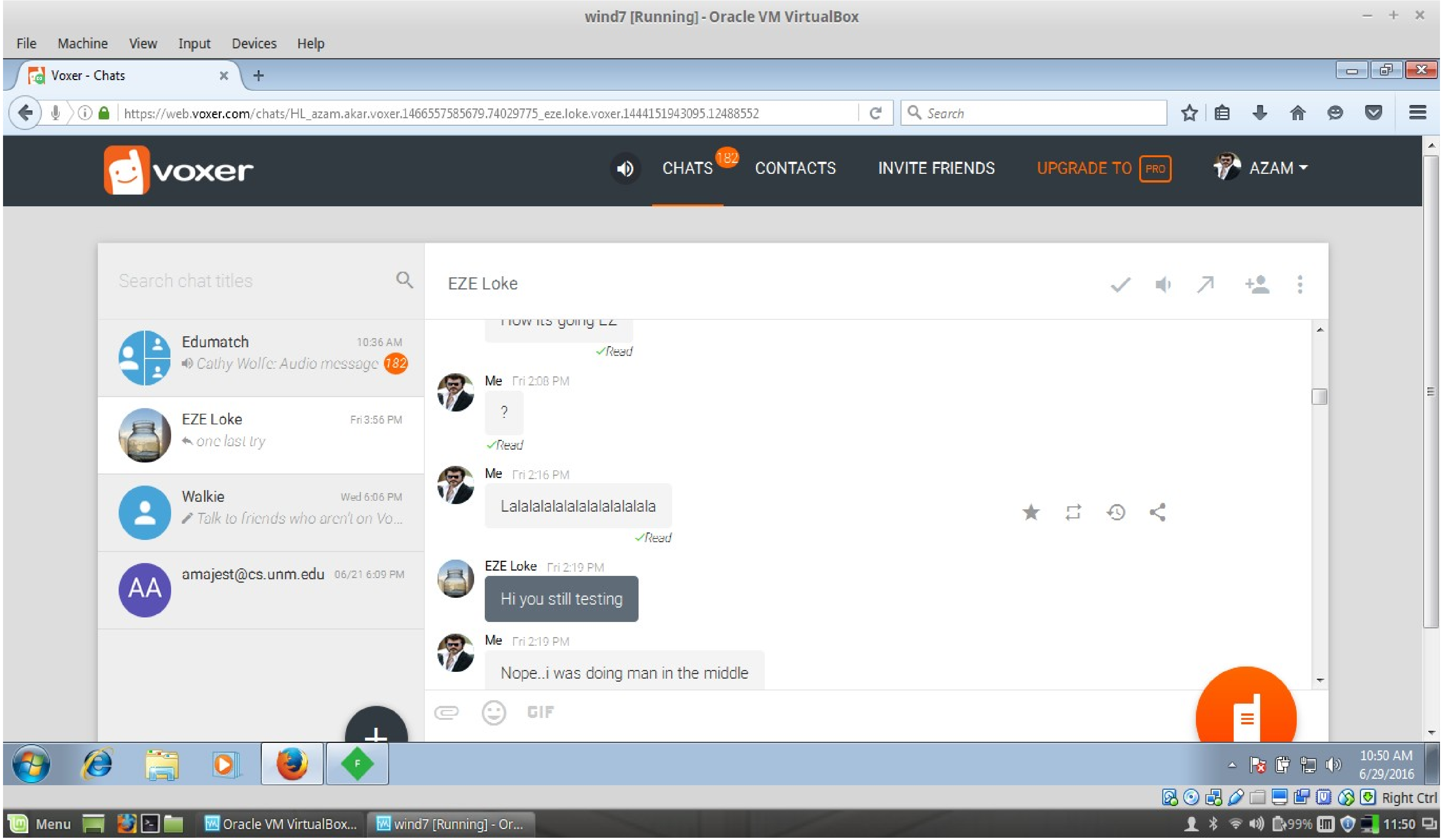
Voxer

- Its a push to talk messaging system.
- Founded by Tom katis in 2007

  Motivation:

  For U.S soldier in Afghanistan to talk other soldier in battle field
- Promises Military grade security.

