HOW TO FIND PASSWORDS USING WIRESHARK

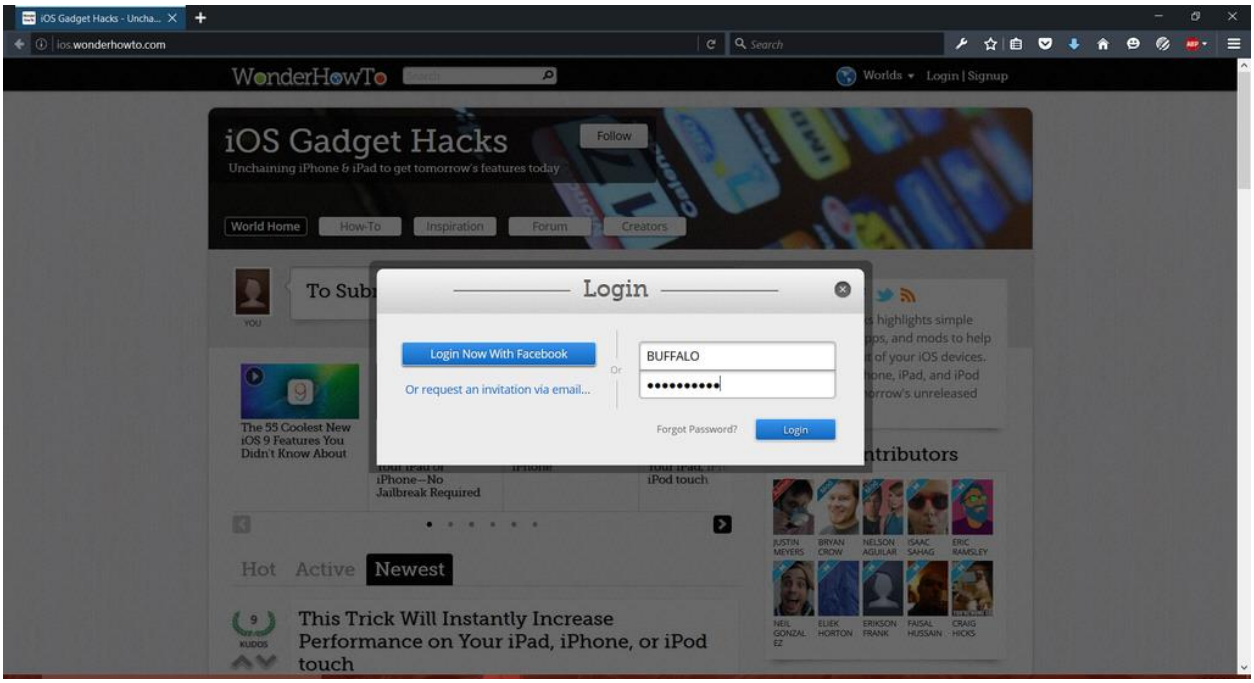
Step 1: Downloading Wireshark to Your CPU

