CS 646

Project Report

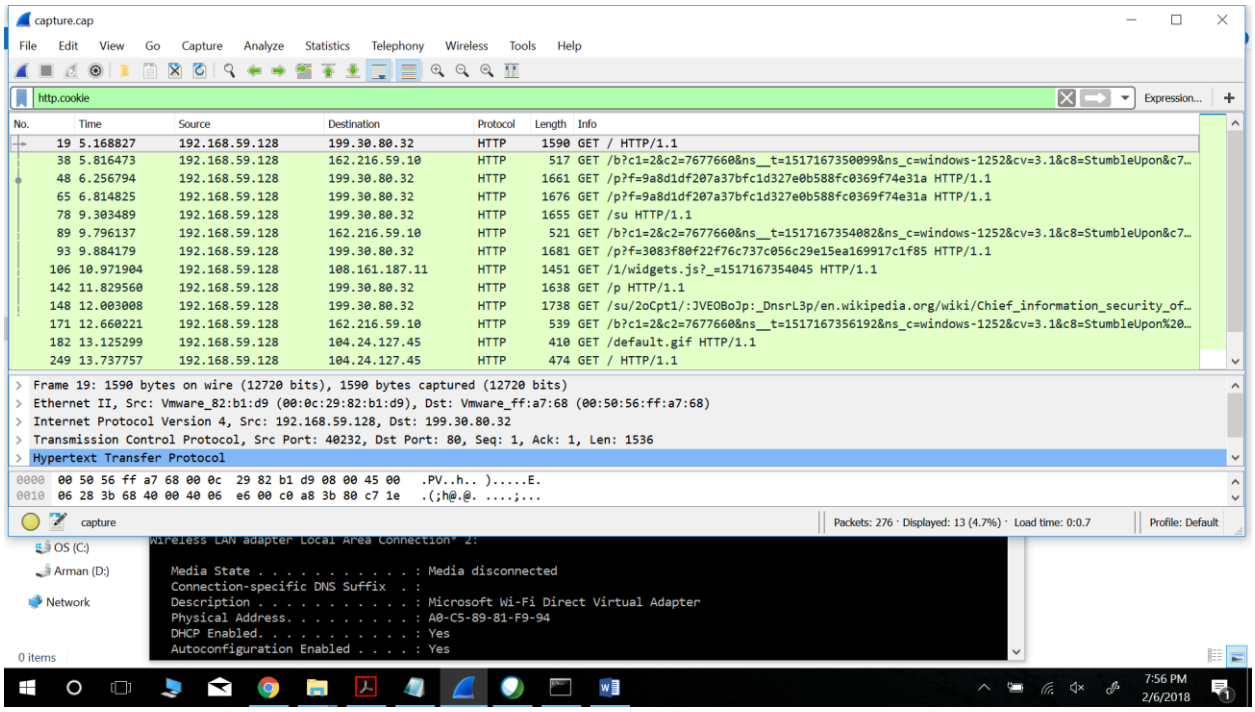
Problem 2 (Cookie Hijacking Attack)

- **Arman gupta (ag986)**
- **Adhithya sivanesh (as3423)**
- **Ketaki kakade (kk524)**

Arman Gupta (ag986@njit.edu)

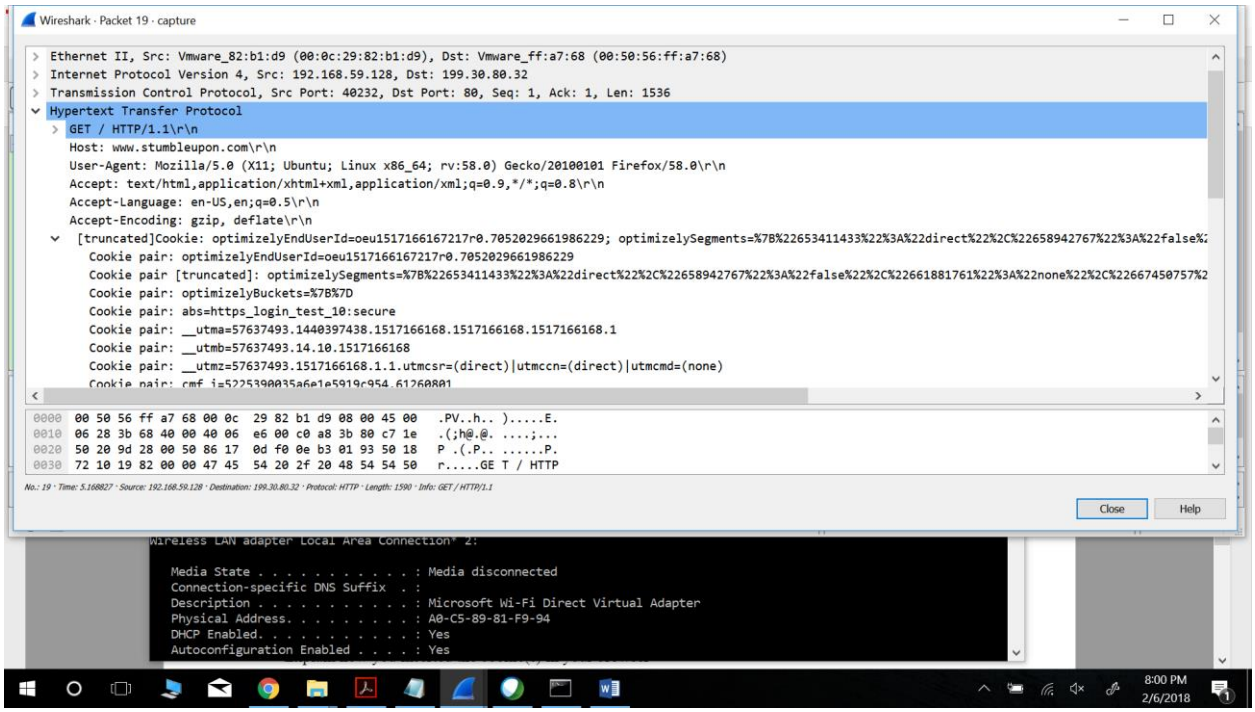
1. Finding packets that contain relevant cookies: -

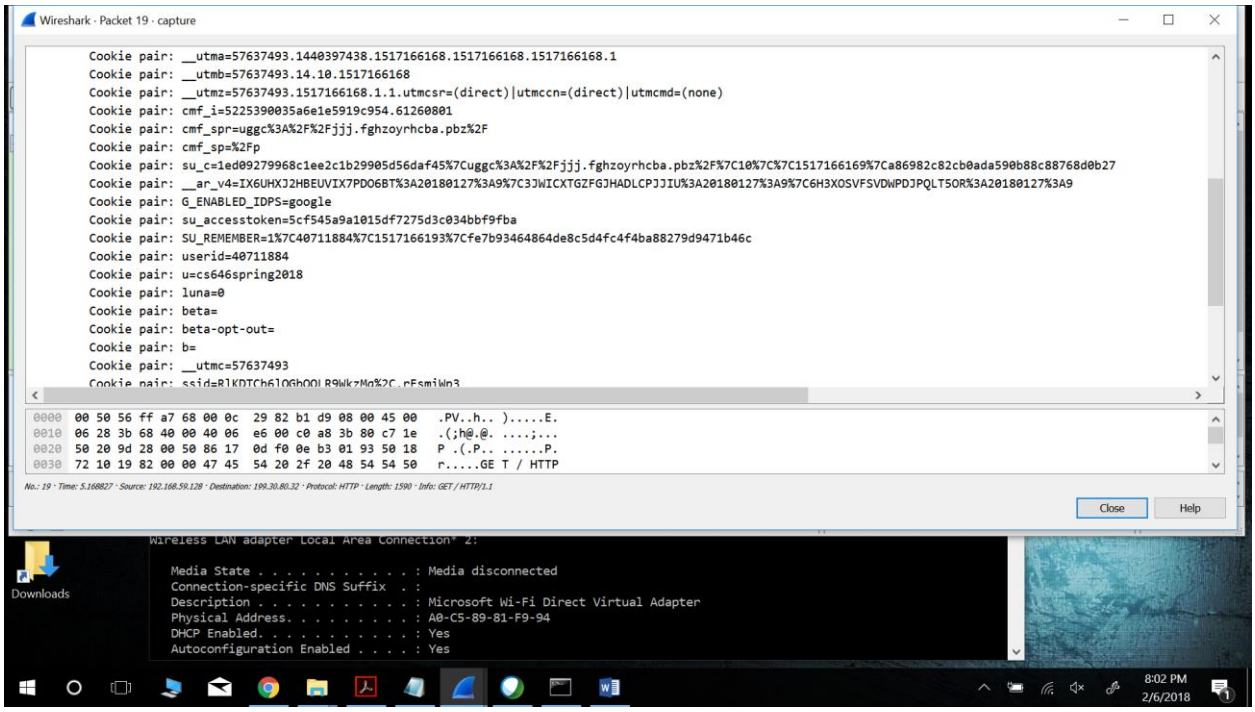
- Open capture.cap file in Wireshark
- Add “http.cookie” as a display filter to filter out the HTTP cookies
- Try selecting each sniffed packet which contains the relevant information such as “userid” or “username”
- Double click the first packet with the HTTP header



2. Packets that contain cookies with the relevant HTTP header: -

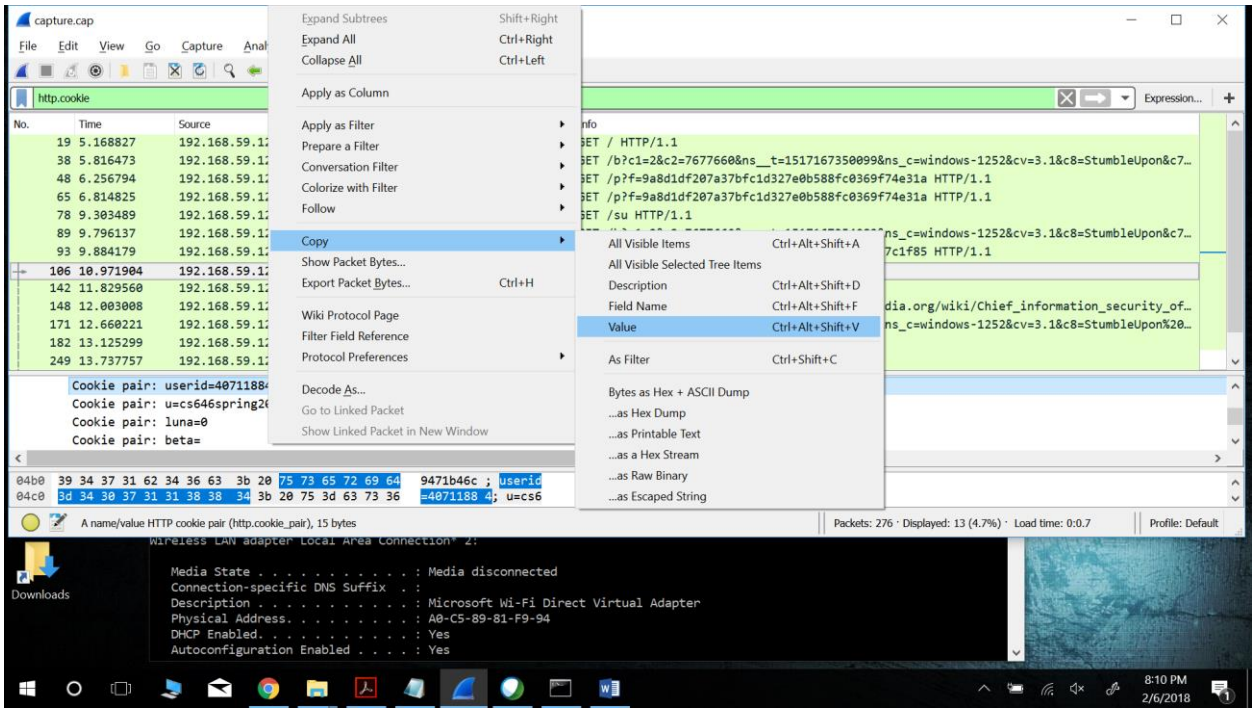
- Expand the header and search for the cookies
- Double click on the header which contains cookies