The Interface



Edumatch 10:36 AM
Cathy Wolfe: Audio message 182

EZE Loke Fri 3:56 PM
one last try

Walkie Wed 6:06 PM
Talk to friends who aren't on Vo...

AA amajest@cs.unm.edu 06/21 6:09 PM

EZE Loke

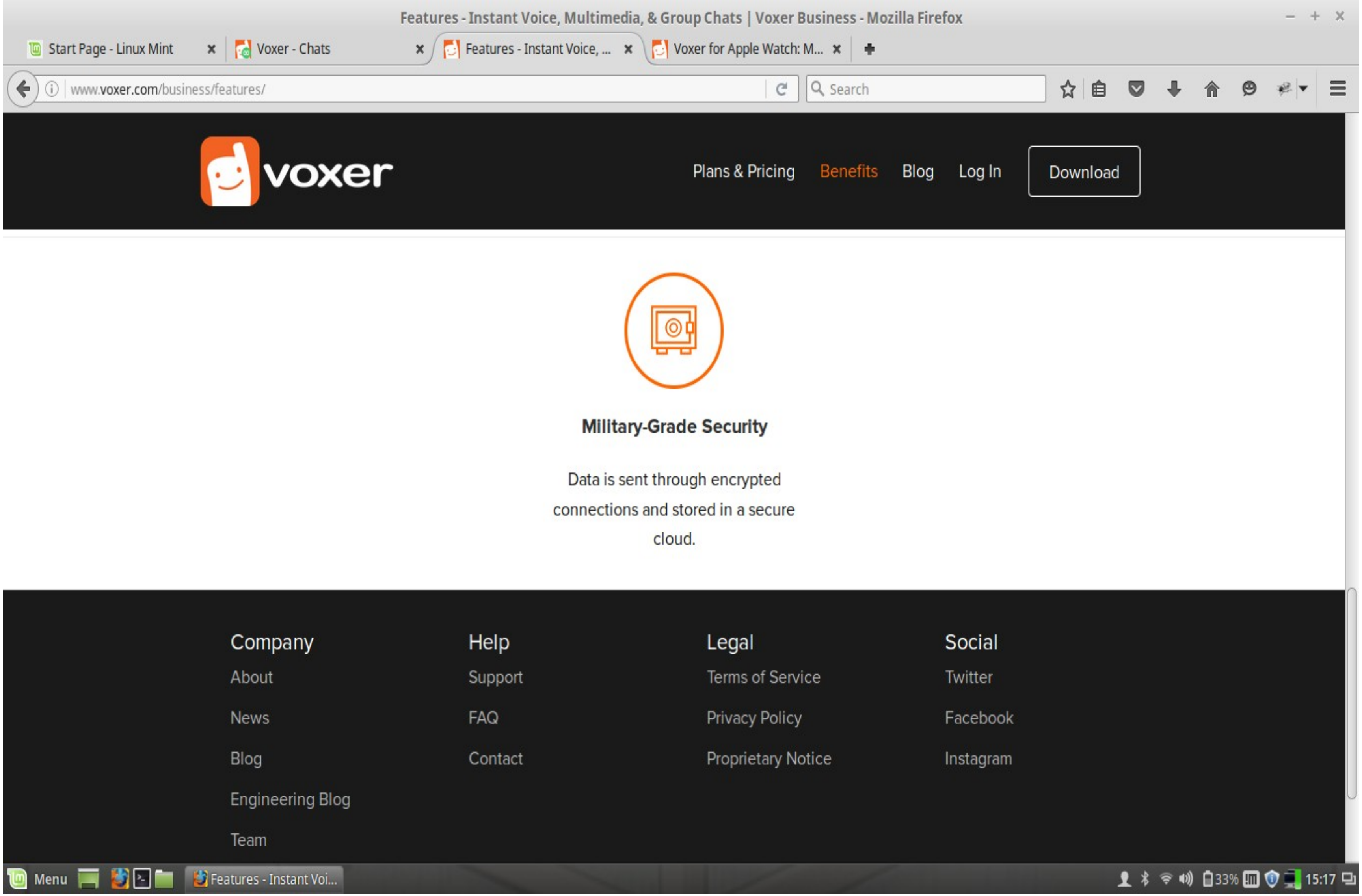
How its going EZ
✓Read

Me Fri 2:08 PM
?
✓Read

Me Fri 2:16 PM
Lalalalalalalalalalalala
✓Read

EZE Loke Fri 2:19 PM
Hi you still testing

Me Fri 2:19 PM
Nope..i was doing man in the middle



Features - Instant Voice, Multimedia, & Group Chats | Voxer Business - Mozilla Firefox
Start Page - Linux Mint
Voxer - Chats
Features - Instant Voice, ...
Voxer for Apple Watch: M...
www.voxer.com/business/features/
Search
voxer
Plans & Pricing
Benefits
Blog
Log In
Download