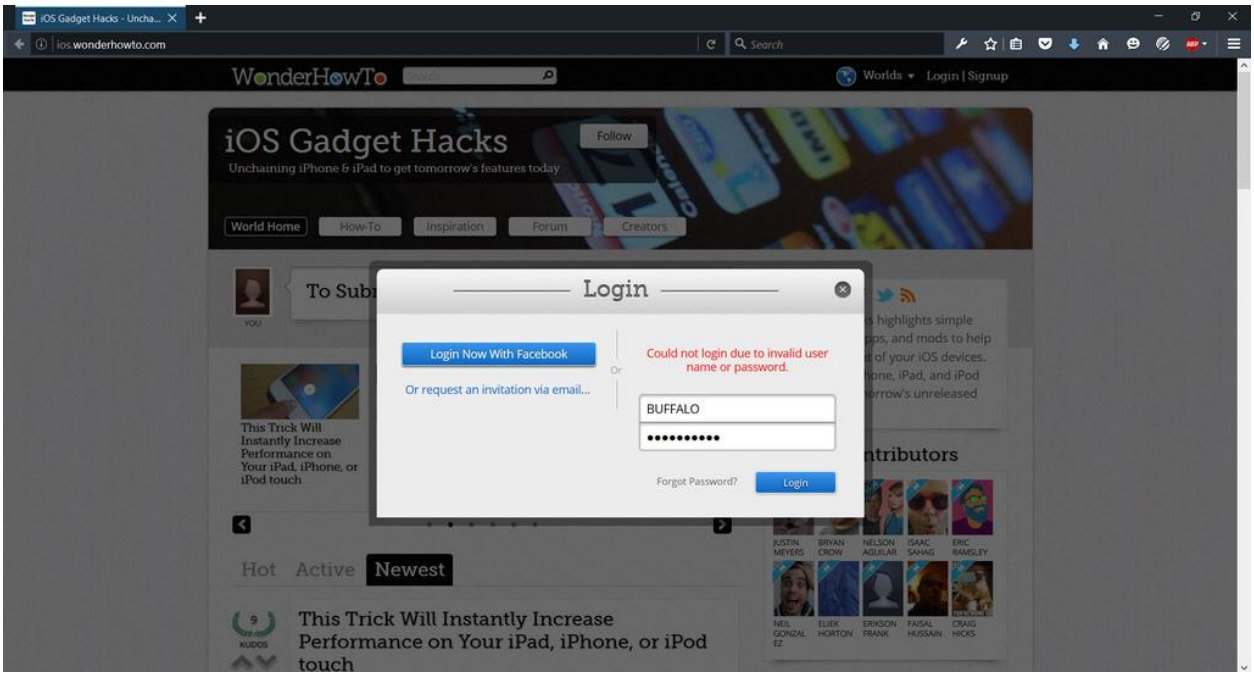
Step 2: How You Know a Website Uses HTTPS

the information in HTTPS packets because some bright people found it useful to protect this information and this is a good thing. Major websites all have encrypted packets and it would be foolish to bother with them, especially if the only thing you have read is this how to. Above are some websites that use HTTPS and you know this because there is a little green lock and the website starts with HTTPS not HTTP.

Step 3: Finding a Password

First one must identify an unprotected website and make a log on attempt - either successful or unsuccessful. It is VERY IMPORTANT that you click the capture button in the upper left corner of wire shark and have it run while you make the logon attempt. In the second step we will follow this packet and track it down using wire shark.

