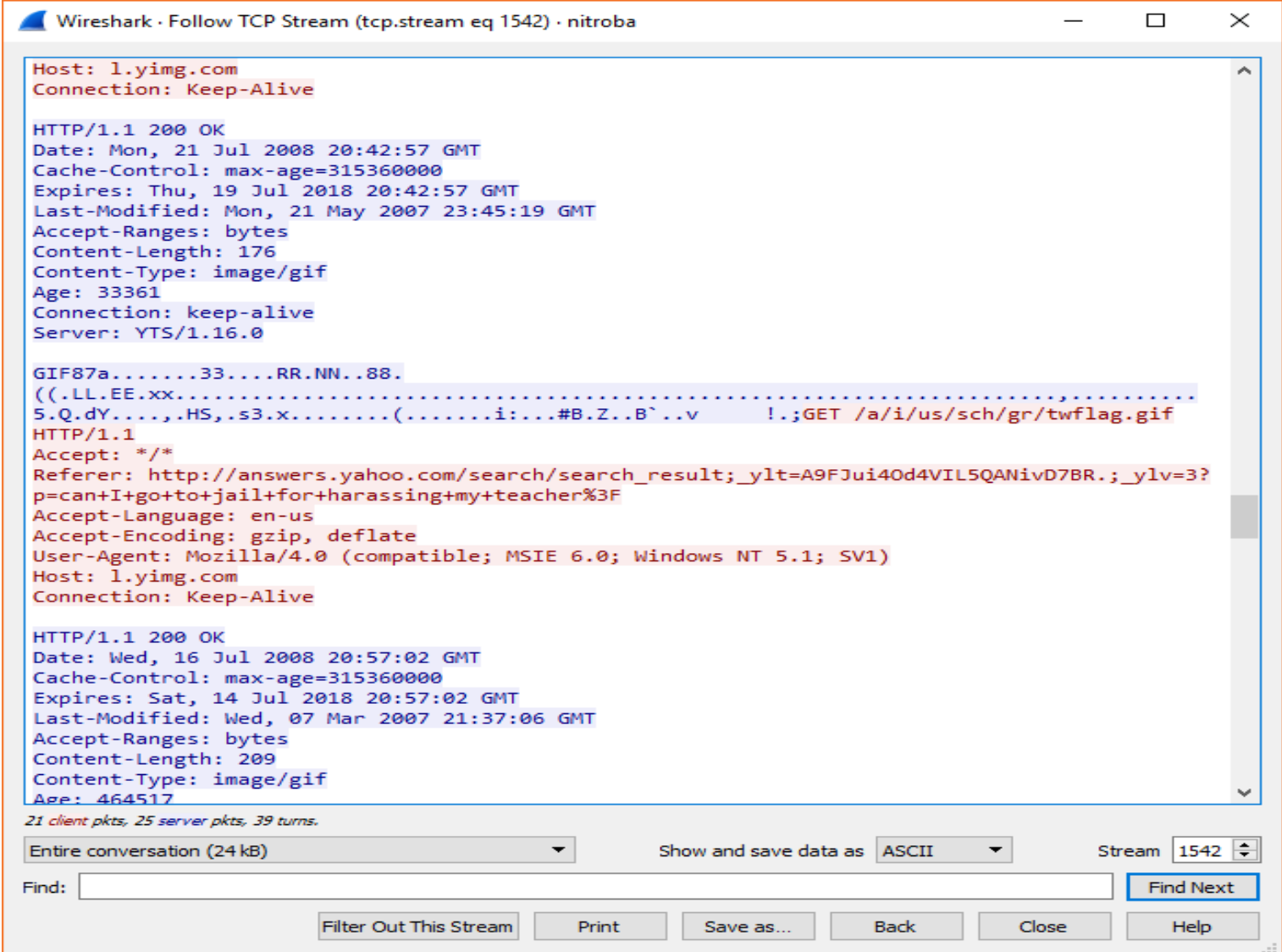
Why do you persist in teaching a boring class?

We don't like it.

We don't like you.