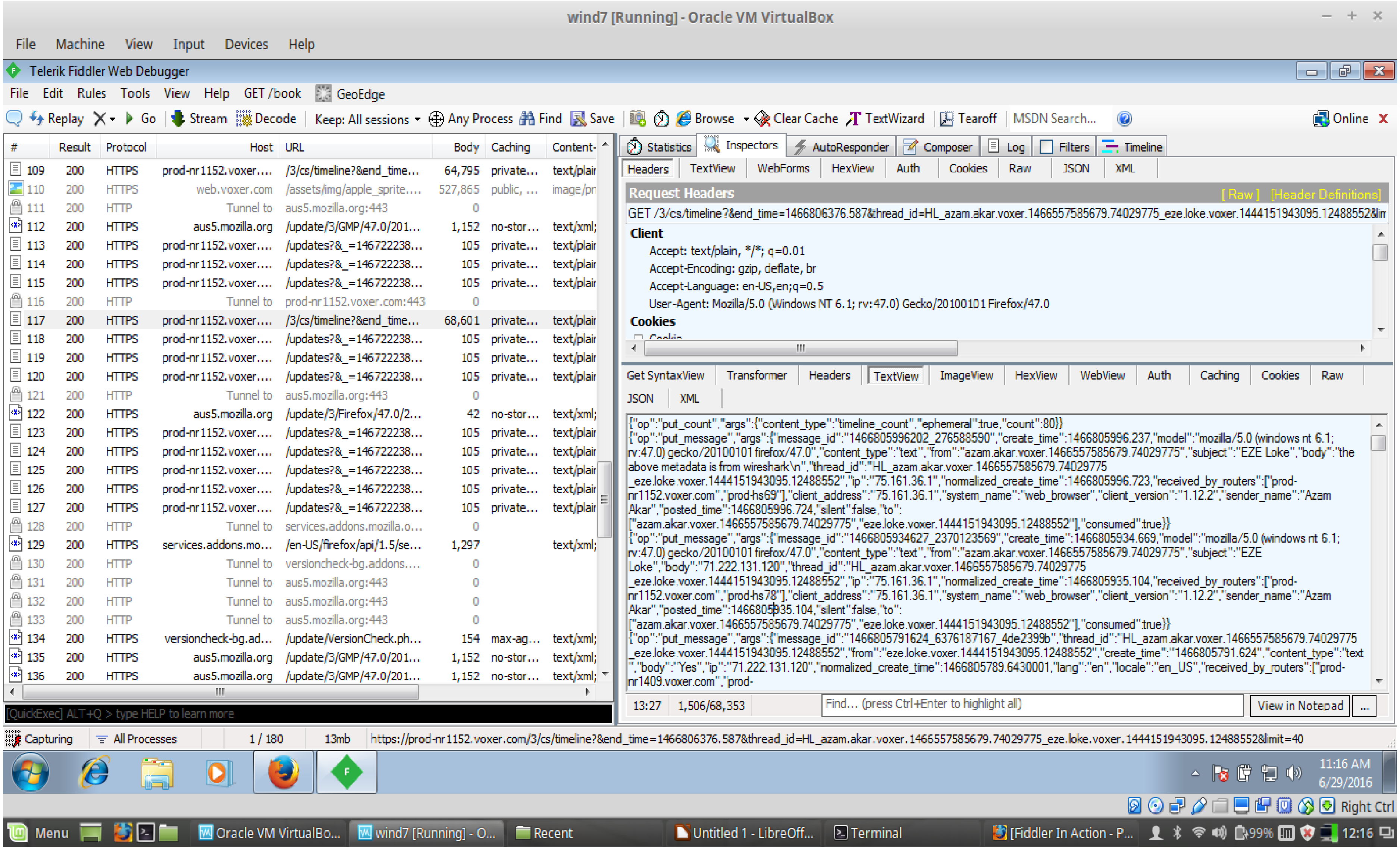
Military-Grade Security

Data is sent through encrypted connections and stored in a secure cloud.