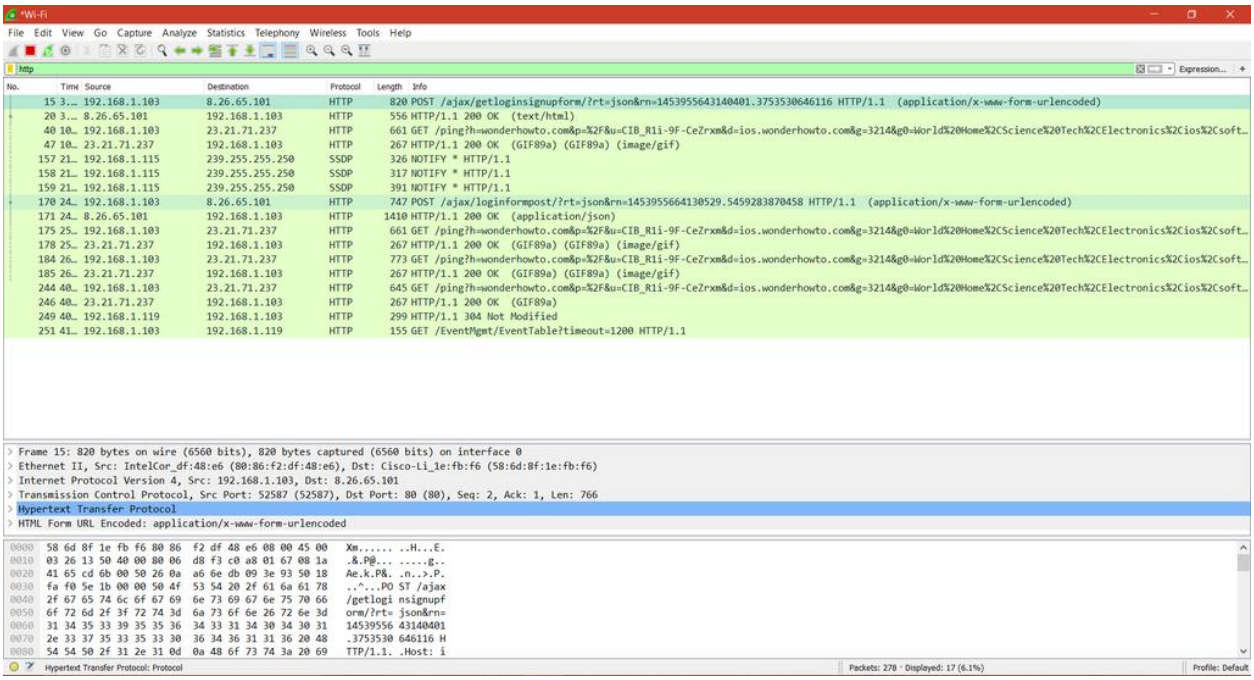


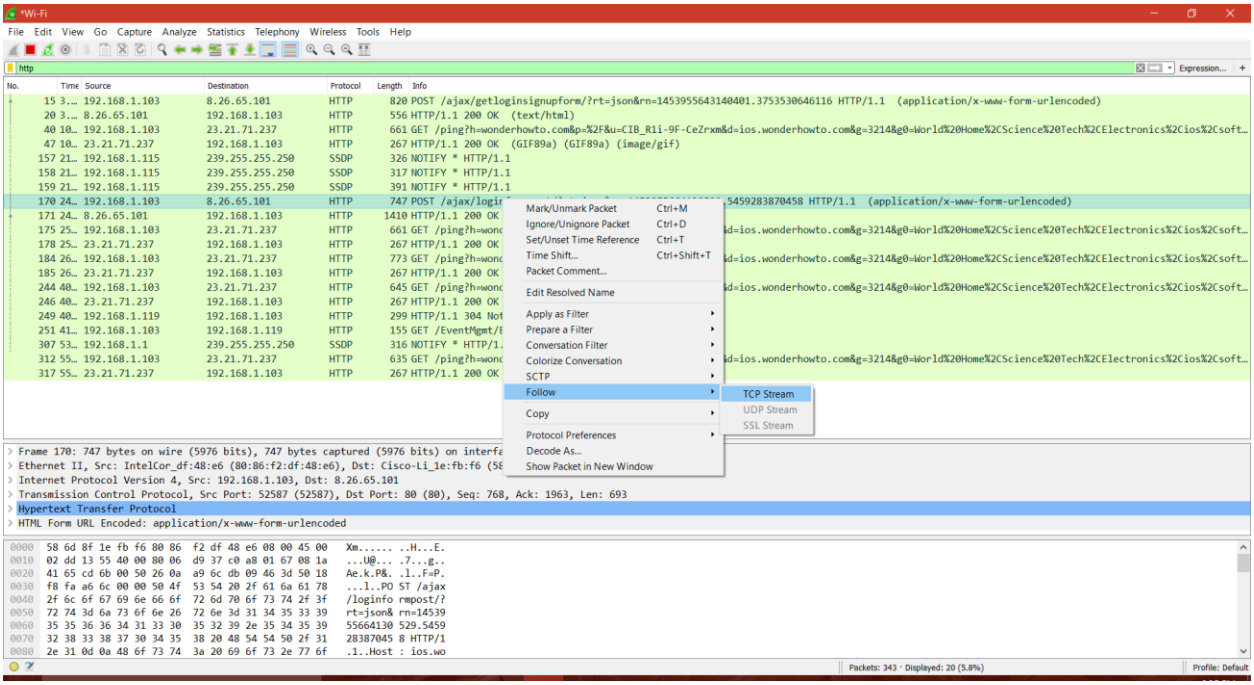