Attachement	Size
-------------	------

By tracing this IP address on the given pcap file using Wireshark and following some of the TCP flows we can see that this person searched for “Can I go to jail for harassing my teacher?” on yahoo search:



Wireshark · Follow TCP Stream (tcp.stream eq 1542) · nitroba

Host: 1.yimg.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 21 Jul 2008 20:42:57 GMT
Cache-Control: max-age=315360000
Expires: Thu, 19 Jul 2018 20:42:57 GMT
Last-Modified: Mon, 21 May 2007 23:45:19 GMT
Accept-Ranges: bytes
Content-Length: 176
Content-Type: image/gif
Age: 33361
Connection: keep-alive
Server: YTS/1.16.0

GIF87a.....33....RR.NN..88.
((.LL.EE.xx.....
5.Q.dY.....,HS,.s3.x.....(.....i:..#B.Z..B`..v !.;GET /a/i/us/sch/gr/twflag.gif
HTTP/1.1
Accept: */*
Referer: http://answers.yahoo.com/search/search_result;_ylt=A9FJui40d4VIL5QANivD7BR.;_ylv=3?
p=can+I+go+to+jail+for+harassing+my+teacher%3F
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 1.yimg.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 16 Jul 2008 20:57:02 GMT
Cache-Control: max-age=315360000
Expires: Sat, 14 Jul 2018 20:57:02 GMT
Last-Modified: Wed, 07 Mar 2007 21:37:06 GMT
Accept-Ranges: bytes
Content-Length: 209
Content-Type: image/gif
Age: 464517

21 client pkts, 25 server pkts, 39 turns.

Entire conversation (24 kB) Show and save data as ASCII Stream 1542

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

On another TCP flow where destination IP address points to google chats we see that the email address of this person which is jcoachj@gmail.com

```

GET /mail/channel/test?
at=zn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&at=zn3j32oktf2a0q6oa3k9sfr6d09yzf&TYPE=html&zx=9thyil
sywkw&DOMIAN=mail.google.com&t=1 HTTP/1.1
Accept: */*
Referer: http://mail.google.com/mail/?ui=1&view=page&name=js&ver=167ge8cpe09rv
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: b.mail.google.com
Connection: Keep-Alive
Cookie: GX=DQAAAG8AAAAm2oW8LqM60qoQ5w2jVJ-
zhIfuyAQ3GUKvcv4N9vQ61WuLpVMcmw1Jhm1m9_P3qZbyTkwIwDo5cnuJHuMxySQ3a5_HduypckaYwOo-
H5KsrUCM822caTi0C7M7WnqJdfJa63rj2FKElFpHqQf52we; S=gmail=L5hb7hHJ9B97n6StW44FvA:gmail_yj=-
OoenmU7qTeuQ1dsN3B1kg; gmpoxy=6uatNcZZmB8:gmpoxy_yj=FRV17ZyWnh8:gmpoxy_yj_sub=bzgowOybBARA;
GMAIL_AT=zn3j32oktf2a0q6oa3k9sfr6d09yzf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/475090;
GMAIL_STAT=lt=500&js=251&dw=62&ct=0&tot=2781&fv=1&id=af7d6ae6be&v=tl&st=53&dbe=0&
PREF=ID=8fc081df5e738a3c; TM=1210743469; LM=1216706486; GM=1; S=vvxexHX0oIXNyR8Zj;
NID=13=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf7l-9JQ2AeoD8oWGN9JtOp775tuskkNgEKMRA9P49vIEasp
6NpBuJWdr5pEv4yh6XE0UboY5r3KgJSFshpsI-TfmV; __utmx=173272373.00000983192309928271:2;;
__utmx=173272373.00000983192309928271:1216706401:2592000;
STD=DQAAAGwAAACH8Y_j5izp1fdbDJzwdRFDgtU3aaeZKwgZ7DwUjYpLoqH7F1_E-
X5taC4l0uvzXtrVeE6Zq1gCoqt50MC7lqGvF5YtK9GsvrNTKTTB36PHXZM_gowkl-6JXuYxwOvX0dtx3GeHiG9jMFjCF
OgqNK0f; TZ=-60; GMAIL_HELP=hosted:0

HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Content-Type: text/html; charset=utf-8
ETag:
Transfer-Encoding: chunked
Date: Tue, 22 Jul 2008 06:01:27 GMT
Server: GFE/1.3

1a2
<html><body><script>try{document.domain='mail.google.com'};catch(e){}</script><script>try
  