Fiddler

- Its HTTP debugging proxy server
- Create root certificate and configure the firefox browser to trust it
- To my browser fiddler act as a secure web server and to my browser it acts as server
- It uses MITM for decrypting HTTPS traffic

Unencrypted Chats



#	Result	Protocol	Host	URL	Body	Caching	Content-
109	200	HTTPS	prod-nr1152.voxer....	/3/cs/timeline?&end_time...	64,795	private...	text/plair
110	200	HTTPS	web.voxer.com	/assets/img/apple_sprite....	527,865	public, ...	image/pr
111	200	HTTP	Tunnel to	aus5.mozilla.org:443	0		
112	200	HTTPS	aus5.mozilla.org	/update/3/GMP/47.0/201...	1,152	no-stor...	text/xml;
113	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
114	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
115	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
116	200	HTTP	Tunnel to	prod-nr1152.voxer.com:443	0		
117	200	HTTPS	prod-nr1152.voxer....	/3/cs/timeline?&end_time...	68,601	private...	text/plair
118	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
119	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
120	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
121	200	HTTP	Tunnel to	aus5.mozilla.org:443	0		
122	200	HTTPS	aus5.mozilla.org	/update/3/Firefox/47.0/2...	42	no-stor...	text/xml;
123	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
124	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
125	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
126	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
127	200	HTTPS	prod-nr1152.voxer....	/updates?&_=146722238...	105	private...	text/plair
128	200	HTTP	Tunnel to	services.addons.mozilla.o...	0		
129	200	HTTPS	services.addons.mo...	/en-US/firefox/api/1.5/se...	1,297		text/xml;
130	200	HTTP	Tunnel to	versioncheck-bg.addons....	0		
131	200	HTTP	Tunnel to	aus5.mozilla.org:443	0		
132	200	HTTP	Tunnel to	aus5.mozilla.org:443	0		
133	200	HTTP	Tunnel to	aus5.mozilla.org:443	0		
134	200	HTTPS	versioncheck-bg.ad...	/update/VersionCheck.ph...	154	max-ag...	text/xml;
135	200	HTTPS	aus5.mozilla.org	/update/3/GMP/47.0/201...	1,152	no-stor...	text/xml;
136	200	HTTPS	aus5.mozilla.org	/update/3/GMP/47.0/201...	1,152	no-stor...	text/xml;

[QuickExec] ALT+Q > type HELP to learn more

Request Headers

```
GET /3/cs/timeline?&end_time=1466806376.587&thread_id=HL_azam.akar.voxer.1466557585679.74029775_eze.loke.voxer.1444151943095.12488552&lim
Client
    Accept: text/plain, */*; q=0.01
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-US,en;q=0.5
    User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:47.0) Gecko/20100101 Firefox/47.0
Cookies
```

```
{"op":"put_count","args":{"content_type":"timeline_count","ephemeral":true,"count":80}}
{"op":"put_message","args":{"message_id":"1466805996202_276588590","create_time":1466805996.237,"model":"mozilla/5.0 (windows nt 6.1;
rv:47.0) gecko/20100101 firefox/47.0","content_type":"text","from":"azam.akar.voxer.1466557585679.74029775","subject":"EZE Loke","body":"the
above metadata is from wireshark\n","thread_id":"HL_azam.akar.voxer.1466557585679.74029775
_eze.loke.voxer.1444151943095.12488552","ip":"75.161.36.1","normalized_create_time":1466805996.723,"received_by_routers":["prod-
nr1152.voxer.com","prod-hs69"],"client_address":"75.161.36.1","system_name":"web_browser","client_version":"1.12.2","sender_name":"Azam
Akar","posted_time":1466805996.724,"silent":false,"to":
["azam.akar.voxer.1466557585679.74029775","eze.loke.voxer.1444151943095.12488552"],"consumed":true}}
{"op":"put_message","args":{"message_id":"1466805934627_2370123569","create_time":1466805934.669,"model":"mozilla/5.0 (windows nt 6.1;
rv:47.0) gecko/20100101 firefox/47.0","content_type":"text","from":"azam.akar.voxer.1466557585679.74029775","subject":"EZE
Loke","body":"71.222.131.120","thread_id":"HL_azam.akar.voxer.1466557585679.74029775
_eze.loke.voxer.1444151943095.12488552","ip":"75.161.36.1","normalized_create_time":1466805935.104,"received_by_routers":["prod-
nr1152.voxer.com","prod-hs78"],"client_address":"75.161.36.1","system_name":"web_browser","client_version":"1.12.2","sender_name":"Azam
Akar","posted_time":1466805935.104,"silent":false,"to":
["azam.akar.voxer.1466557585679.74029775","eze.loke.voxer.1444151943095.12488552"],"consumed":true}}
{"op":"put_message","args":{"message_id":"1466805791624_6376187167_4de2399b","thread_id":"HL_azam.akar.voxer.1466557585679.74029775
_eze.loke.voxer.1444151943095.12488552","from":"eze.loke.voxer.1444151943095.12488552","create_time":"1466805791.624","content_type":"text
","body":"Yes","ip":"71.222.131.120","normalized_create_time":1466805789.6430001,"lang":"en","locale":"en_US","received_by_routers":["prod-
nr1409.voxer.com","prod-
```