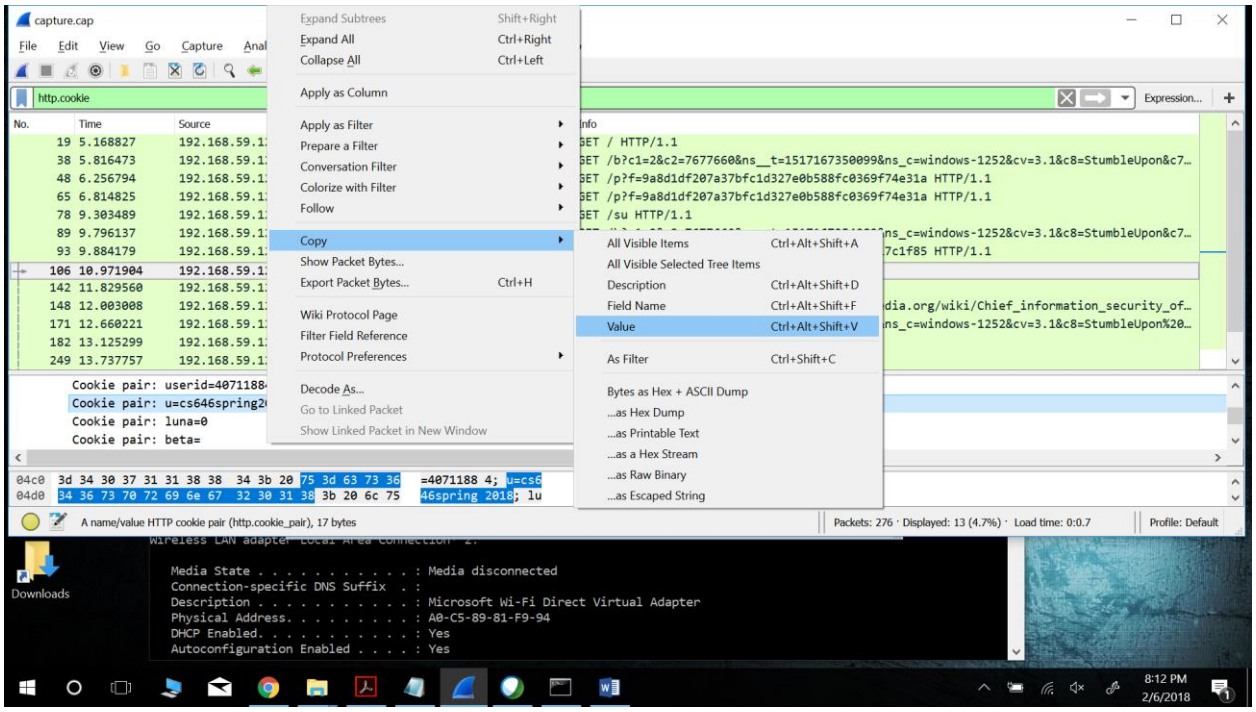


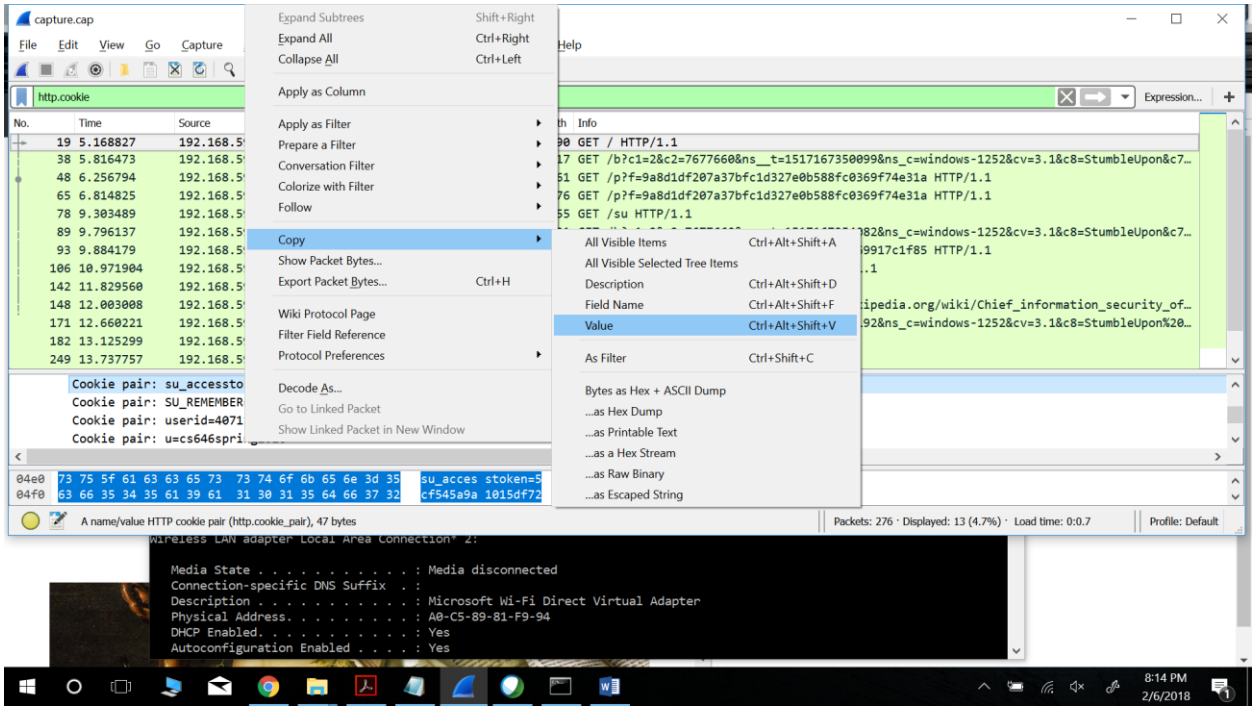


3. Extracting cookies from Wireshark: -

- Locate the fields “userid”, “u”, “su_accesstoken”
- Copy and paste the fields in the text editor one by one





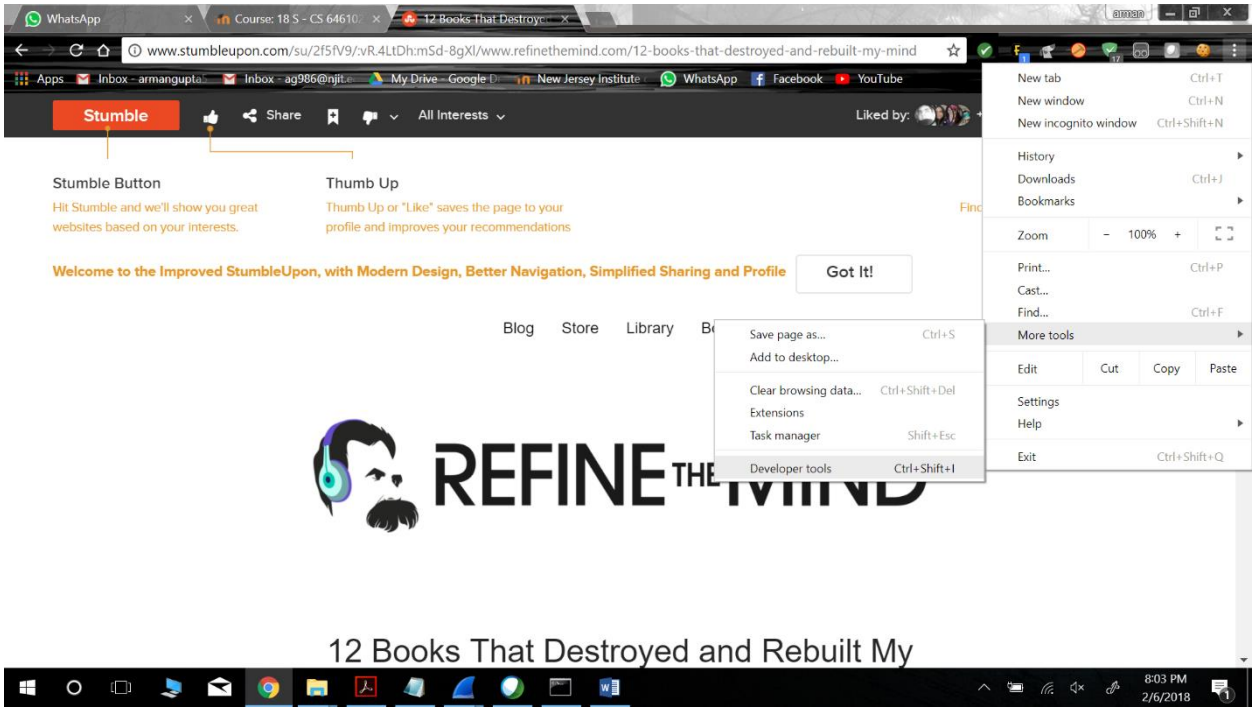


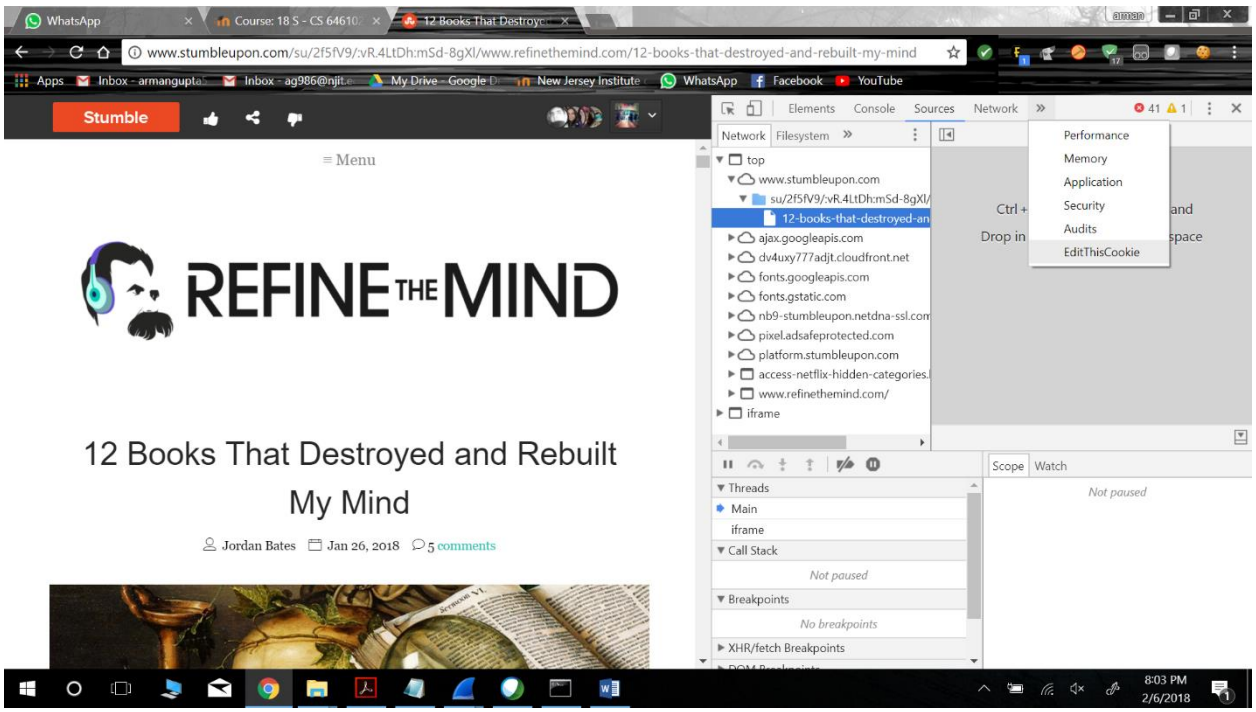
4. Cookies relevant and required for authentication: -

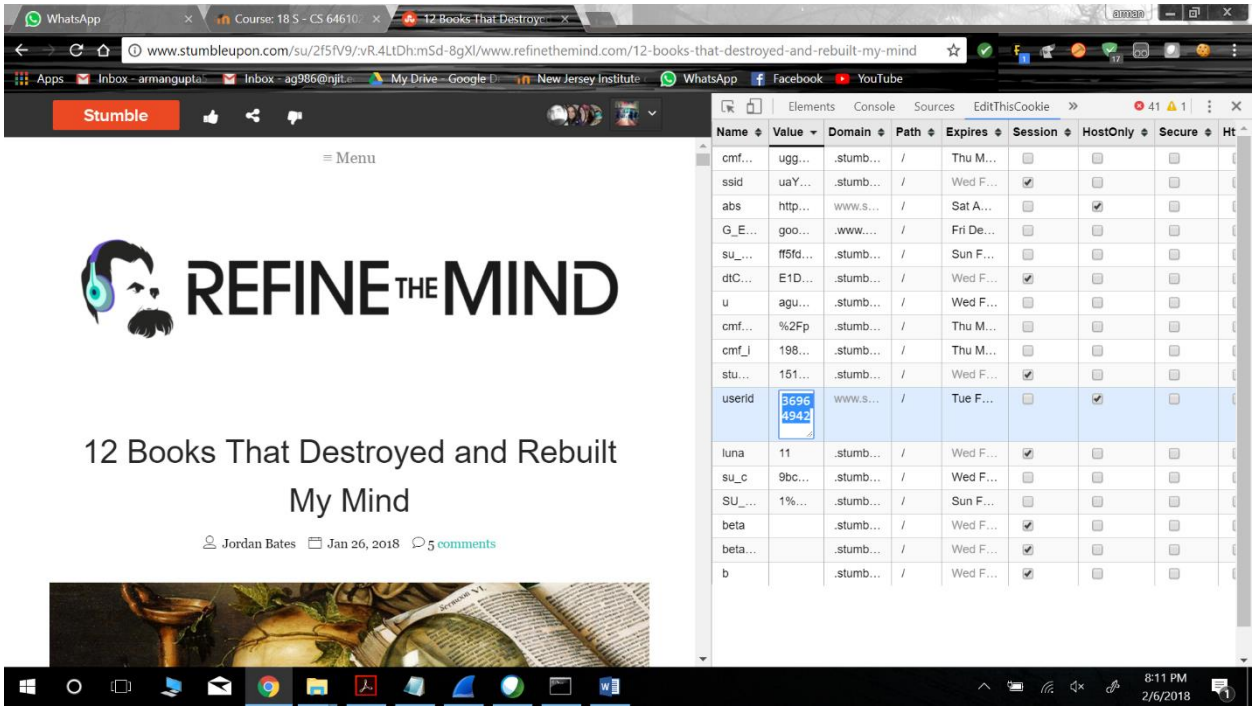
- “userid”, “u”, “su_accesstoken” are the cookies required for authentication