```

Hosts (747)	Files (4301)	Images (2349)	Messages (2)	Credentials (810)	Sessions (2108)	DNS (2560)	Parameters (99012)	Keywords	Anomalies					
Filter keyword:										<input type="checkbox"/> Case sensitive	ExactPhase	<input type="checkbox"/> Any column	Clear	Apply
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Rec...	...			
90785	NON-914RDopen[1].jpg	jpg	480 731 B	209.177.73.6 [253.photobucket.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 36558	HttpGetNormal	2008-07-22 06:10:12 UTC	C...	i			
90440	us.BEA5B7EC[3].xml	xml	304 B	209.191.93.51 [address2.pim.vip.mud.yahoo.com] [address...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 36526	HttpGetNormal	2008-07-22 06:09:59 UTC	C...	a			
48627	us.BEA5B7EC[2].xml	xml	1 076 B	209.191.93.51 [address2.pim.vip.mud.yahoo.com] [address...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34282	HttpGetNormal	2008-07-22 05:02:05 UTC	C...	a			
20145	ga[1].js	js	22 759 B	209.85.171.127 [www.google-analytics.l.google.com] [jw...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 32896	HttpGetNormal	2008-07-22 04:30:44 UTC	C...	v			
20181	__utm.gif.3D2E1B8D[1].gif	gif	35 B	209.85.171.127 [www.google-analytics.l.google.com] [jw...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 32896	HttpGetNormal	2008-07-22 04:30:45 UTC	C...	v			
20221	__utm.gif.2F428187[1].gif	gif	35 B	209.85.171.127 [www.google-analytics.l.google.com] [jw...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 32896	HttpGetNormal	2008-07-22 04:30:47 UTC	C...	v			
50028	update.33C9374F[1].html	html	60 480 B	209.85.171.136 [sb.l.google.com] [sb.google.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34466	HttpGetNormal	2008-07-22 05:19:44 UTC	C...	s			
94254	google.com[1].cer	cer	906 B	209.85.171.190 [sb.l.google.com] [sb.google.com] [sb-sl.j...	TCP 443	192.168.15.4 (Apple_iOS)	TCP 36862	TlsCertificate	2008-07-22 06:11:34 UTC	C...	1			
78984	cleardot.gif.65084796[1].gif	gif	43 B	209.85.201.189 [b.googlemail.l.google.com] [chatenablen....	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35826	HttpGetNormal	2008-07-22 06:01:02 UTC	C...	c			
79014	test.9A335343[1].html	html	515 B	209.85.201.189 [b.googlemail.l.google.com] [chatenablen....	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35828	HttpGetChunked	2008-07-22 06:01:02 UTC	C...	b			
79117	bind.4B5F7513[1].html	html	1 813 B	209.85.201.189 [b.googlemail.l.google.com] [chatenablen....	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35828	HttpGetChunked	2008-07-22 06:01:05 UTC	C...	b			
67335	DSC01727e[1].jpg	jpg	12 348 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35266	HttpGetNormal	2008-07-22 05:53:53 UTC	C...	v			
67432	DSC01712s[1].jpg	jpg	11 926 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35266	HttpGetNormal	2008-07-22 05:53:53 UTC	C...	v			
67333	DSC01705[1].jpg	jpg	52 182 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35264	HttpGetNormal	2008-07-22 05:53:53 UTC	C...	v			
67537	DSC01715e[1].jpg	jpg	13 322 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35264	HttpGetNormal	2008-07-22 05:53:53 UTC	C...	v			
67582	DSC01708s[1].jpg	jpg	14 711 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35264	HttpGetNormal	2008-07-22 05:53:54 UTC	C...	v			
67639	DSC01706[1].jpg	jpg	64 315 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35266	HttpGetNormal	2008-07-22 05:53:54 UTC	C...	v			
67668	DSC01710[1].jpg	jpg	191 948 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35264	HttpGetNormal	2008-07-22 05:53:54 UTC	C...	v			
67858	DSC01711[1].jpg	jpg	49 941 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35266	HttpGetNormal	2008-07-22 05:53:54 UTC	C...	v			
68067	DSC01716[1].jpg	jpg	58 237 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35266	HttpGetNormal	2008-07-22 05:53:55 UTC	C...	v			
68037	DSC01714[1].jpg	jpg	182 178 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35264	HttpGetNormal	2008-07-22 05:53:55 UTC	C...	v			
68316	DSC01722[1].jpg	jpg	80 167 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35266	HttpGetNormal	2008-07-22 05:53:55 UTC	C...	v			
68416	14[1].jpg	jpg	99 929 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35264	HttpGetNormal	2008-07-22 05:53:55 UTC	C...	v			
69869	12s[1].jpg	jpg	13 492 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35312	HttpGetNormal	2008-07-22 05:55:25 UTC	C...	v			
69867	8s[1].jpg	jpg	18 968 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35310	HttpGetNormal	2008-07-22 05:55:25 UTC	C...	v			
69932	9s[1].jpg	jpg	15 656 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35312	HttpGetNormal	2008-07-22 05:55:25 UTC	C...	v			
69943	4s[1].jpg	jpg	21 796 B	209.123.229.231 [www.toroleather.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 35310	HttpGetNormal	2008-07-22 05:55:25 UTC	C...	v			
47463	index[2].html	html	122 499 B	209.131.36.158 [www.yahoo-hi3.akadns.net] [www.yahoo....	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34168	HttpGetChunked	2008-07-22 04:57:19 UTC	C...	v			
48255	index[3].html	html	125 011 B	209.131.36.158 [www.yahoo-hi3.akadns.net] [www.yahoo....	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34240	HttpGetChunked	2008-07-22 05:00:00 UTC	C...	v			