13:27 1,506/68,353 Find... (press Ctrl+Enter to highlight all)

Capturing All Processes 1 / 180 13mb https://prod-nr1152.voxer.com/3/cs/timeline?&end_time=1466806376.587&thread_id=HL_azam.akar.voxer.1466557585679.74029775_eze.loke.voxer.1444151943095.12488552&limit=40

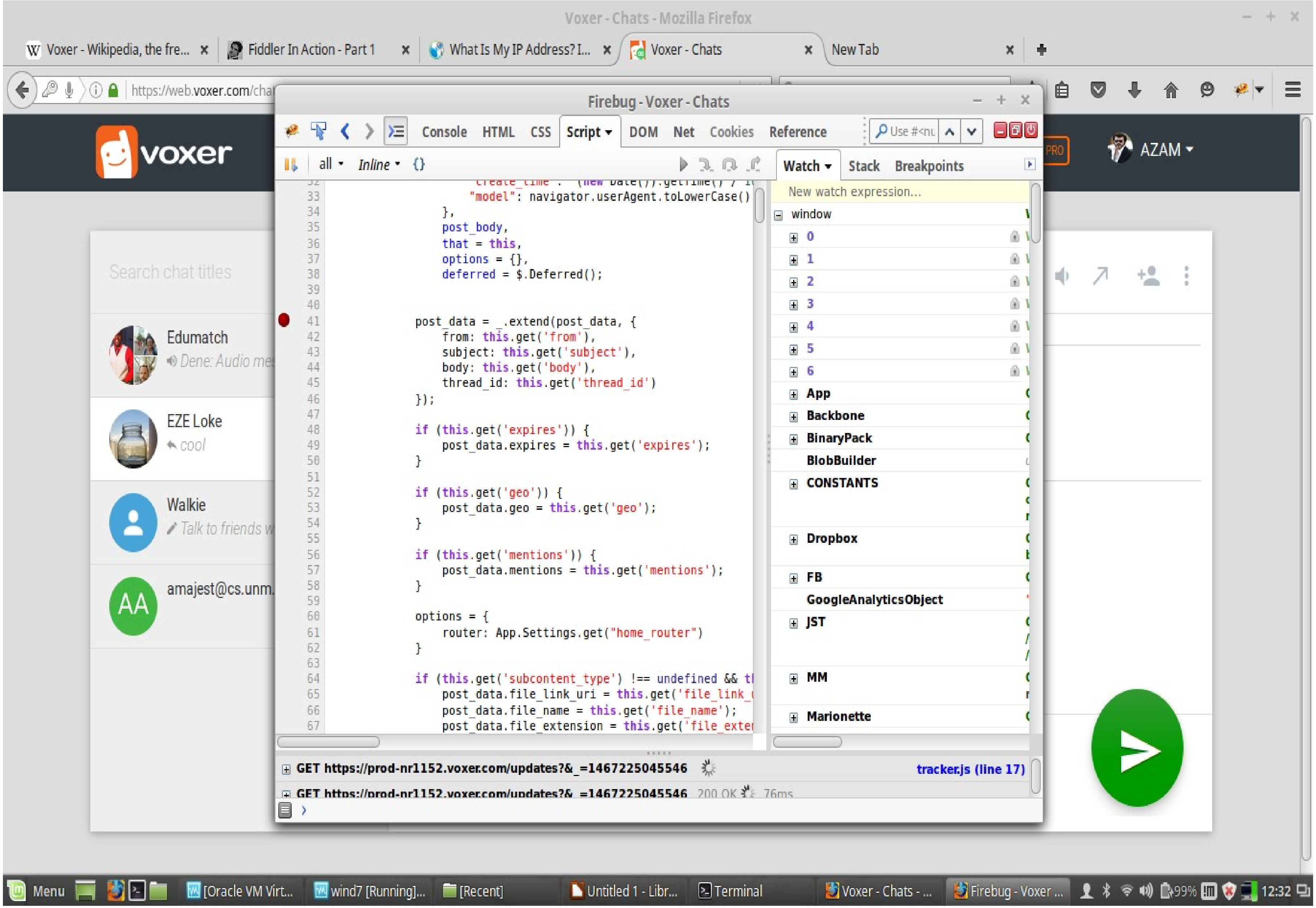
11:16 AM
6/29/2016

Closer look

from":"eze.loke.voxer.1444151943095.12488552","create_time":"1466806378.557","content_type":"text","body":**"You can't say that with certainty. You just know that if it is happening it's not client side.**","ip":"**71.222.131.120**","normalized_create_time":1466806376.587,"lang":"en","locale":"en_US","received_by_routers":["prod-nr1409.voxer.com","prod-hs108"],"client_address":"71.222.131.120","system_name":"Android","client_version":"2.7.12.015020","client_name":"voxer","model":"XT1063","sender_name":"EZE Loke","posted_time":1466806376.689,"silent":false,"to":["eze.loke.voxer.1444151943095.12488552","azam.akar.voxer.1466557585679.74029775"],"consumed":true}} {"op":"put_message","args":{"message_id":"1466808591214_2901138732","create_time":1466808591.249,"model":"mozilla/5.0 (windows nt 6.1; rv:47.0) gecko/20100101 firefox/47.0","content_type":"text","from":"azam.akar.voxer.1466557585679.74029775","subject":"EZE Loke","body":"**my final check thats it\n**","thread_id":"HL_azam.akar.voxer.1466557585679.74029775_eze.loke.voxer.1444151943095.12488552","ip":"75.161.36.1","normalized_create_time":1466808591.61,"received_by_routers":["prod-nr1152.voxer.com","prod-hs66"],"client_address":"**75.161.36.1**","system_name":"web_browser","client_version":"1.12.2","sender_name":"Azam Akar","posted_time":1466808591.61,"silent":false,"to":["azam.akar.voxer.1466557585679.74029775","eze.loke.voxer.1444151943095.12488552"],"consumed":true}} {"op":"put_message","