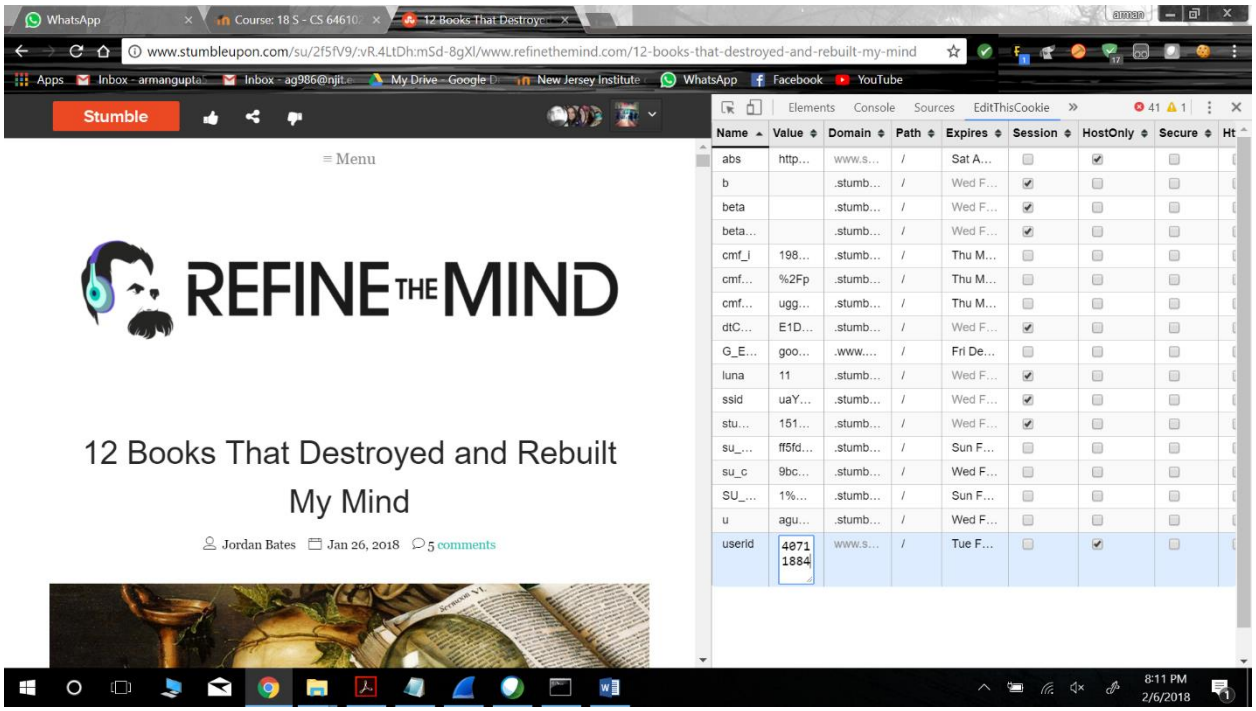
5. Inserting cookies in the browser: -

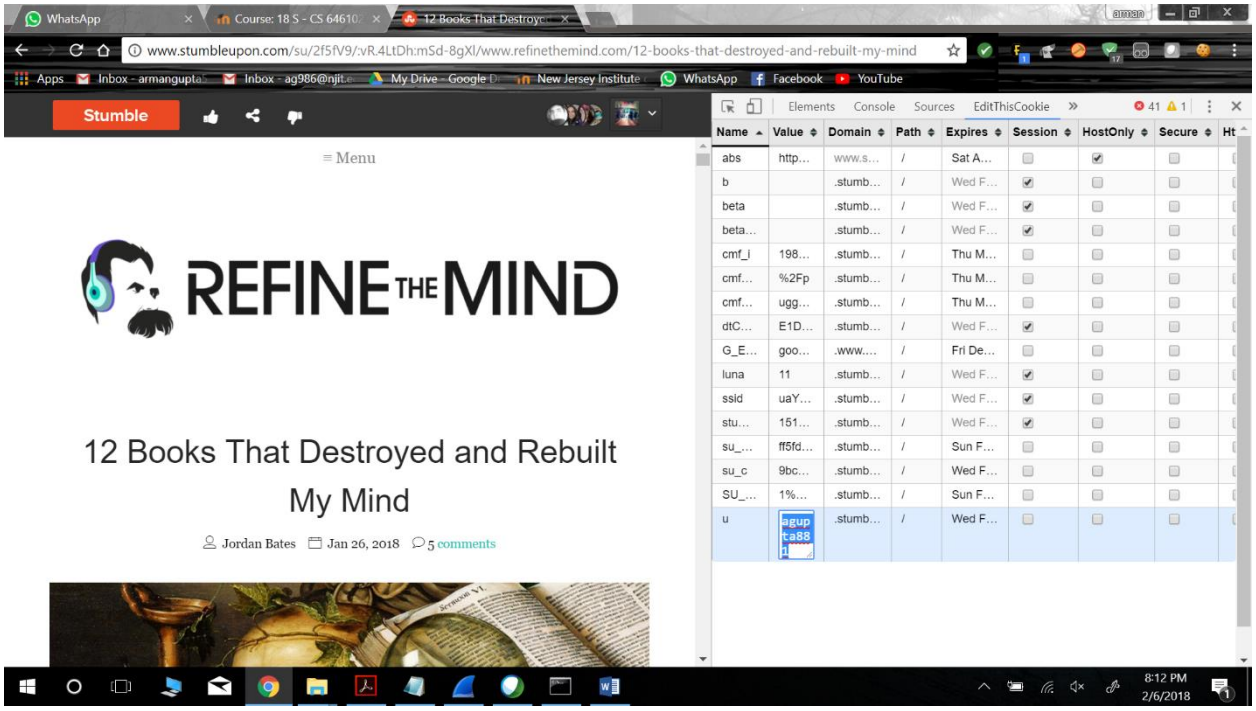
- Go to options in the web browser
- Look for more tools and then to developer tools
- Find an option to “Edit this cookie”
- Change the desired fields of this cookie as copied from Wireshark
- Reload the page
- The account changes and ready to be used

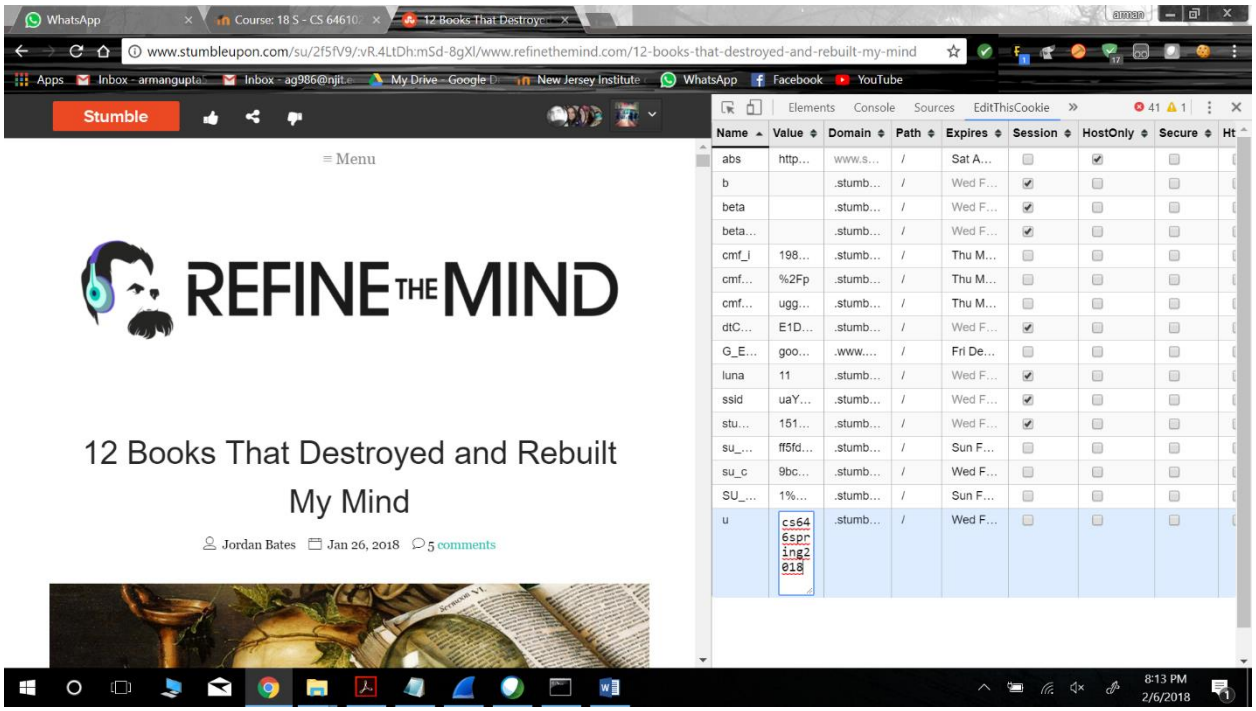


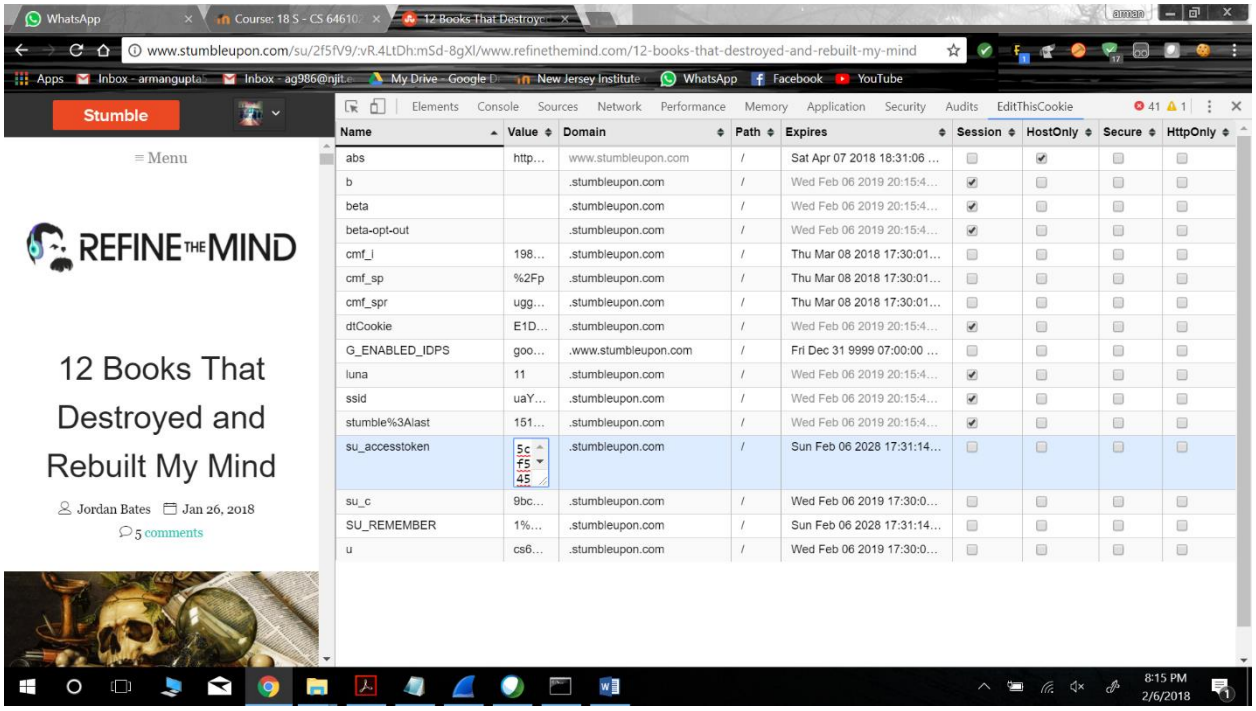



WhatsApp
Course: 18 S - CS 64610
12 Books That Destroyed
www.stumbleupon.com/su/2f5fV9/:vR.4LtDh:mSd-8gXl/www.refinethemind.com/12-books-that-destroyed-and-rebuilt-my-mind
Apps
Inbox - armangupta
Inbox - ag986@njit.e
My Drive - Google D
New Jersey Institute
WhatsApp
Facebook
YouTube
Stumble
Menu
REFINE THE MIND
12 Books That Destroyed and Rebuilt My Mind
Jordan Bates
Jan 26, 2018
5 comments
Elements
Console
Sources
EditThisCookie
Name
Value
Domain
Path
Expires
Session
HostOnly
Secure
userid
8:11 PM
2/6/2018


WhatsApp
Course: 18 S - CS 64610
12 Books That Destroyed
www.stumbleupon.com/su/2f5fV9/:vR.4LtDh:mSd-8gXl/www.refinethemind.com/12-books-that-destroyed-and-rebuilt-my-mind
Apps
Inbox - armangupta
Inbox - ag986@njit.e
My Drive - Google D
New Jersey Institute
WhatsApp
Facebook
YouTube
Stumble
Menu
REFINE THE MIND
12 Books That Destroyed and Rebuilt My Mind
Jordan Bates
Jan 26, 2018
5 comments
Elements
Console
Sources
EditThisCookie
Name
Value
Domain
Path
Expires
Session
HostOnly
Secure
userid
8:11 PM
2/6/2018