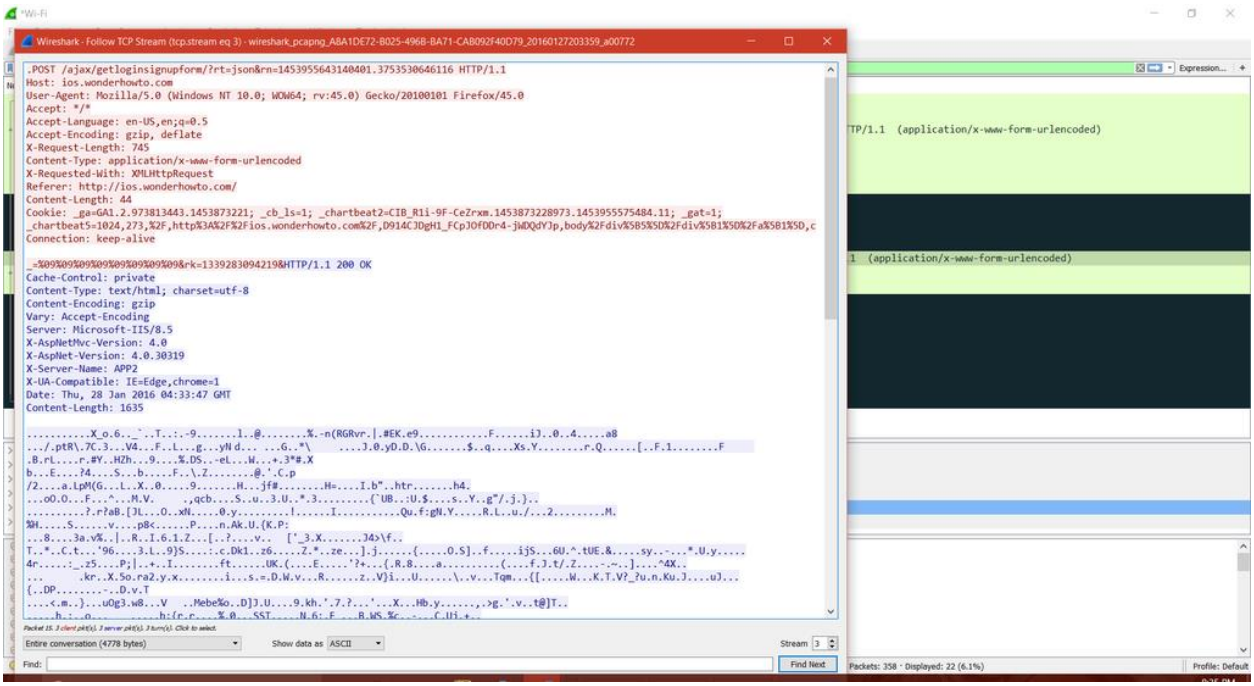
Step 6: Finding a Password (Continued)

