

**CS 646**

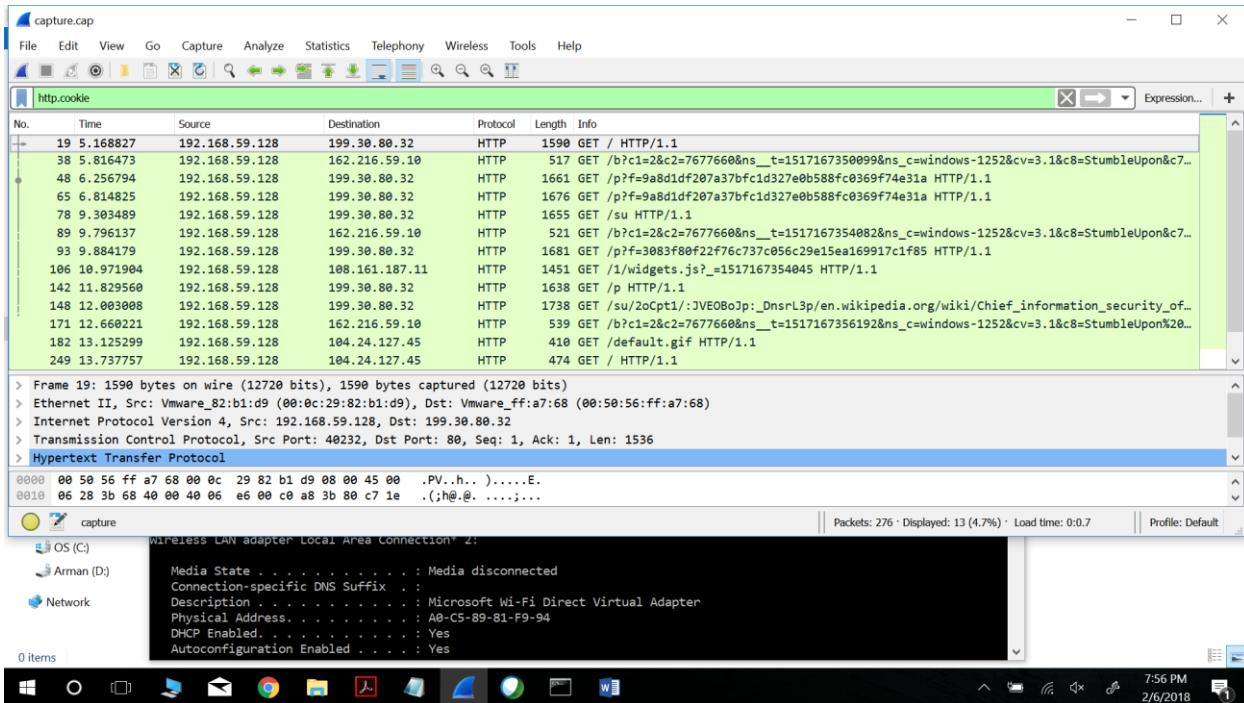
**Project Report**

**Problem 2 (Cookie Hijacking Attack)**

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