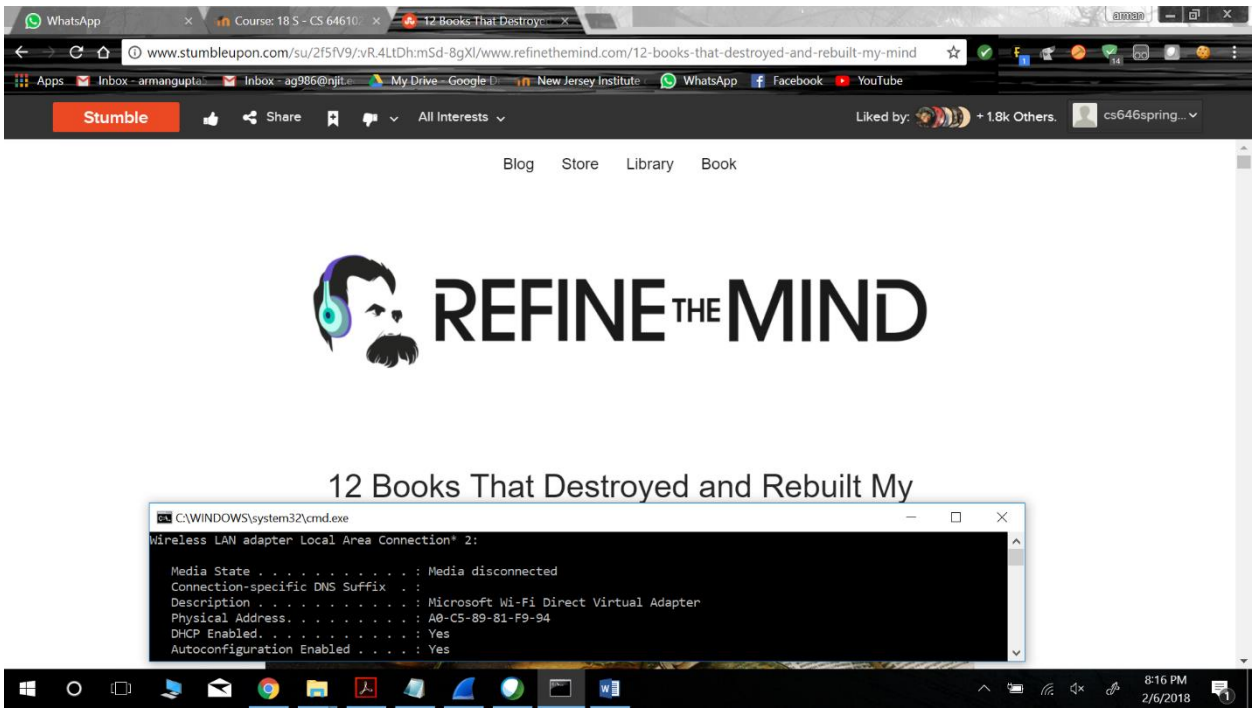

WhatsApp
Course: 18 S - CS 64610
12 Books That Destroyed
www.stumbleupon.com/su/2f5fV9/:vR.4LtDh:mSd-8gXl/www.refinethemind.com/12-books-that-destroyed-and-rebuilt-my-mind
Apps
Inbox - armangupta
Inbox - ag986@njit.e
My Drive - Google D
New Jersey Institute
WhatsApp
Facebook
YouTube
Stumble
Menu
REFINE THE MIND
12 Books That Destroyed and Rebuilt My Mind
Jordan Bates
Jan 26, 2018
5 comments
Elements
Console
Sources
EditThisCookie
Name
Value
Domain
Path
Expires
Session
HostOnly
Secure
abs
b
beta
cmf_l
cmf...
dtC...
G_E...
luna
ssid
stu...
su_...
su_c
SU_...
u
agupta881
8:12 PM
2/6/2018

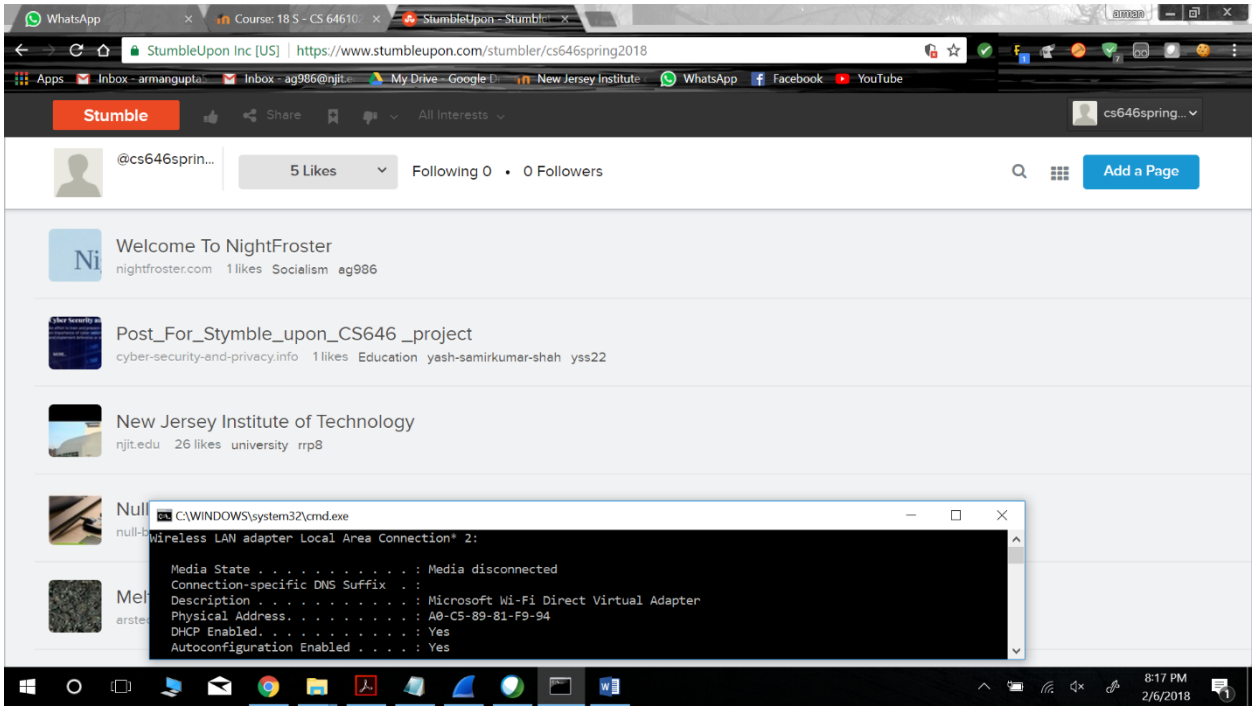

WhatsApp
Course: 18 S - CS 64610
12 Books That Destroyed
www.stumbleupon.com/su/2f5fV9/:vR.4LtDh:mSd-8gXl/www.refinethemind.com/12-books-that-destroyed-and-rebuilt-my-mind
Apps
Inbox - armangupta
Inbox - ag986@njit.e
My Drive - Google D
New Jersey Institute
WhatsApp
Facebook
YouTube
Stumble
Menu
REFINE THE MIND
12 Books That Destroyed and Rebuilt My Mind
Jordan Bates
Jan 26, 2018
5 comments
Elements
Console
Sources
EditThisCookie
Name
Value
Domain
Path
Expires
Session
HostOnly
Secure
abs
b
beta
cmf_l
cmf...
dtC...
G_E...
luna
ssid
stu...
su_...
su_c
SU_...
u
cs646spring2018
8:13 PM
2/6/2018



6. Adding page to cs646spring2018 account: -

- Page added with a link by UCID “ag986”

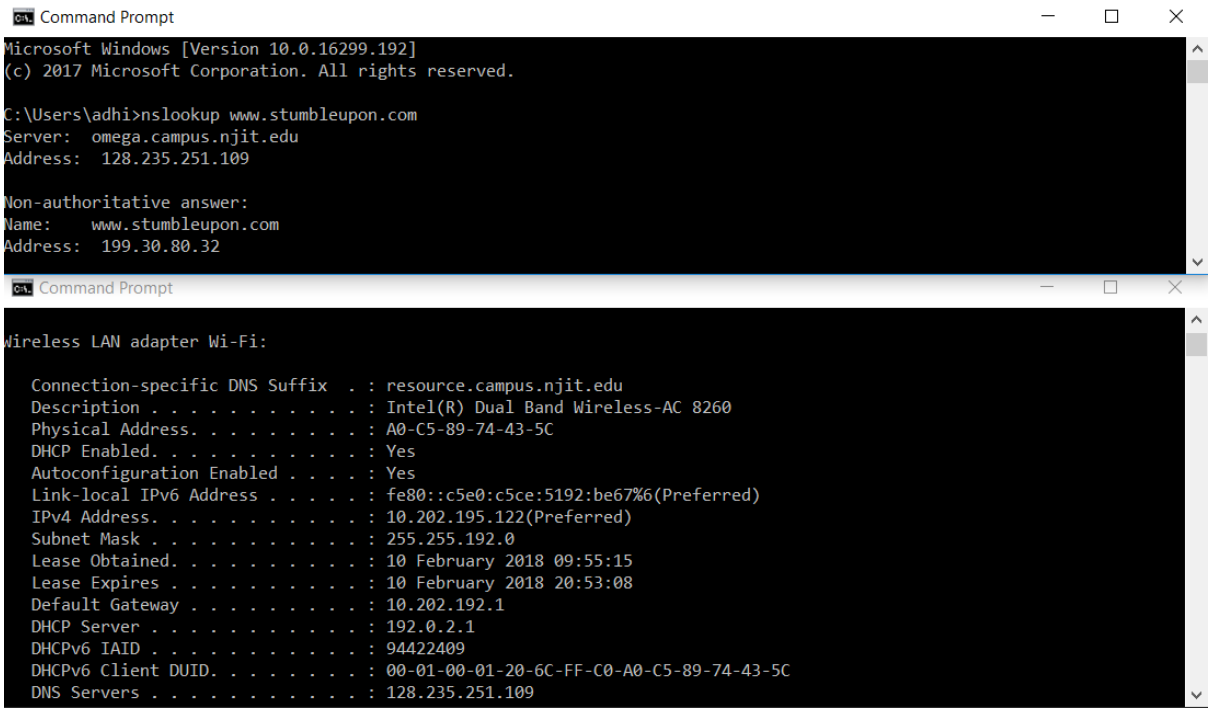



WhatsApp
Course: 18 S - CS 646
StumbleUpon - Stumble!
StumbleUpon Inc [US] | https://www.stumbleupon.com/stumbler/cs646spring2018
Apps
Inbox - armangupta
Inbox - ag986@njit.e
My Drive - Google D
New Jersey Institute
WhatsApp
Facebook
YouTube
Stumble
Share
All Interests
cs646spring...
@cs646sprin...
5 Likes
Following 0 • 0 Followers
Add a Page
Welcome To NightFroster
nightfroster.com 1 likes Socialism ag986
Post_For_Stymble_upon_CS646 _project
cyber-security-and-privacy.info 1 likes Education yash-samirkumar-shah yss22
New Jersey Institute of Technology
njit.edu 26 likes university rrp8
C:\WINDOWS\system32\cmd.exe
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : A0-C5-89-81-F9-94
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
8:17 PM
2/6/2018

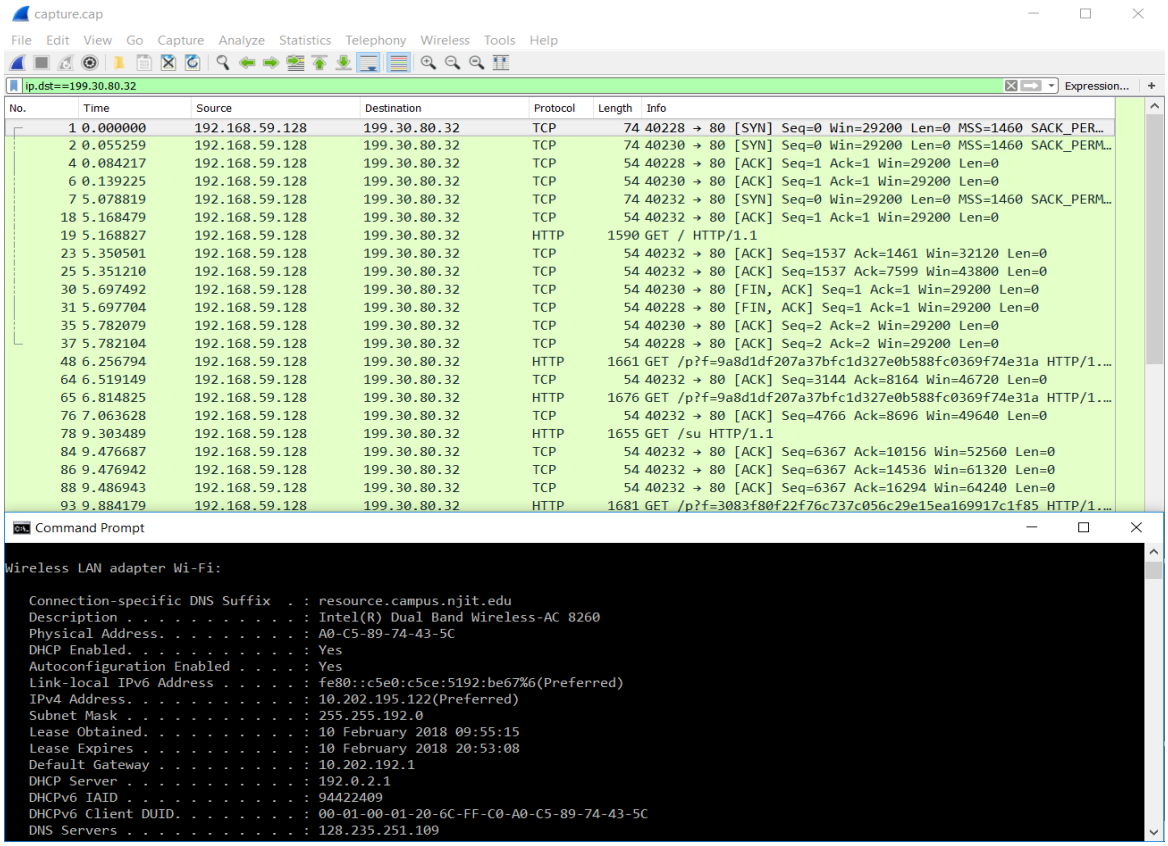
Adhithya Sivanesh(as3423@njit.edu)