Client side codes

- Unlike Facebook and Twitter, Voxer got scripts on client side for detecting the device
- Also the code for processing the messages or audios were also in the client side.
- The code am currently debugging to find the parameters is shown in the following slide.



Edumatch
Dene: Audio me

EZE Loke
cool

Walkie
Talk to friends w

AA amajest@cs.unm.

```
                     "create_time": (new Date()).getTime() / 1(
                    "model": navigator.userAgent.toLowerCase()
                },
                post_body,
                that = this,
                options = {},
                deferred = $.Deferred();


            post_data = _.extend(post_data, {
                from: this.get('from'),
                subject: this.get('subject'),
                body: this.get('body'),
                thread_id: this.get('thread_id')
            });

            if (this.get('expires')) {
                post_data.expires = this.get('expires');
            }

            if (this.get('geo')) {
                post_data.geo = this.get('geo');
            }

            if (this.get('mentions')) {
                post_data.mentions = this.get('mentions');
            }

            options = {
                router: App.Settings.get("home_router")
            }

            if (this.get('subcontent_type') !== undefined && tl
                post_data.file_link_uri = this.get('file_link_u
                post_data.file_name = this.get('file_name');
                post_data.file_extension = this.get('file_exter
```

```
GET https://prod-nr1152.voxer.com/updates?&_=1467225045546
GET https://prod-nr1152.voxer.com/updates?&_=1467225045546   200 OK   76ms
```