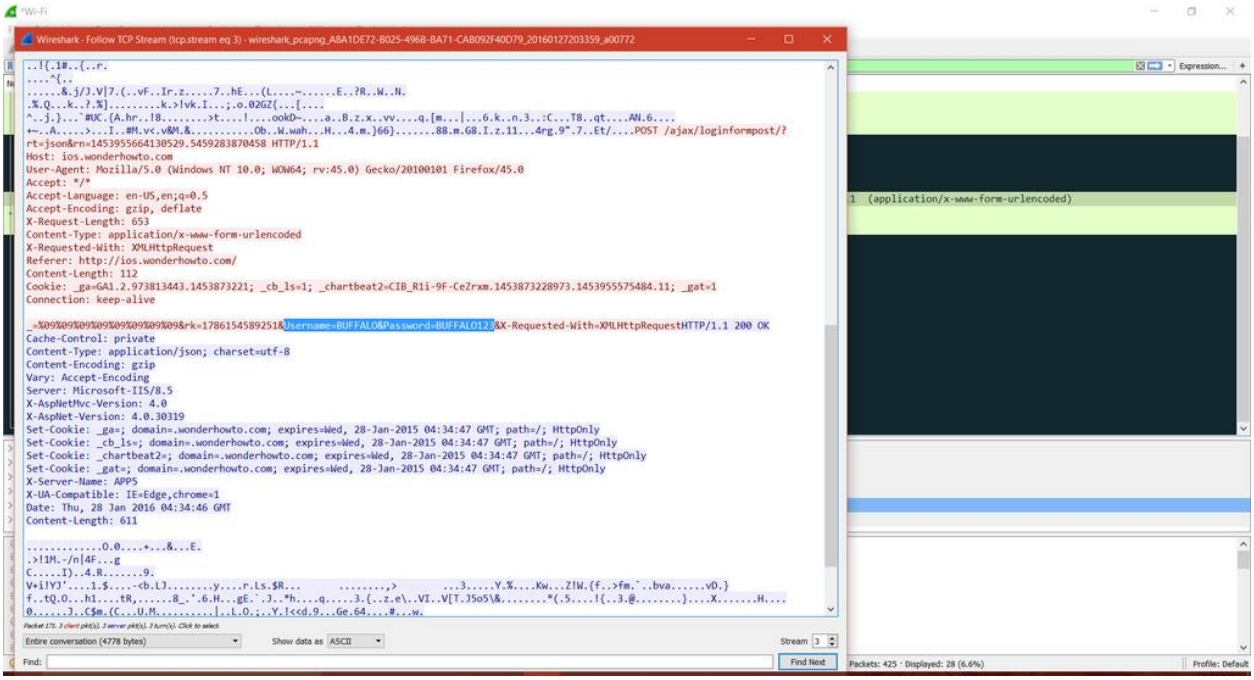
The second step to finding the packets that contain login information is to understand the protocol to look for. HTTP is the protocol we will be dealing with when looking for passwords. Wireshark comes with the option to filter packets. In the filter box type "http.request.method == POST". By filtering this you are now only looking at the post

packet for HTTP. This drastically narrows the search and helps to slow down the traffic by minimizing what pops up on the screen. Then at the far right of the packet in the info section you will see something like ".login" or "/login". You can see exactly what I am talking about if you follow the pictures above. Then you will right click on it and go down to "FOLLOW" then to "TCP STREAM". Once you get there look in the red text paragraphs and try to find what I was able to locate in the picture. And you have just located the password and username you have entered on the unprotected login page - whether or not the password and username are correct are irrelevant.