To make sure that this is the email address used on this IP address when we do a search on NetworkMiner we can see that jcoachj@gmail.com is used multiple times with the IP address 192.168.15.4.

Looking at the list of people taking the course we can see that there is only one person with the last name Coach who is Johnny Coach.

Hosts (747) Files (4301) Images (2349) Messages (2) Credentials (810) Sessions (2108) DNS (2560) Parameters (99012) Keywords (122) Anomalies					
Enter keyword as string like "foo" or in hex format like "\xc626172"					
Add keywords from text file					
tuckrige lly coach		Frame number	Timestamp	Keyword	Context
		77506	2008-07-22 06:00:44 UTC	coach [0x636F616368]	aUuLKeDM4CzM1Z7yPw3P4-V&gausr=jcoachj%40gmail.c...
		77514	2008-07-22 06:00:44 UTC	coach [0x636F616368]	lendar.Set-Cookie: OL_SESSION=jcoachj@gmail.com-cal...
		77528	2008-07-22 06:00:44 UTC	coach [0x636F616368]	fiR-uG9g7c8EUw6UHA; OL_SESSION=jcoachj@gmail.co...
		77546	2008-07-22 06:00:44 UTC	coach [0x636F616368]	fiR-uG9g7c8EUw6UHA; OL_SESSION=jcoachj@gmail.co...
		77692	2008-07-22 06:00:45 UTC	coach [0x636F616368]	fiR-uG9g7c8EUw6UHA; OL_SESSION=jcoachj@gmail.co...
		77706	2008-07-22 06:00:45 UTC	coach [0x636F616368]	fiR-uG9g7c8EUw6UHA; OL_SESSION=jcoachj@gmail.co...
		77725	2008-07-22 06:00:50 UTC	coach [0x636F616368]	fiR-uG9g7c8EUw6UHA; OL_SESSION=jcoachj@gmail.co...
		78571	2008-07-22 06:00:56 UTC	coach [0x636F616368]	0kcmelZwr2r_SK5dN9qyOuHg&gausr=jcoachj%40gmail.co...
		78573	2008-07-22 06:00:56 UTC	coach [0x636F616368]	0kcmelZwr2r_SK5dN9qyOuHg&gausr=jcoachj%40gmail.co...
		78575	2008-07-22 06:00:56 UTC	coach [0x636F616368]	0kcmelZwr2r_SK5dN9qyOuHg&gausr=jcoachj%40gmail.co...
		78967	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		78968	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		78975	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		78977	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		78984	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		78990	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		78996	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79007	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79008	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79012	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79019	2008-07-22 06:01:02 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79023	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79032	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79036	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79040	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79044	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79049	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79053	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79057	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79061	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79065	2008-07-22 06:01:03 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
		79069	2008-07-22 06:01:04 UTC	coach [0x636F616368]	6d09ydf; GMAIL_SU=1; gmailchat=jcoachj@gmail.com/47...
Remove					