3 important sequence of headers

- POST: Post a audio/text message to their server

  Request header:**URL: /2/cs/post_message?now=1467789411.579 HTTP/1.1**

  Host Name: prod-nr1152.voxer. com

- GET:

  Request header: **URL: /track/?data = eyJldmVud....**

  Hostname: api.mixpanel.com(api for visualizing data)

- GET: retrieving the timeline with the updated messages.

  Request header: **URL: /updates/&_1467788990443 HTTP/1.1**

  Host Name: prod-nr1152.voxer.com

Fields in the request

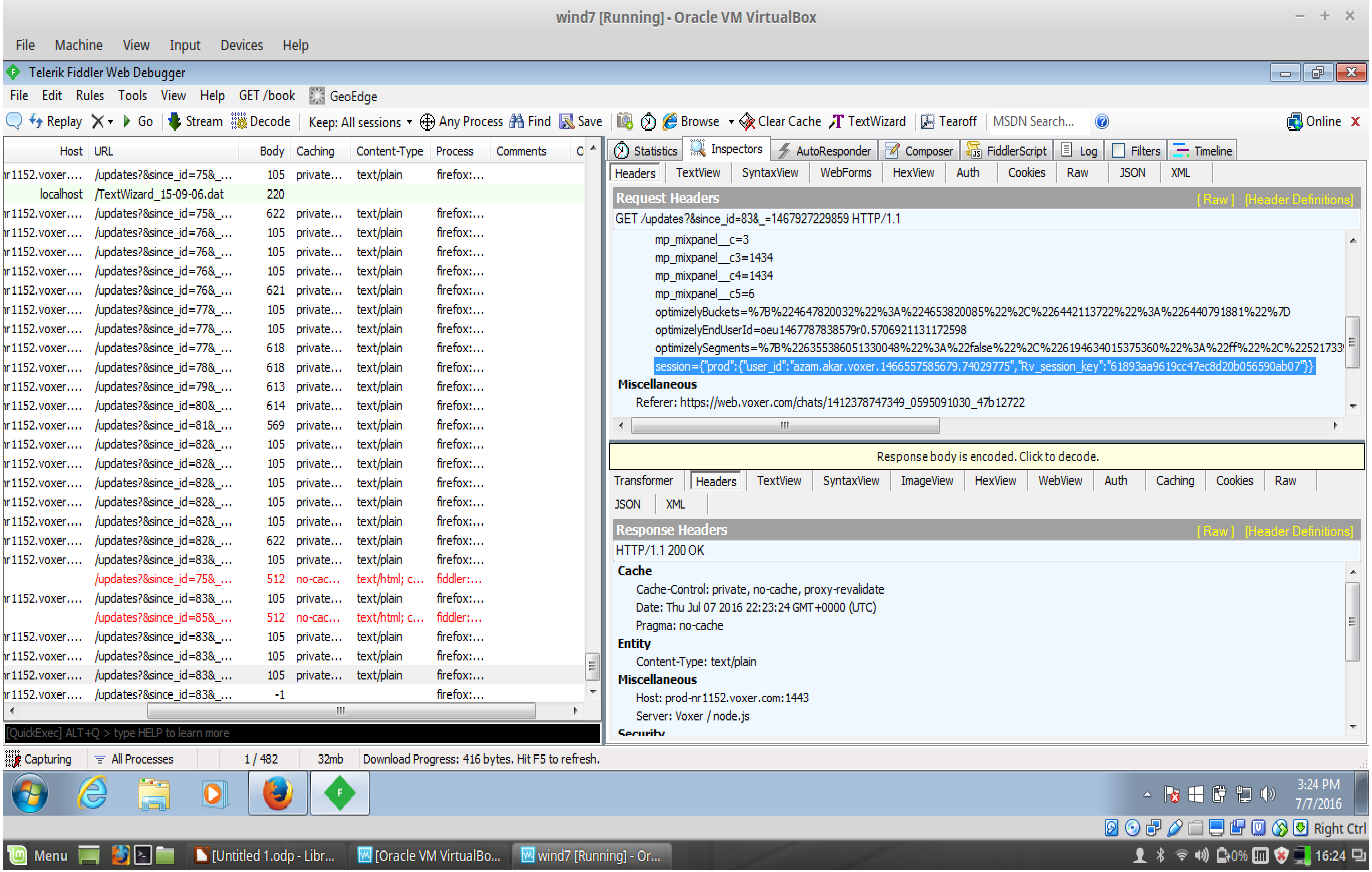
- Message id : Its a unique number given to each messages and its not sequential.
- Create time : The time when the message created in decimal format.
- Model: device information regarding browsers and operating system and IP addresses.
- Content_type: text /audios
- From Ids, To Ids. Thread ids{each chat is a one thread}
- Body and Subject.
- If the device allows location information, it also takes the location information.