*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Protocol Length Info
15 3... 192.168.1.103 8.26.65.101 HTTP 820 POST /ajax/getloginsignupform/?rt=json&rn=1453955643140401.3753530646116 HTTP/1.1 (application/x-www-form-urlencoded)
20 3... 8.26.65.101 192.168.1.103 HTTP 556 HTTP/1.1 200 OK (text/html)
40 10... 192.168.1.103 23.21.71.237 HTTP 661 GET /ping?h=wonderhowto.com&p=%2F&u=CIB_R1i-9F-CeZrxm&d=ios.wonderhowto.com&g=3214&g0=World%20Home%2CScience%20Tech%2CElectronics%2Cios%2Csoft...
47 10... 23.21.71.237 192.168.1.103 HTTP 267 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
157 21... 192.168.1.115 239.255.255.250 SSDP 326 NOTIFY * HTTP/1.1
158 21... 192.168.1.115 239.255.255.250 SSDP 317 NOTIFY * HTTP/1.1
159 21... 192.168.1.115 239.255.255.250 SSDP 391 NOTIFY * HTTP/1.1
170 24... 192.168.1.103 8.26.65.101 HTTP 747 POST /ajax/logir ,5459283870458 HTTP/1.1 (application/x-www-form-urlencoded)
171 24... 8.26.65.101 192.168.1.103 HTTP 1410 HTTP/1.1 200 OK
175 25... 192.168.1.103 23.21.71.237 HTTP 661 GET /ping?h=wonc d=ios.wonderhowto.com&g=3214&g0=World%20Home%2CScience%20Tech%2CElectronics%2Cios%2Csoft...
178 25... 23.21.71.237 192.168.1.103 HTTP 267 HTTP/1.1 200 OK
184 26... 192.168.1.103 23.21.71.237 HTTP 773 GET /ping?h=wonc d=ios.wonderhowto.com&g=3214&g0=World%20Home%2CScience%20Tech%2CElectronics%2Cios%2Csoft...
185 26... 23.21.71.237 192.168.1.103 HTTP 267 HTTP/1.1 200 OK
244 40... 192.168.1.103 23.21.71.237 HTTP 645 GET /ping?h=wonc d=ios.wonderhowto.com&g=3214&g0=World%20Home%2CScience%20Tech%2CElectronics%2Cios%2Csoft...
246 40... 23.21.71.237 192.168.1.103 HTTP 267 HTTP/1.1 200 OK
249 40... 192.168.1.119 192.168.1.103 HTTP 299 HTTP/1.1 304 Not
251 41... 192.168.1.103 192.168.1.119 HTTP 155 GET /EventMgmt/E
307 53... 192.168.1.1 239.255.255.250 SSDP 316 NOTIFY * HTTP/1.
312 55... 192.168.1.103 23.21.71.237 HTTP 635 GET /ping?h=wonc d=ios.wonderhowto.com&g=3214&g0=World%20Home%2CScience%20Tech%2CElectronics%2Cios%2Csoft...
317 55... 23.21.71.237 192.168.1.103 HTTP 267 HTTP/1.1 200 OK
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
Frame 170: 747 bytes on wire (5976 bits), 747 bytes captured (5976 bits) on interfa
Ethernet II, Src: IntelCor_df:48:e6 (80:86:f2:df:48:e6), Dst: Cisco-Li_1e:fb:f6 (58
Internet Protocol Version 4, Src: 192.168.1.103, Dst: 8.26.65.101
Transmission Control Protocol, Src Port: 52587 (52587), Dst Port: 80 (80), Seq: 768, Ack: 1963, Len: 693
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 58 6d 8f 1e fb f6 80 86 f2 df 48 e6 08 00 45 00 Xm..... ..H...E.
0010 02 dd 13 55 40 00 80 06 d9 37 c0 a8 01 67 08 1a ...U@... .7...g..
0020 41 65 cd 6b 00 50 26 0a a9 6c db 09 46 3d 50 18 Ae.k.P&. .l..F=P.
0030 f8 fa a6 6c 00 00 50 4f 53 54 20 2f 61 6a 61 78 ...l..PO ST /ajax
0040 2f 6c 6f 67 69 6e 66 6f 72 6d 70 6f 73 74 2f 3f /loginfo rmpost/?
0050 72 74 3d 6a 73 6f 6e 26 72 6e 3d 31 34 35 33 39 rt=json& rn=14539
0060 35 35 36 36 34 31 33 30 35 32 39 2e 35 34 35 39 55664130 529.5459
0070 32 38 33 38 37 30 34 35 38 20 48 54 54 50 2f 31 28387045 8 HTTP/1
0080 2e 31 0d 0a 48 6f 73 74 3a 20 69 6f 73 2e 77 6f .1..Host : ios.wo
Packets: 343 · Displayed: 20 (5.8%)
Profile: Default


*Wi-Fi
Wireshark · Follow TCP Stream (tcp.stream eq 3) · wireshark_pcapng_A8A1DE72-B025-496B-BA71-CAB092F40D79_20160127203359_a00772
.POST /ajax/getloginsignupform/?rt=json&rn=1453955643140401.3753530646116 HTTP/1.1
Host: ios.wonderhowto.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Request-Length: 745
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://ios.wonderhowto.com/
Content-Length: 44
Cookie: _ga=GA1.2.973813443.1453873221; _cb_ls=1; _chartbeat2=CIB_R1i-9F-CeZrxm.1453873228973.1453955575484.11; _gat=1;
_chartbeat5=1024,273,%2F,http%3A%2F%2Fios.wonderhowto.com%2F,D914CJDgH1_FCpJOfDDr4-jWDQdYJp,body%2Fdiv%5B5%5D%2Fdiv%5B1%5D%2Fa%5B1%5D,c
Connection: keep-alive
_=%09%09%09%09%09%09%09&rk=1339283094219&HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
X-AspNetMvc-Version: 4.0
X-AspNet-Version: 4.0.30319
X-Server-Name: APP2
X-UA-Compatible: IE=Edge,chrome=1
Date: Thu, 28 Jan 2016 04:33:47 GMT
Content-Length: 1635
Entire conversation (4778 bytes)
Show data as ASCII
Stream 3
Find:
Find Next
Packets: 358 · Displayed: 22 (6.1%)
Profile: Default