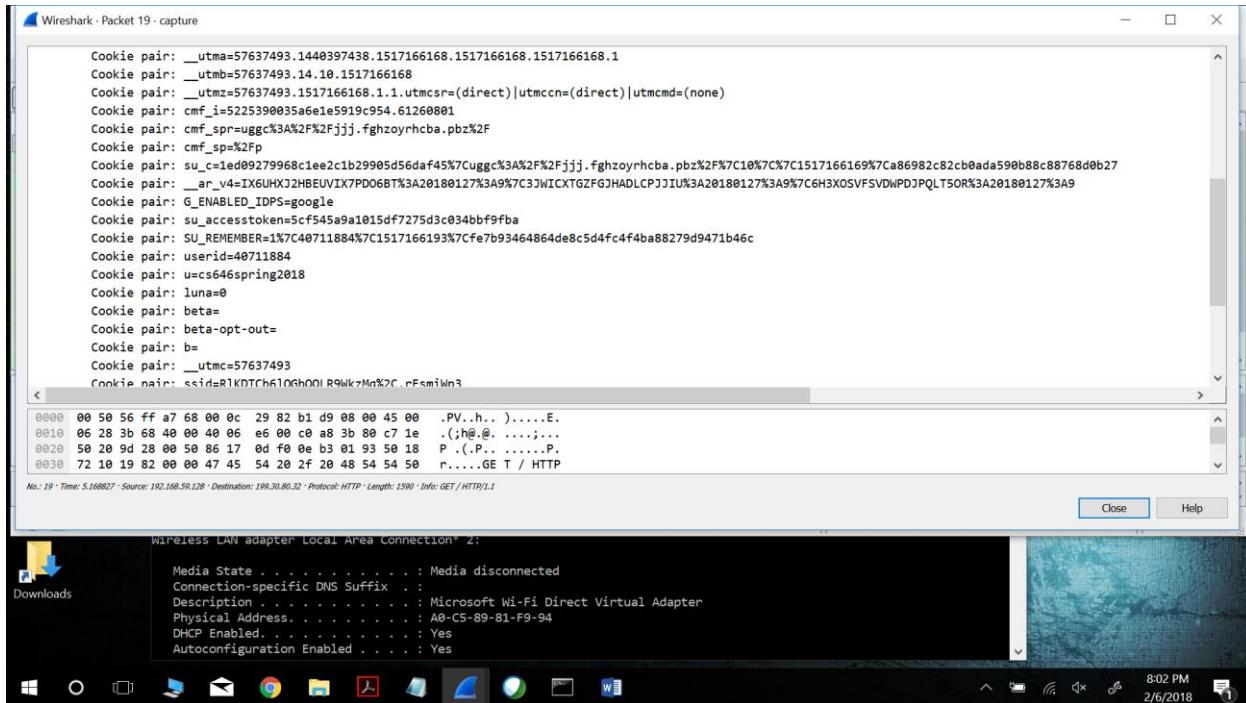
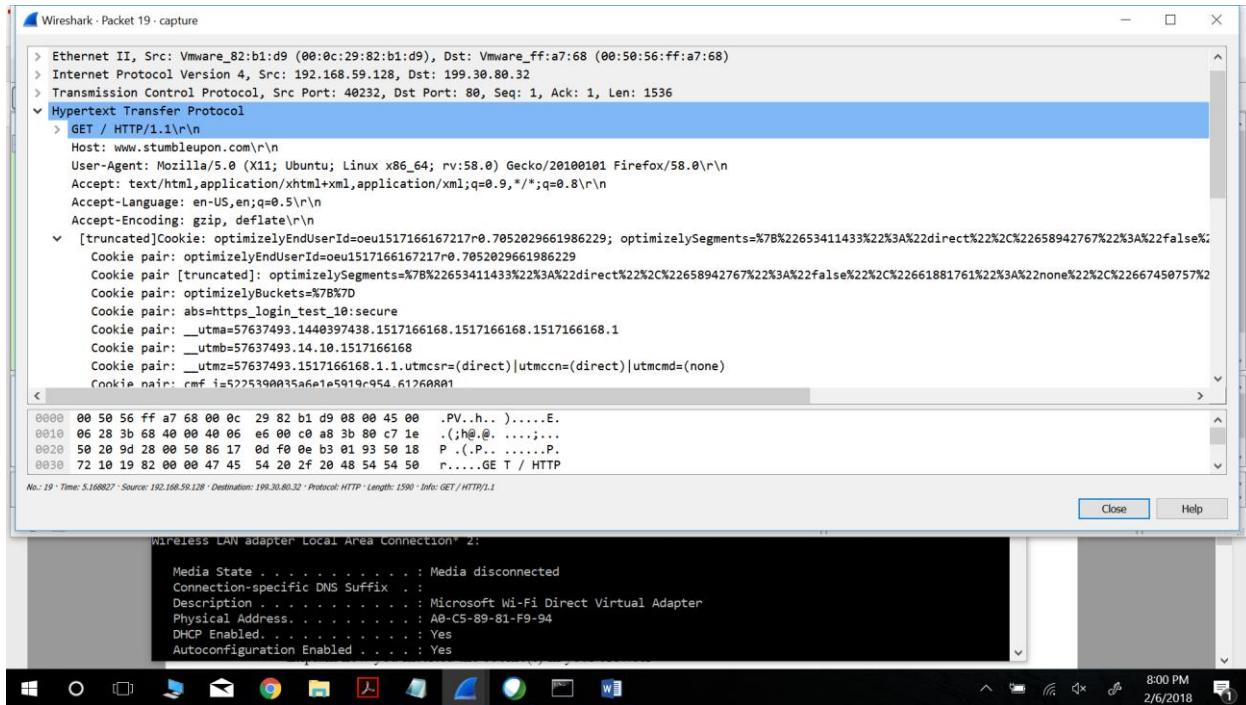
## 1. Finding packets that contain relevant cookies: -