Fields in the response

- header_store_status: For successful response it is 200
- body_store_status: For successful its 0
- client_message_id: The message id originally created
- final_message_id: The same as the original id.
- Name : server_name
- Posted time: Different from the create time
- Thread id

Session key protection for timelines

- You need the users Rvsession key to look in their timelines
- Fiddler being a mitm proxy reveals the unencrypted Rvsession key of the user but however we were able to see the messages and timeline of the user in plain text.



Host	URL	Body	Caching	Content-Type	Process	Comments	C
r1152.voxer....	/updates?&since_id=75&_...	105	private...	text/plain	firefox:...		
localhost	/TextWizard_15-09-06.dat	220					
r1152.voxer....	/updates?&since_id=75&_...	622	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=76&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=76&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=76&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=76&_...	621	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=77&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=77&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=77&_...	618	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=78&_...	618	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=79&_...	613	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=80&_...	614	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=81&_...	569	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=82&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=82&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=82&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=82&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=82&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=82&_...	622	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=83&_...	105	private...	text/plain	firefox:...		
	/updates?&since_id=75&_...	512	no-cac...	text/html; c...	fiddler:...		
r1152.voxer....	/updates?&since_id=83&_...	105	private...	text/plain	firefox:...		
	/updates?&since_id=85&_...	512	no-cac...	text/html; c...	fiddler:...		
r1152.voxer....	/updates?&since_id=83&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=83&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=83&_...	105	private...	text/plain	firefox:...		
r1152.voxer....	/updates?&since_id=83&_...	-1			firefox:...		

Request Headers [Raw] [Header Definitions]

```
GET /updates?&since_id=83&_=1467927229859 HTTP/1.1
        mp_mixpanel__c=3
        mp_mixpanel__c3=1434
        mp_mixpanel__c4=1434
        mp_mixpanel__c5=6
        optimizelyBuckets=%7B%224647820032%22%3A%224653820085%22%2C%226442113722%22%3A%226440791881%22%7D
        optimizelyEndUserId=oeu1467787838579r0.5706921131172598
        optimizelySegments=%7B%2263553860513300 48%22%3A%22false%22%2C%22619463401537 5360%22%3A%22ff%22%2C%22521733
        session={"prod":{"user_id":"azam.akar.voxer.1466557585679.74029775","Rv_session_key":"61893aa9619cc47ec8d20b056590ab07"}}
Miscellaneous
    Referer: https://web.voxer.com/chats/1412378747349_0595091030_47b12722
```

Response body is encoded. Click to decode.

Response Headers [Raw] [Header Definitions]

```
HTTP/1.1 200 OK
Cache
    Cache-Control: private, no-cache, proxy-revalidate
    Date: Thu Jul 07 2016 22:23:24 GMT+0000 (UTC)
    Pragma: no-cache
Entity
    Content-Type: text/plain
Miscellaneous
    Host: prod-nr1152.voxer.com:1443
    Server: Voxer / node.js
Security
```

1 / 482   32mb   Download Progress: 416 bytes. Hit F5 to refresh.

Key observation

- Unencrypted chats and audio.
- Uses standard UNIX epoch time for create, post and delivery time and there is no much difference between create and post time.
- No hardware ID's transferred to the server other than device information like browser, OS details and the IP details.
- After each POST message request there was a api downloaded from api.mixpanel.com which is a tool for visualizing data.