Problem 2: Cookie hijacking attack

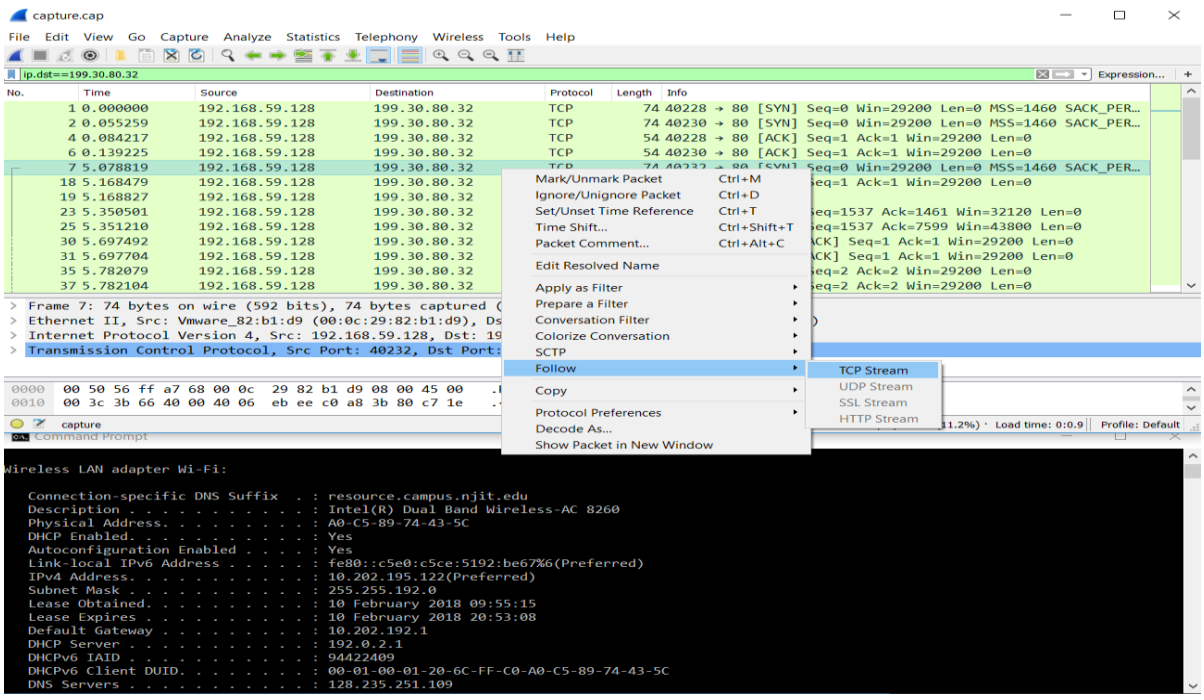
1] For this problem, the first step I took was to find out the ip address of www.stumbleupon.com. This was found out by using the nslookup command in cmd in my windows 10 machine.



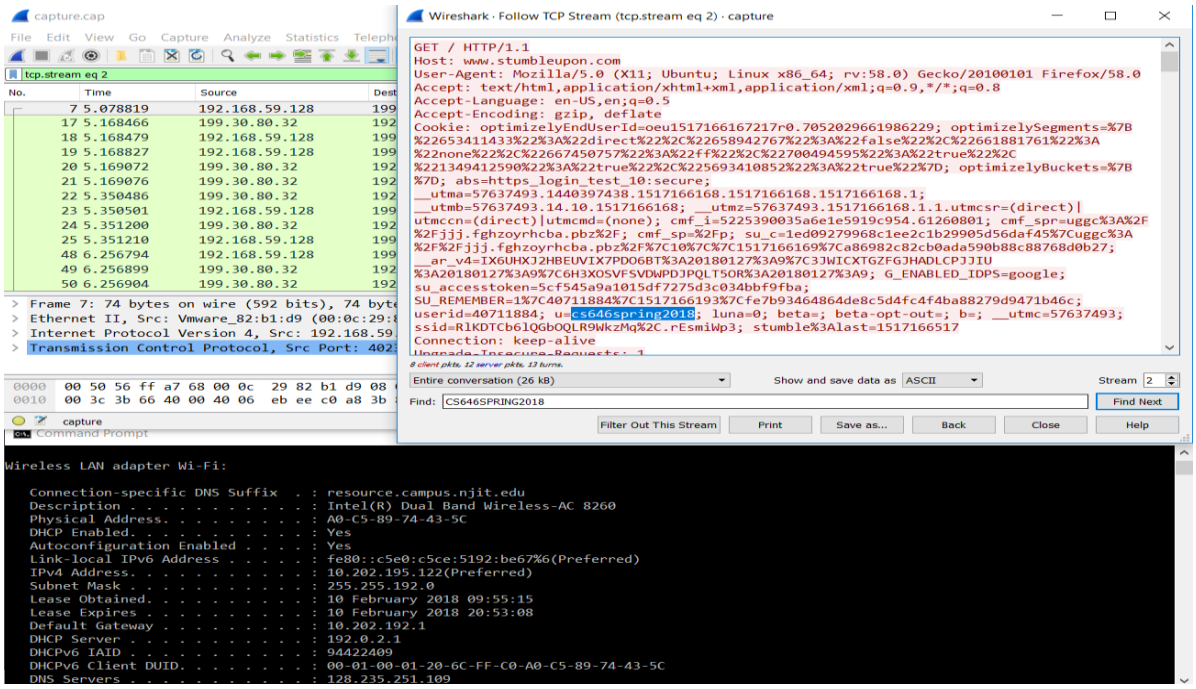
2] Then I opened the provided capture.cap file in Wireshark, applied a filter (ip.dst==199.30.80.32)



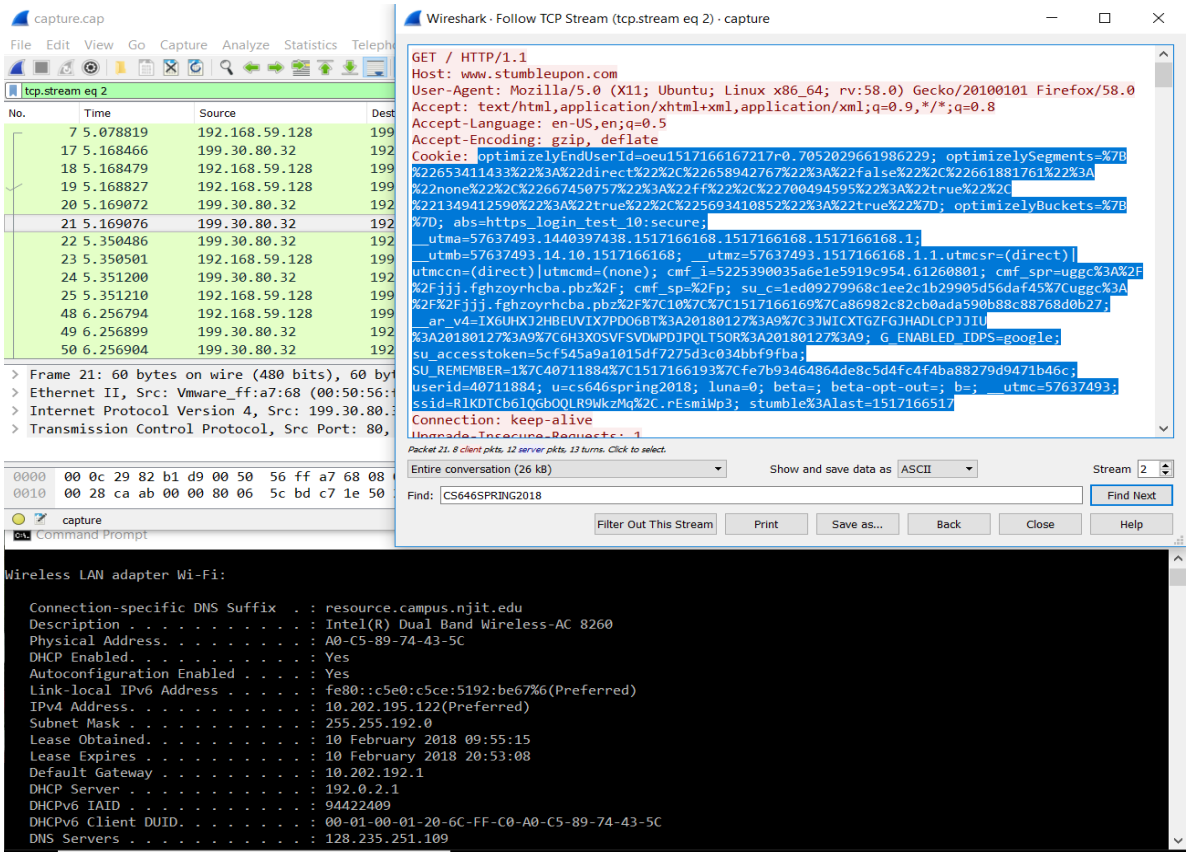
3] This filter displayed all the wireless traffic that was captured with destination ip address: (199.30.80.32), which is the ip address of www.stumbleupon.com . The next step was to inspect the captured packet. The inspection was done by right clicking on the packet and selecting “TCP Stream” from “follow” option in the menu as shown in the below diagram.



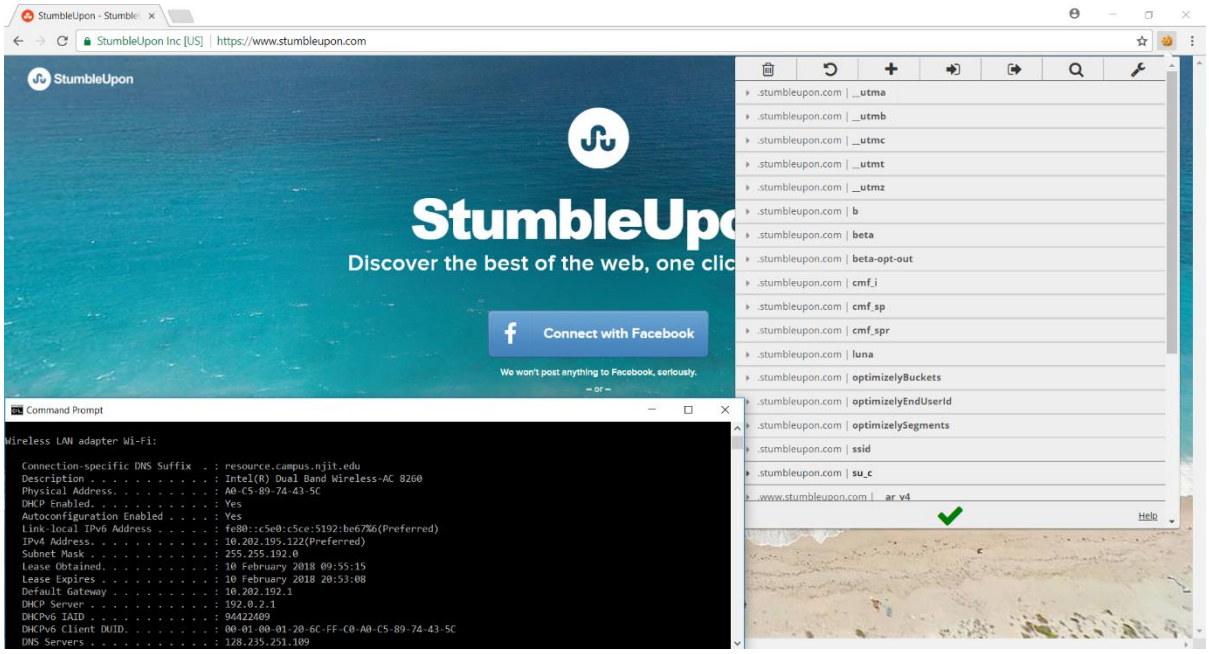
4] After selecting TCP Stream, search for “CS646SPRING2018” which is the username for the account. We will find the cookie as follows:



5] Now copy the cookie and download an add on for chrome called EditThisCookie.