- 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



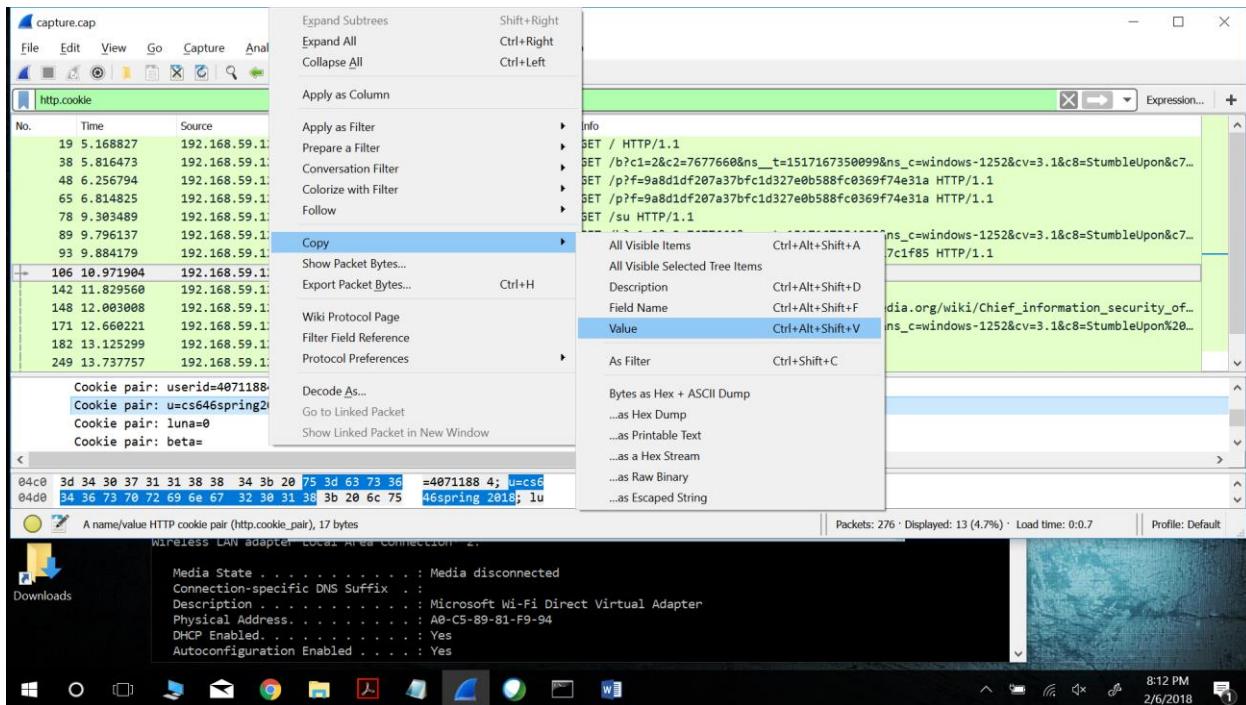
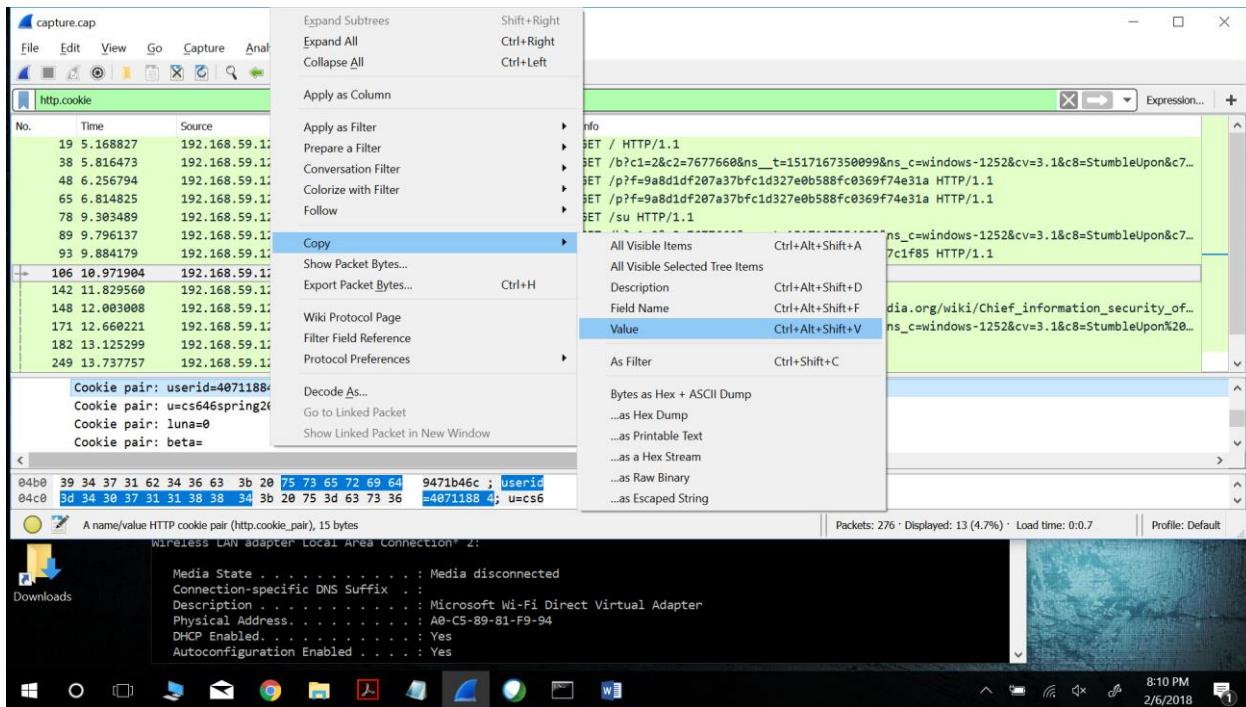
## 2. Packets that contain cookies with the relevant HTTP header: -