Wireshark - Follow TCP Stream (tcp.stream eq 3) - wireshark_pcapng_A8A1DE72-B025-496B-BA71-CAB092F40D79_20160127203359_a00772
..!{.1#..{..r.
....^{..
.....&.j/J.V|7.(..vF..Ir.z.....7..hE...(L....~.....E..?R..W..N.
.%.Q...k..?.%].....k.>!vk.I...;.o.02GZ{...[....
^..}.}...`#UC.{A.hr..!8.....>t....!....ookD~....a..B.z.x..vv....q.[m...|...6.k..n.3..:C...T8..qt....AN.6....
+~..A.....>...I..#M.v<.v&M.&.....Ob..W.wah...H...4.m.}66}.....88.m.G8.I.z.11...4rg.9".7..Et/....POST /ajax/loginformpost/?
rt=json&rn=1453955664130529.5459283870458 HTTP/1.1
Host: ios.wonderhowto.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Request-Length: 653
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://ios.wonderhowto.com/
Content-Length: 112
Cookie: _ga=GA1.2.973813443.1453873221; _cb_ls=1; _chartbeat2=CIB_R1i-9F-CeZrxm.1453873228973.1453955575484.11; _gat=1
Connection: keep-alive
_=%09%09%09%09%09%09%09%09&rk=17861545892518Username=BUFFALO&Password=BUFFALO12&X-Requested-With=XMLHttpRequestHTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Content-Encoding: gzip
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
X-AspNetMvc-Version: 4.0
X-AspNet-Version: 4.0.30319
Set-Cookie: _ga=; domain=.wonderhowto.com; expires=Wed, 28-Jan-2015 04:34:47 GMT; path=/; HttpOnly
Set-Cookie: _cb_ls=; domain=.wonderhowto.com; expires=Wed, 28-Jan-2015 04:34:47 GMT; path=/; HttpOnly
Set-Cookie: _chartbeat2=; domain=.wonderhowto.com; expires=Wed, 28-Jan-2015 04:34:47 GMT; path=/; HttpOnly
Set-Cookie: _gat=; domain=.wonderhowto.com; expires=Wed, 28-Jan-2015 04:34:47 GMT; path=/; HttpOnly
X-Server-Name: APP5
X-UA-Compatible: IE=Edge,chrome=1
Date: Thu, 28 Jan 2016 04:34:46 GMT
Content-Length: 611
.............O.0....+...&...E.
.>!1M.-/n|4F...g
C.....I)..4.R......9.
V+iIYJ'....1.$....<b.LJ........y....r.Ls.$R... ....,> ...3.....Y.%....Kw...ZIW.{f..>fm.`..bva......vD.}
f..tQ.O...h1....tR,......8_.'.6.H...gE.`.J..*h....q.....3.{..z.e\..VI..V[T.J5o5\&........*(.5....!{..3.@........}....X.......H....
0.....J..C$m.(C...U.M.........|..L.O.;..Y.!<<d.9...Ge.64....#...w.
Packet 173. 3 client pkt(s), 3 server pkt(s), 3 turn(s). Click to select.
Entire conversation (4778 bytes)
Show data as ASCII
Stream 3
Find:
Find Next
Expression...
1 (application/x-www-form-urlencoded)
Packets: 425 · Displayed: 28 (6.6%)
Profile: Default