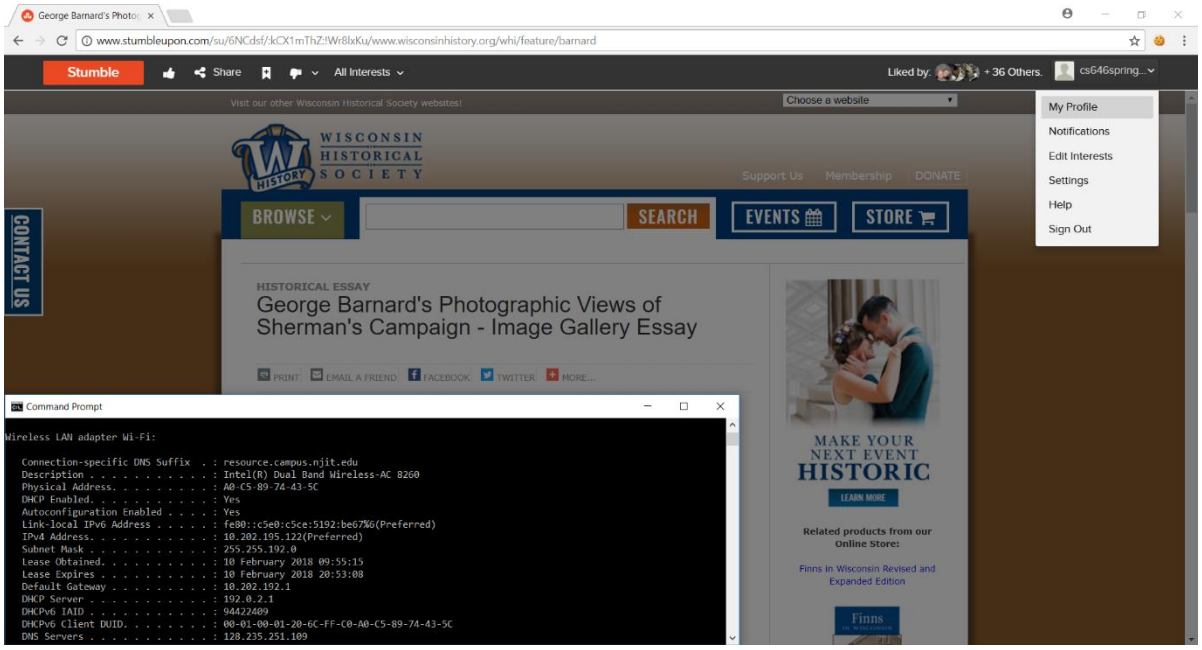
6] The next step is to go to www.stumbleupon.com in your chrome browser, and then open EditThisCookie to edit the cookie. Remove all the present cookies that are shown in the below screenshot.



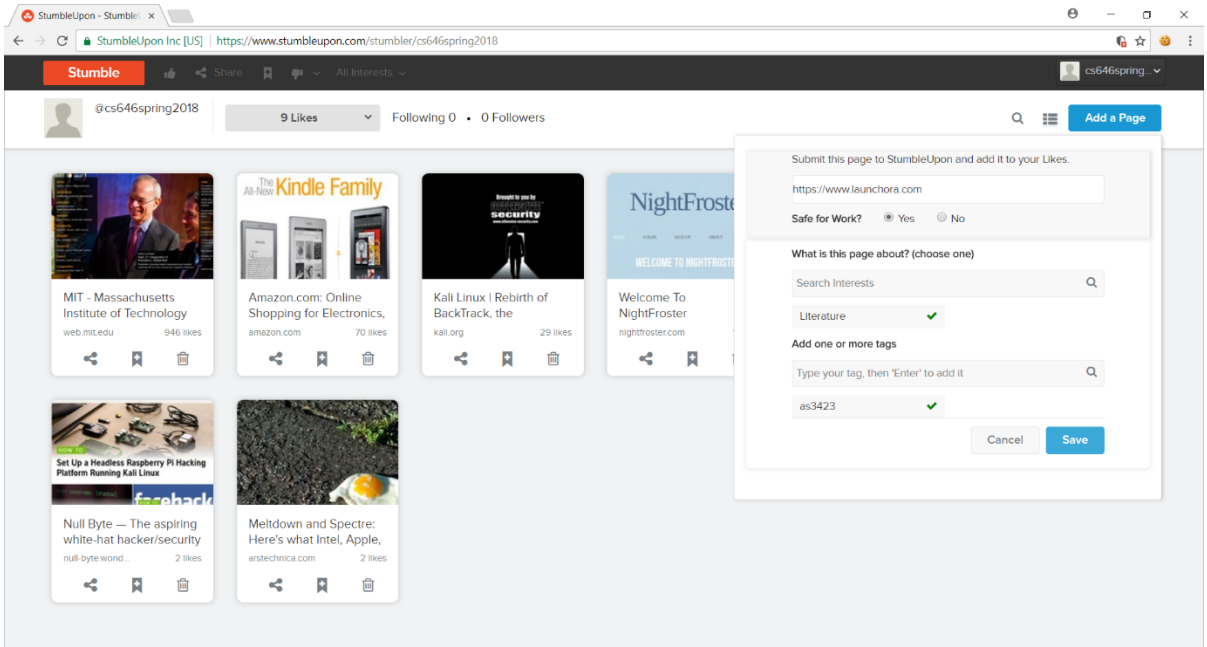
7] After removing all the present cookies, add the cookies as follows with a suitable expiration date:

su_accesstoken=5cf545a9a1015df7275d3c034bbf9fba;
u=cs646spring2018;
userid=40711884;
These cookies are enough to perform the authentication. This was found out by making a new account of my own and removing all other cookies and only keeping the fields for su_accesstoken, u, userid. I was able to access the account with just these cookie values.

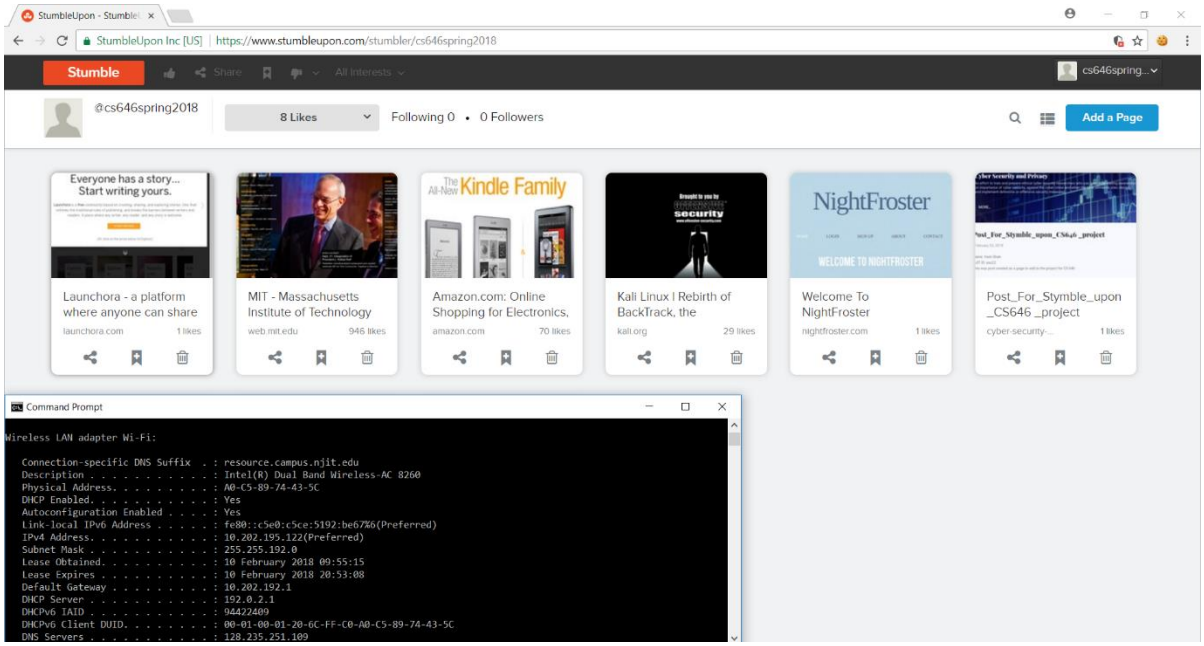
8) Now reload the page and you will see that you have successfully hijacked the account. Now click on "My Profile" button under the drop-down menu on the right side.



9] After clicking on the "Add Page" button on the top right side of the profile, added a page https://www.launchora.com with tag of "as3423".



10] Now reload the page and you can see that the entry for https://www.launchora.com has been added to the page.



This shows that an account could be hijacked if the cookies are send in plain text and were captured by an eavesdropper.

Ketaki Kakade(kk524@njit.edu)

Problem 2: Cookie Hijacking Attack

Step 1:

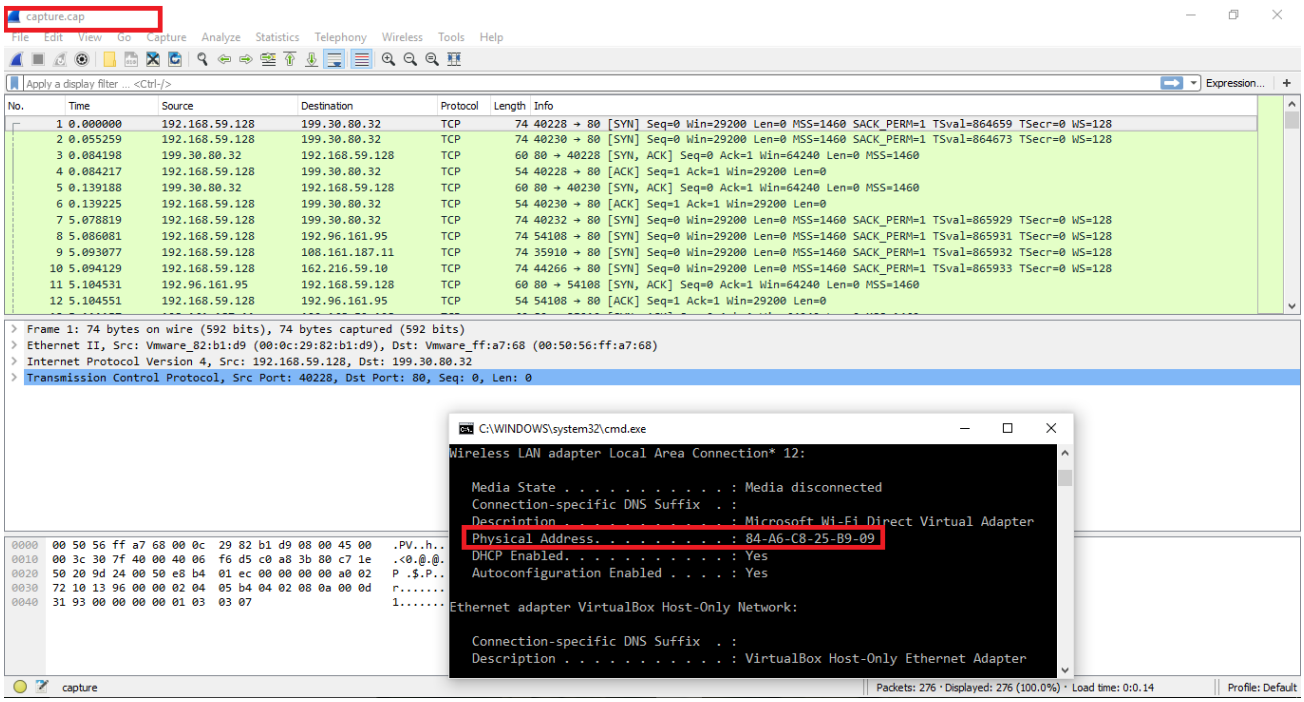
For the cookie hijacking attack, first create an account on Stumleupon.com with your own credentials.

Screenshot – 1

Screenshot – 2

Step 2:

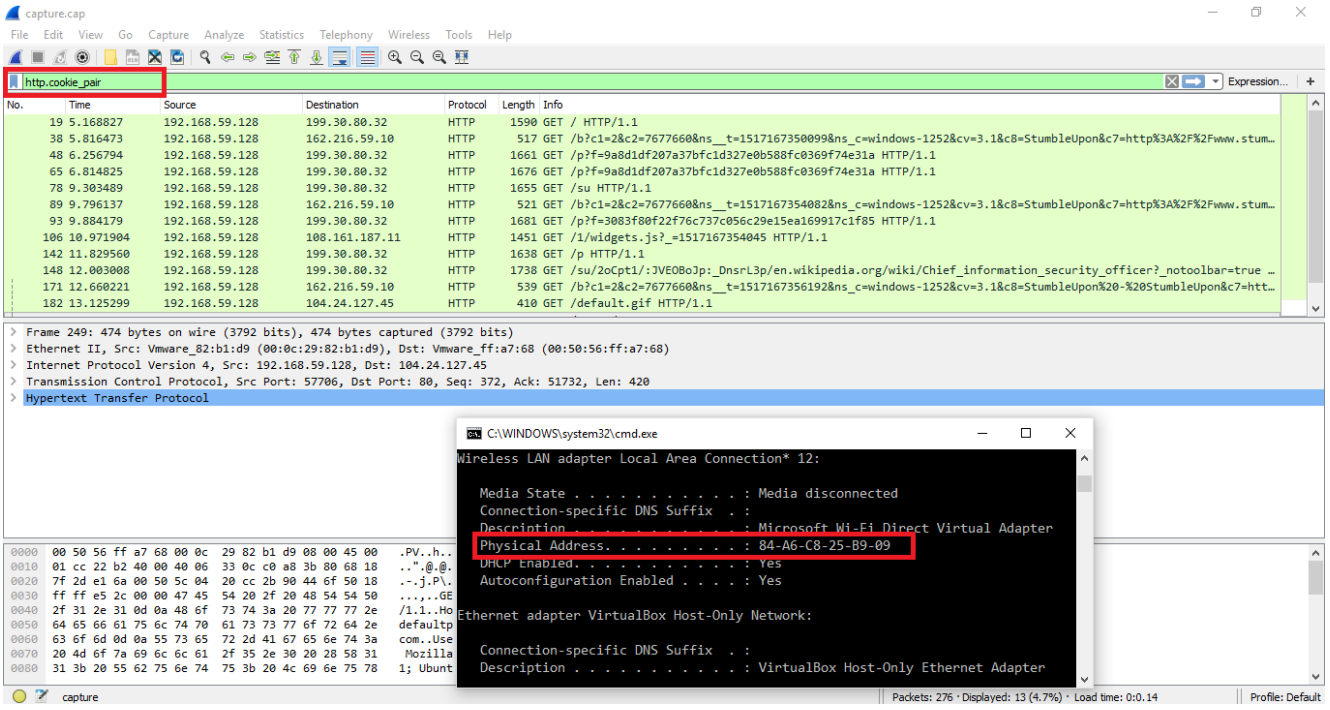
Open the capture.cap file in wireshark which contains wireless traffic captured when a client connected to the website www.stumbleupon.com over an insecure wireless connection.