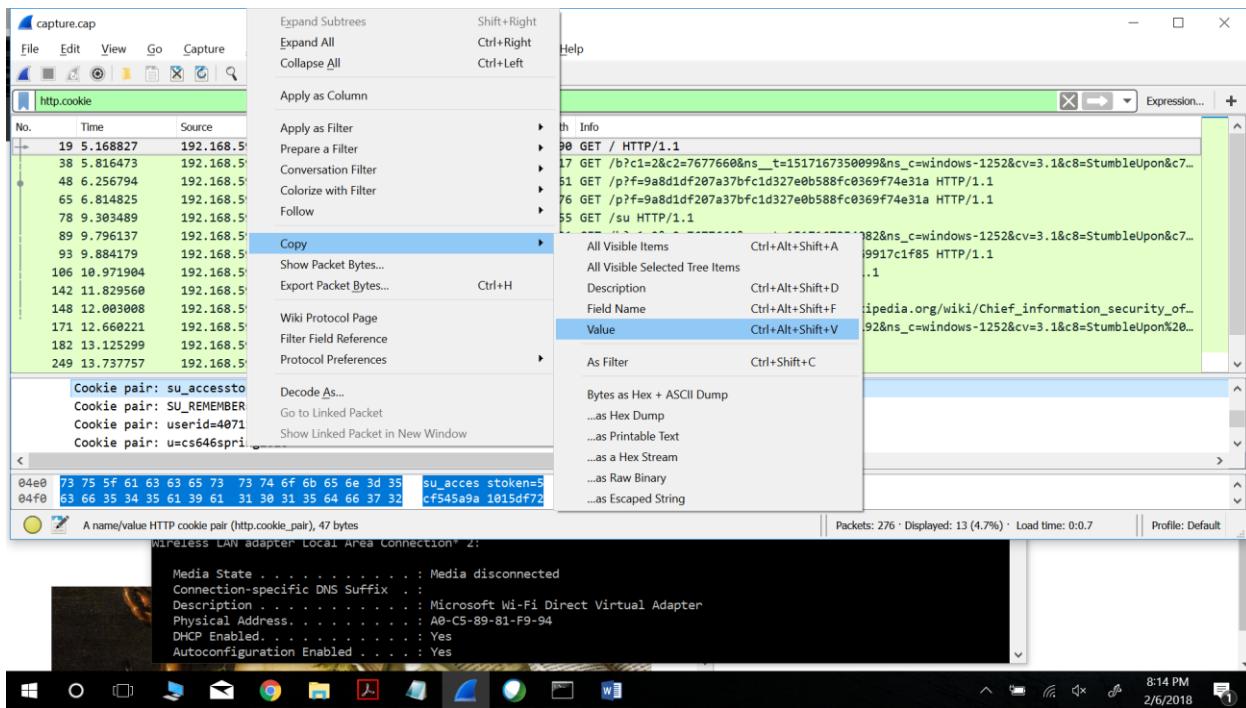
- Expand the header and search for the cookies
- Double click on the header which contains cookies



### 3. Extracting cookies from Wireshark: -

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



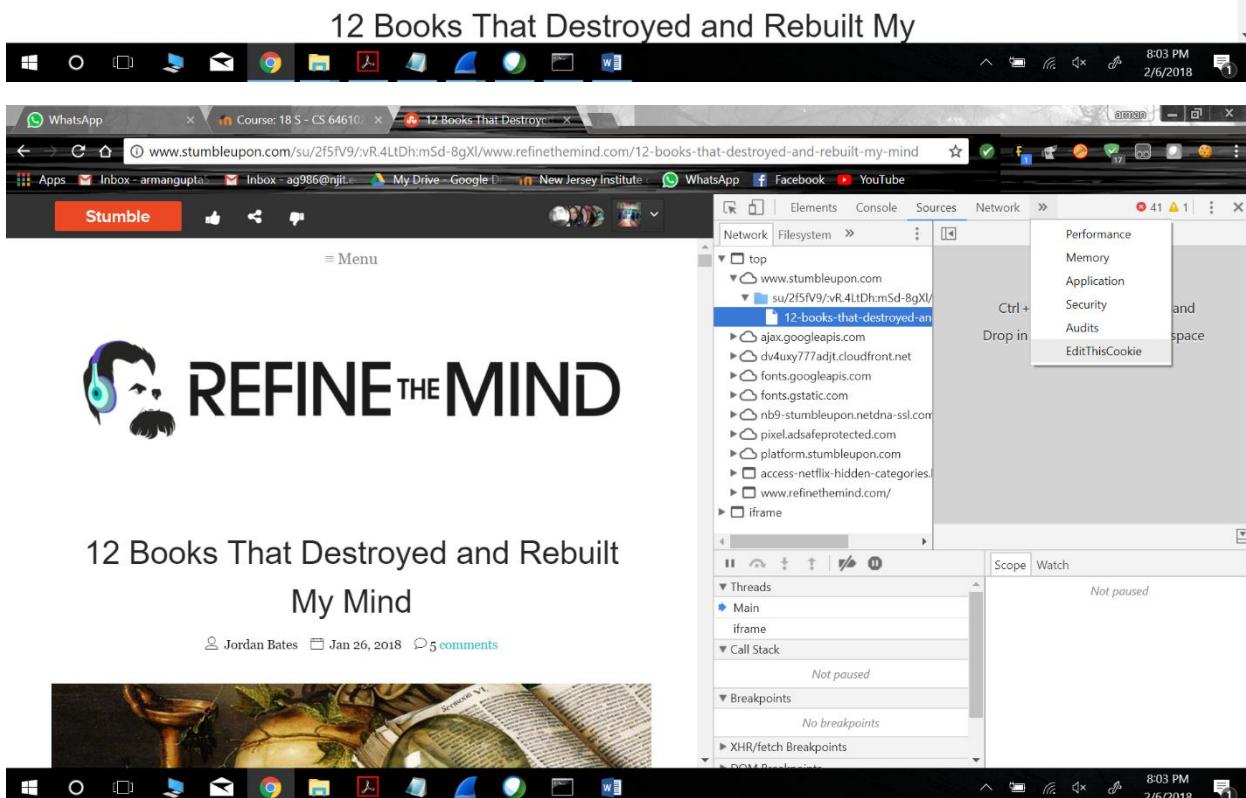
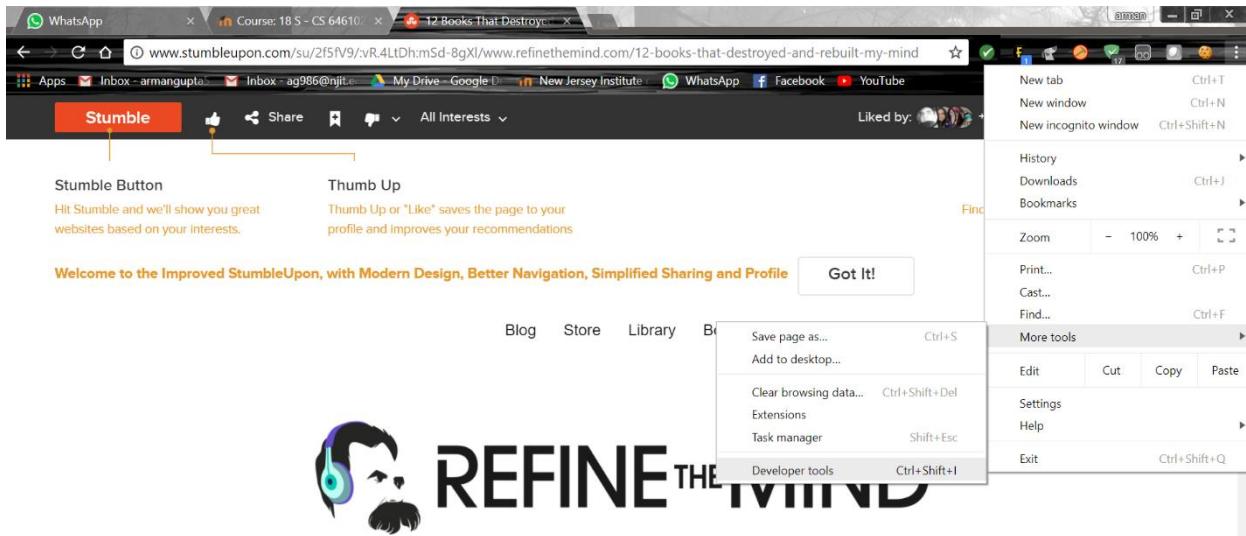