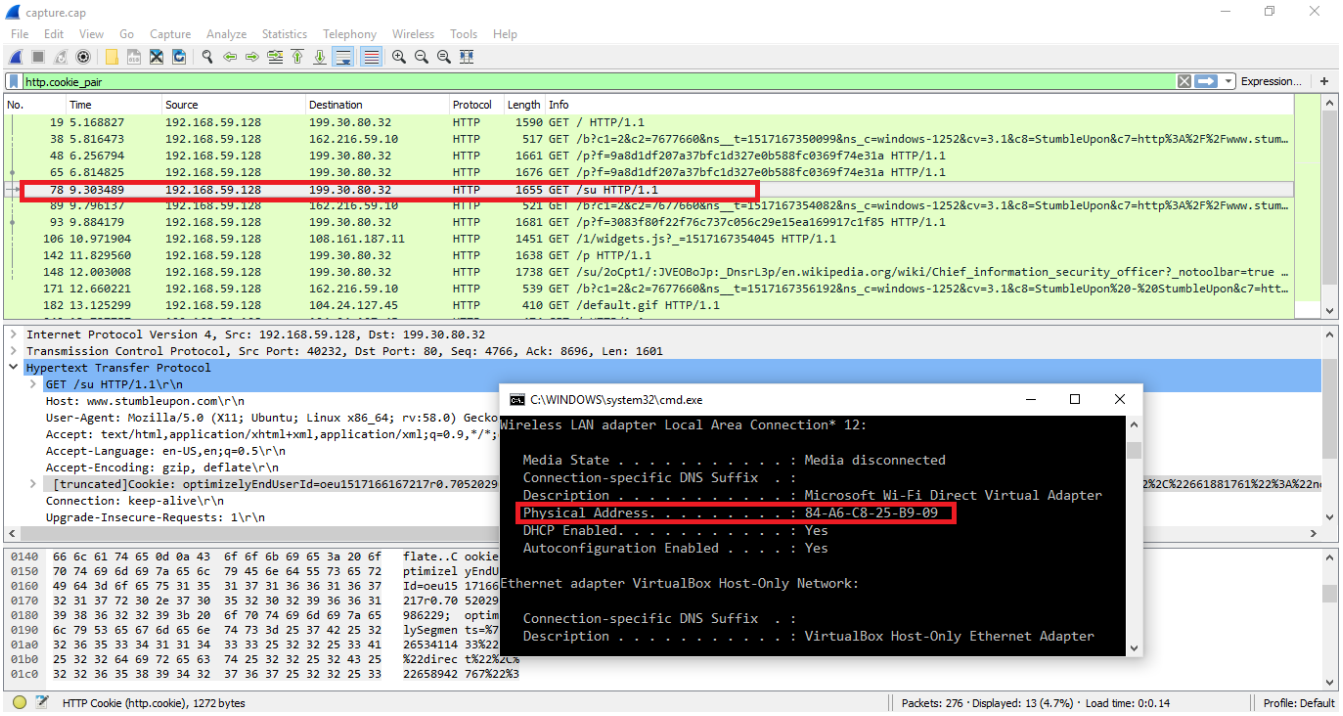
Screenshot – 3

Step 3:

Apply the wireshark filter for analyzing only http cookies- http.cookie_pair.



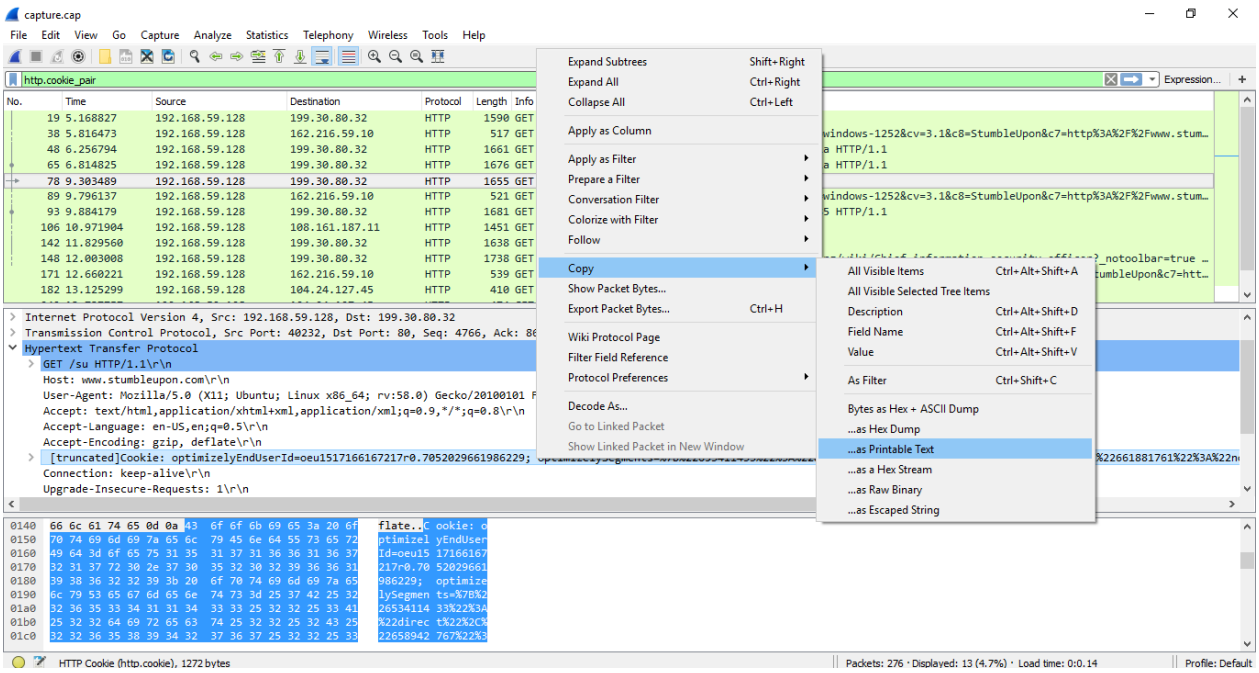
Screenshot – 4



Screenshot – 5

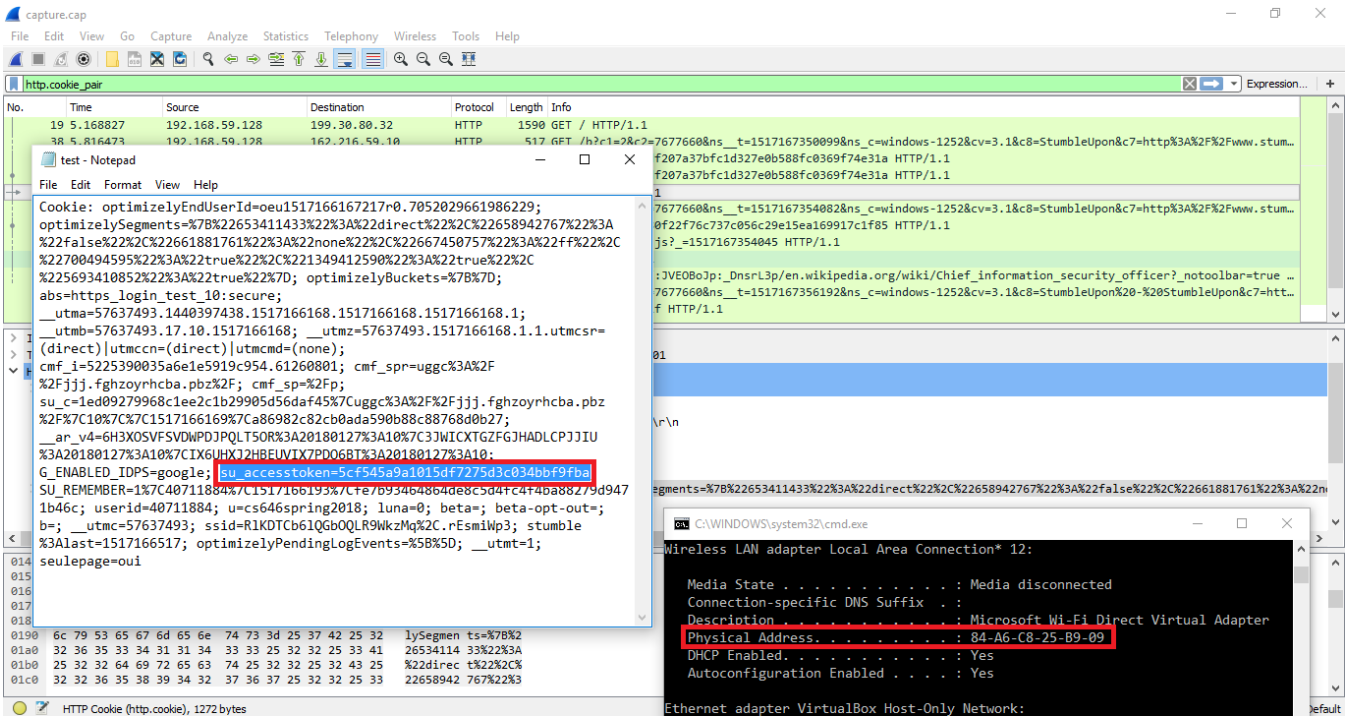
Step 4:

Copy the cookie as a printable text.



Screenshot - 6

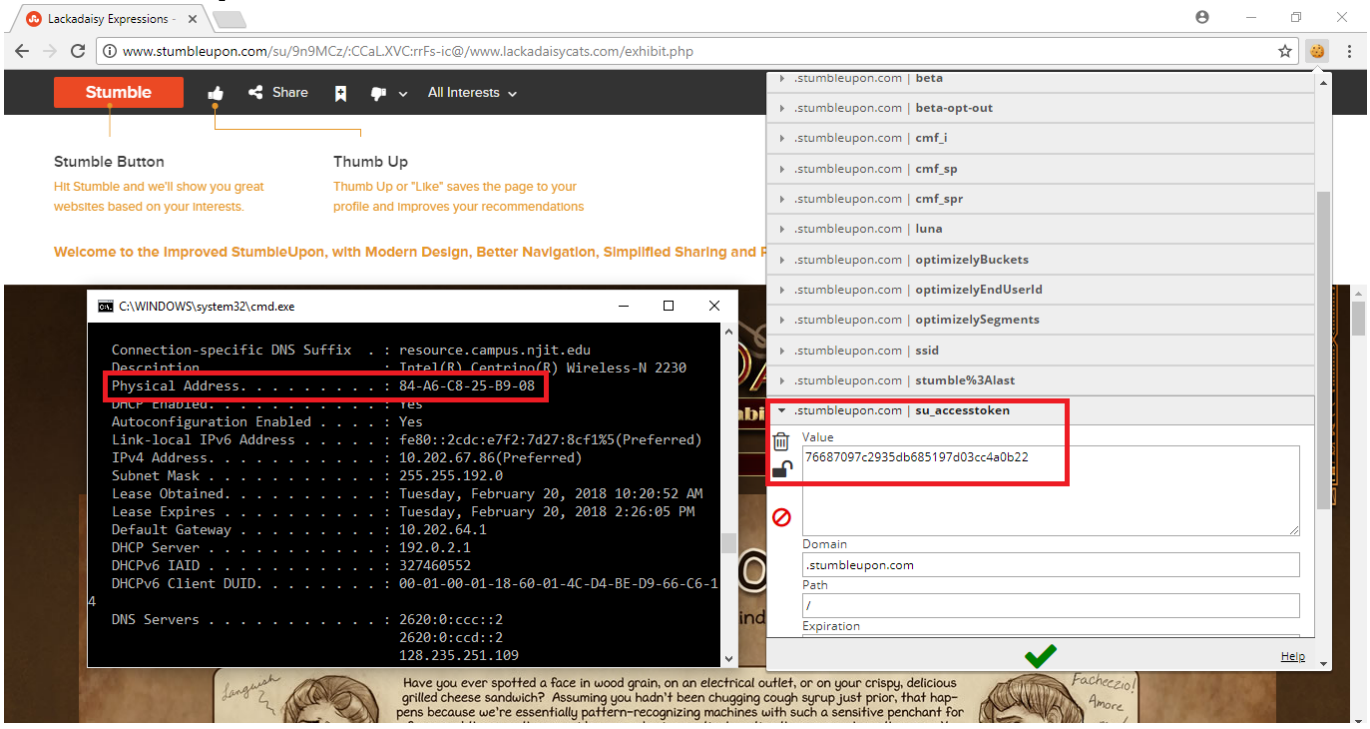
Look for “**su_accesstoken**” which gives access to the victim’s account and its value when the cookie is copied to a text editor.