#### 4. Cookies relevant and required for authentication: -

- “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 Destroy... 41 A 1

www.stumbleupon.com/su/2f5f9/v.R4LtDh:mSd-8gXI/www.refinethemind.com/12-books-that-destroyed-and-rebuilt-my-mind

Apps Inbox - armangupta... Inbox - ag986@njit.edu My Drive Google Docs 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



Name	Value	Domain	Path	Expires	Session	HostOnly	Secure	HttpOnly
cmf...	ugg...	.stumb...	/	Thu M...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ssid	uaY...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
abs	http...	www.s...	/	Sat A...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G_E...	goo...	.www....	/	Fri De...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
su...	ff5fd...	.stumb...	/	Sun F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dtC...	E1D...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
u	agu...	.stumb...	/	Wed F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cmf...	%2Fp...	.stumb...	/	Thu M...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cmf_i	198...	.stumb...	/	Thu M...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
stu...	151...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
userId	3696 4942	www.s...	/	Tue F...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
luna	11	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
su_c	9bc...	.stumb...	/	Wed F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SU_...	1%...	.stumb...	/	Sun F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
beta	.	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
beta...	.	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b	.	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8:11 PM 2/6/2018

The screenshot shows a browser window with several tabs open. The active tab displays a cookie table from the developer tools, listing various session cookies for the domain www.refinethemind.com. The table includes columns for Name, Value, Domain, Path, Expires, Session, HostOnly, Secure, and HttpOnly. Notable entries include 'beta' and 'beta...' under the .stumbleUpon.com domain, and 'userid' with values '4871' and '1884'. Below the table, the main content of the website 'Refine THE MIND' is visible, featuring a stylized logo and the title '12 Books That Destroyed and Rebuilt My Mind'.