Screenshot – 7

Step 5:

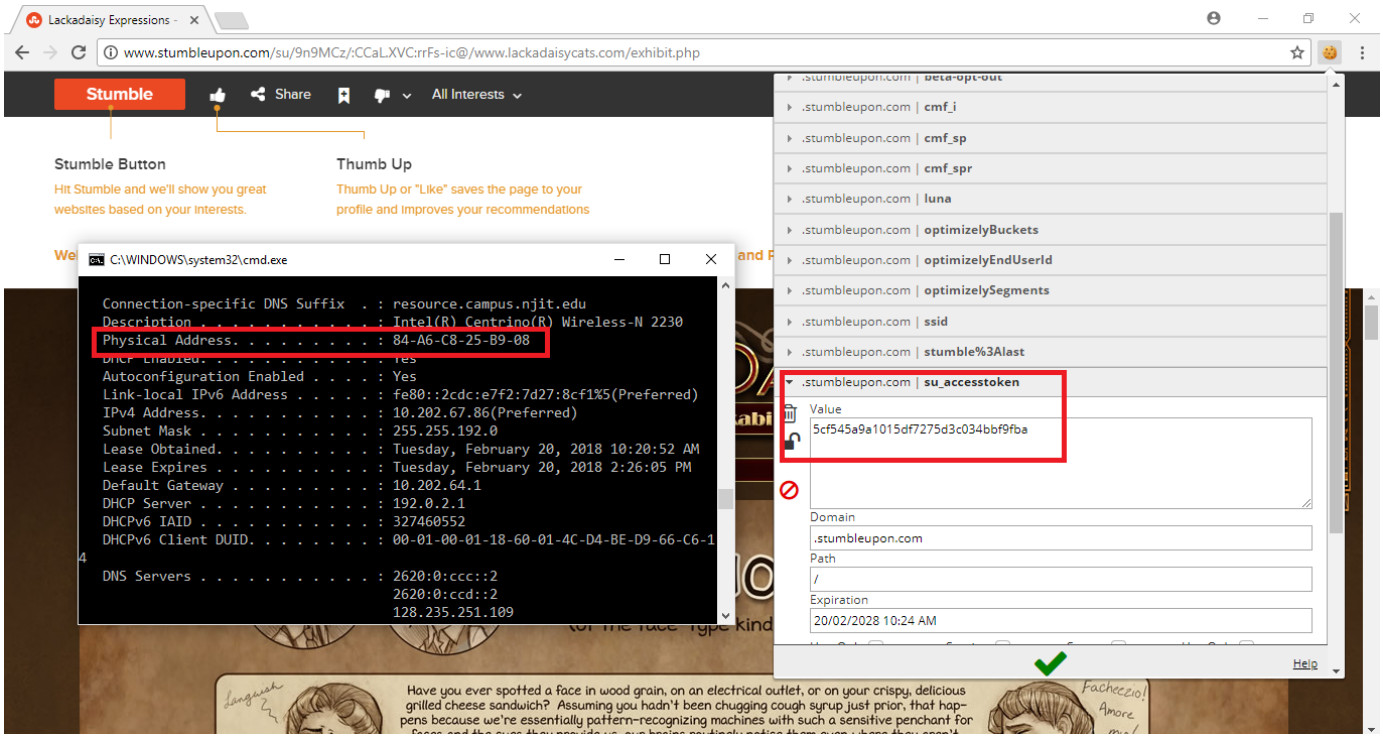
For this type of cookie hijacking we make use of the chrome plugin called **“Edit this cookie”.** This plugin gives us a simplified look at the cookies created for the website and also enables us to easily edit them. Now, look for “**su_accesstoken**” field. This will show the accesstoken for our login account which will have its unique value.



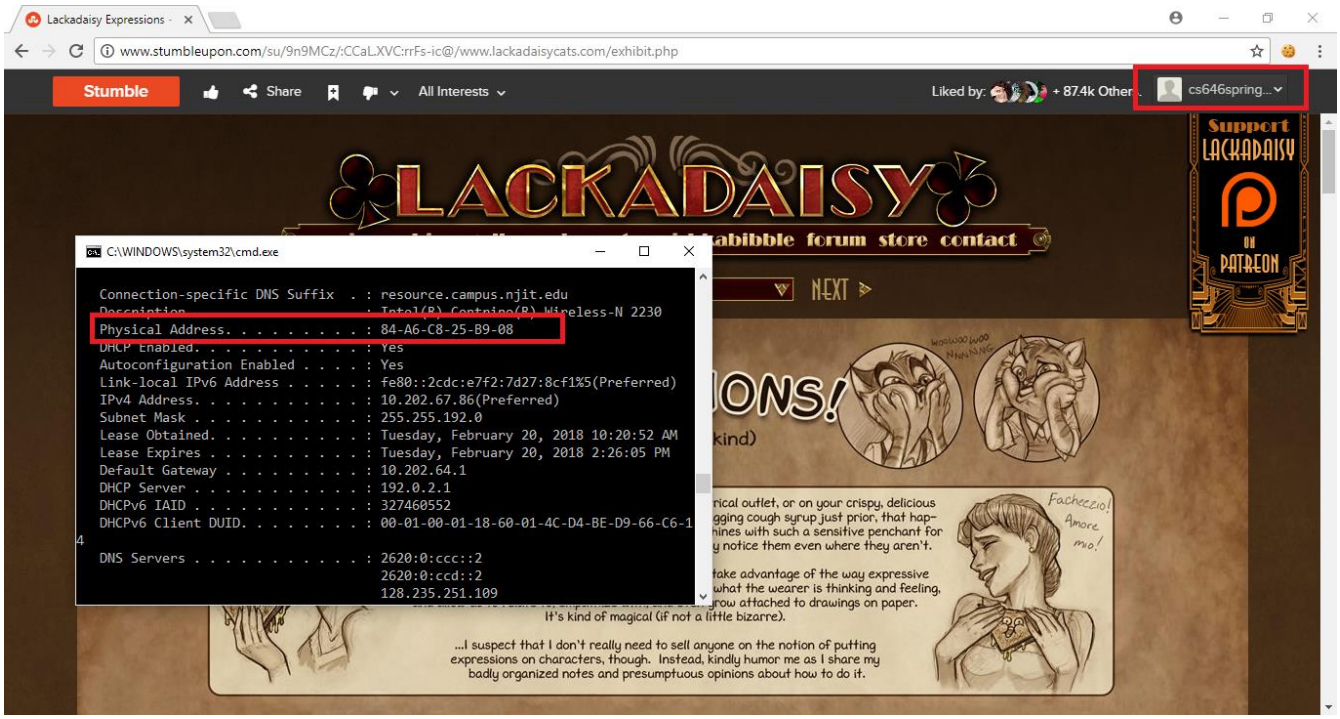
Screenshot – 8

Step 6:

Replace this token value of our **su_accesstoken** in our account with the **su_accesstoken** value from the capture.cap file's cookie and refresh the web page. You will now be logged in as victim's account.



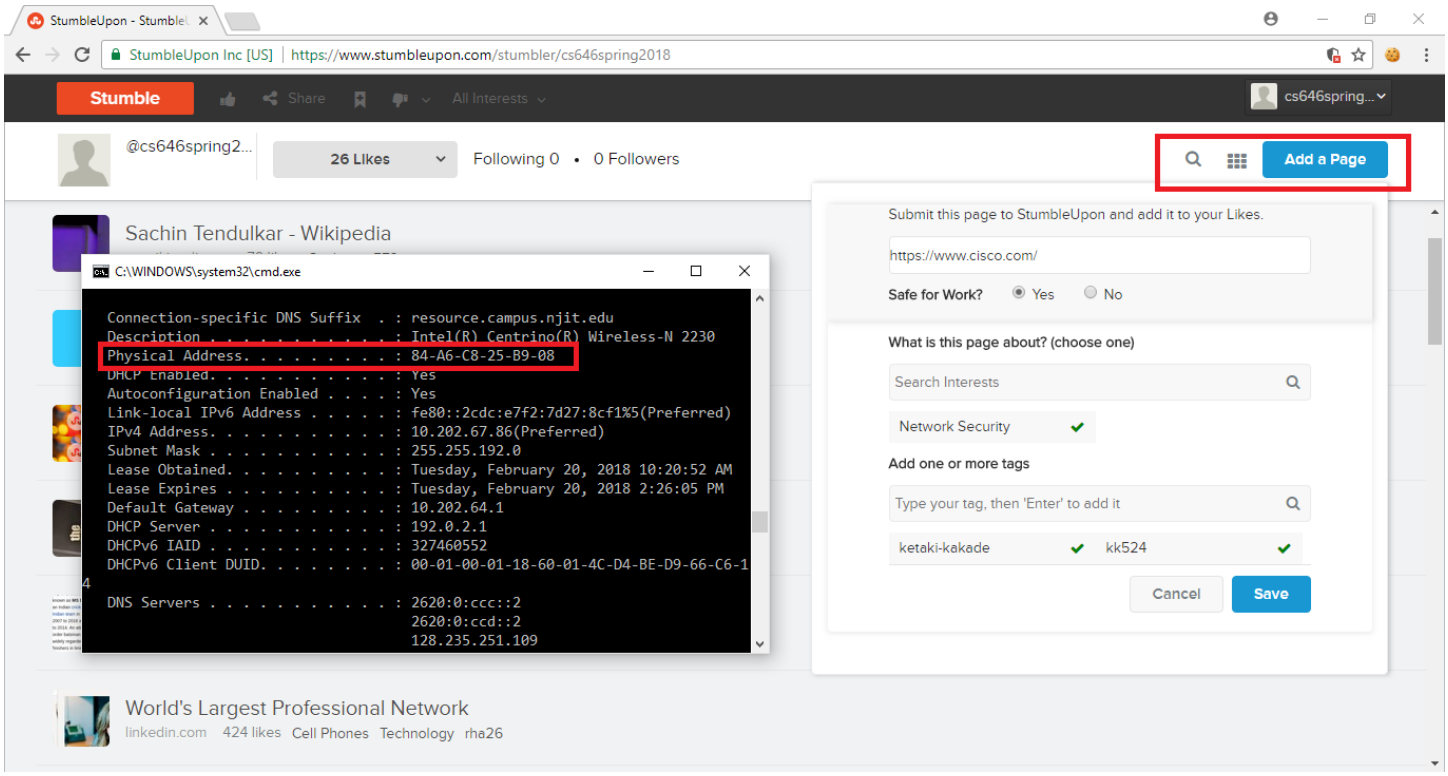
Screenshot – 9



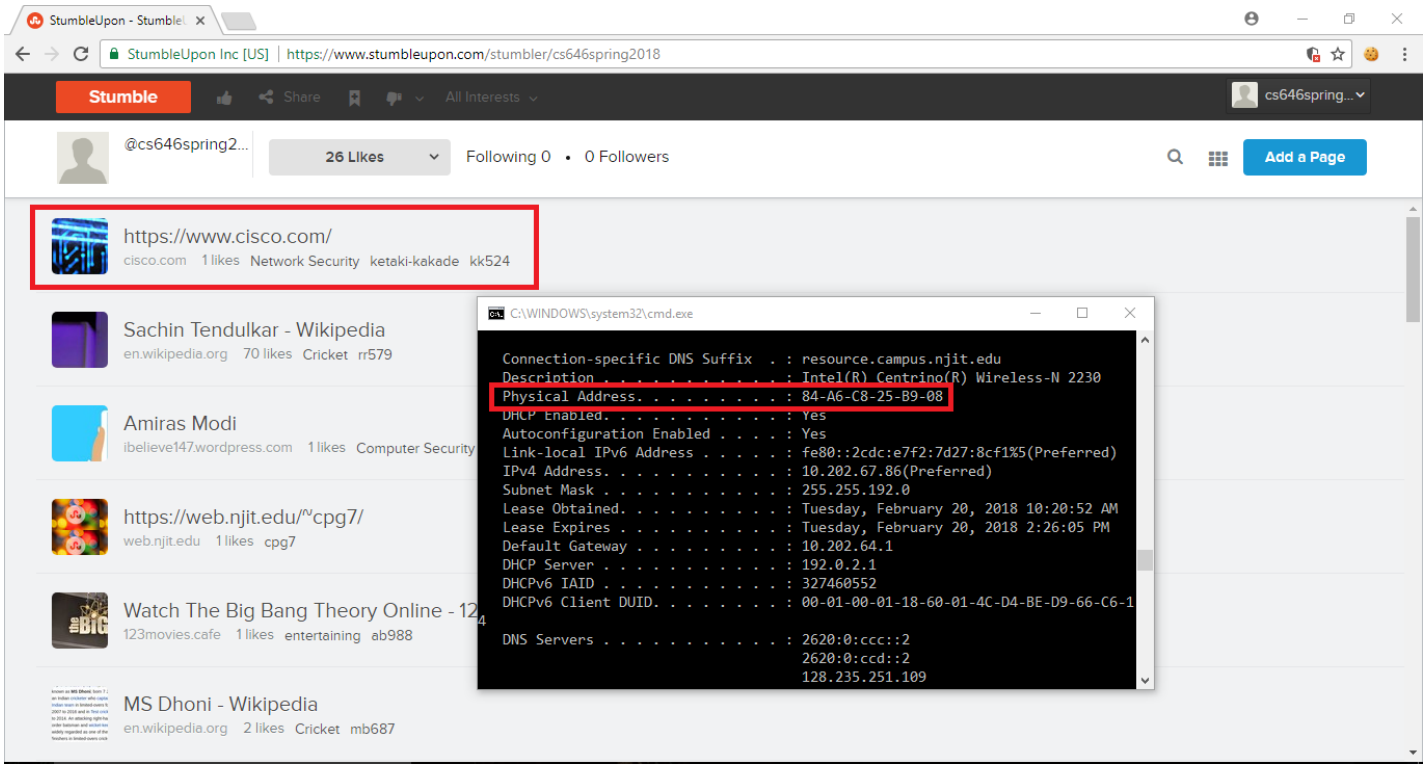
Screenshot – 10

Step 7:

Go to “My Profile” and select “add a page”. Fill in the website, write a small description of the page and all the tags you want to add to the page and select save.



Screenshot – 11



Screenshot -12