Name	Value	Domain	Path	Expires	Session	HostOnly	Secure	HttpOnly
abs	http...	www.s...	/	Sat A...			<input checked="" type="checkbox"/>	
b		.stumble...	/	Wed F...	<input checked="" type="checkbox"/>			
beta		.stumble...	/	Wed F...	<input checked="" type="checkbox"/>			
beta...		.stumble...	/	Wed F...	<input checked="" type="checkbox"/>			
cmf_i	198...	.stumble...	/	Thu M...				
cmf%	%2Fp	.stumble...	/	Thu M...				
cmf%	ugg...	.stumble...	/	Thu M...				
dtc...	E1D...	.stumble...	/	Wed F...	<input checked="" type="checkbox"/>			
G_E...	goo...	.www....	/	Fri De...				
luna	11	.stumble...	/	Wed F...	<input checked="" type="checkbox"/>			
ssid	uaY...	.stumble...	/	Wed F...	<input checked="" type="checkbox"/>			
stu...	151...	.stumble...	/	Wed F...	<input checked="" type="checkbox"/>			
su...	ff5fd...	.stumble...	/	Sun F...				
su_c	9bc...	.stumble...	/	Wed F...				
SU...	1%...	.stumble...	/	Sun F...				
u	agu...	.stumble...	/	Wed F...				
userid	4871 1884	www.s...	/	Tue F...		<input checked="" type="checkbox"/>		

WhatsApp Course: 18 S - CS 64610 12 Books That Destroy... 1 amap

www.stumbleupon.com/su/2f5f9/v.R4LtDh:mSd-8gXI/www.refinethemind.com/12-books-that-destroyed-and-rebuilt-my-mind

Apps Inbox - armangupta... Inbox - ag986@njit.edu My Drive Google Docs 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



Name	Value	Domain	Path	Expires	Session	HostOnly	Secure	Ht
abs	http...	www.s...	/	Sat A...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
b	.stumb...		/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
beta	.stumb...		/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
beta...	.stumb...		/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
cmf_I	198...	.stumb...	/	Thu M...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
cmf...	%2Fp...	.stumb...	/	Thu M...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
cmf...	ugg...	.stumb...	/	Thu M...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
dtC...	E1D...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G_E...	goo...	.www....	/	Fri De...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
luna	11	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
ssid	uaY...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
stu...	151...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
su...	ff5fd...	.stumb...	/	Sun F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
su_c	9bc...	.stumb...	/	Wed F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SU_...	1%...	.stumb...	/	Sun F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
u	agup... t88 1	.stumb...	/	Wed F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

The screenshot shows a browser window with several tabs open. The active tab displays a cookie table from the developer tools, listing various session cookies for the domain www.refinethemind.com. The table includes columns for Name, Value, Domain, Path, Expires, Session, HostOnly, Secure, and HttpOnly. One cookie, 'u', has its value highlighted with a red box containing the text 'cs64 6spr ing2 018'. The background of the browser shows the homepage of 'Refine The Mind', which features a stylized profile icon and the text 'REFINE THE MIND'. Below the header, the main content area displays the title '12 Books That Destroyed and Rebuilt My Mind' and a snippet of text by Jordan Bates from January 26, 2018.

Name	Value	Domain	Path	Expires	Session	HostOnly	Secure	HttpOnly
abs	http...	www.s...	/	Sat A...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
b		.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
beta		.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
beta...		.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
cmf_i	198...	.stumb...	/	Thu M...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
cmf%	%2Fp	.stumb...	/	Thu M...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
cmf%	ugg...	.stumb...	/	Thu M...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dtc...	E1D...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G_E...	goo...	.www....	/	Fri De...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
luna	11	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ssid	uaY...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
stu...	151...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
su...	ff5fd...	.stumb...	/	Sun F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
su_c	9bc...	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SU...	1%...	.stumb...	/	Sun F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
u	cs64 6spr ing2 018	.stumb...	/	Wed F...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The screenshot shows a browser window with several tabs open. The active tab displays a list of cookies for the domain www.stumbleupon.com. The table has columns for Name, Value, Domain, Path, Expires, Session, HostOnly, Secure, and HttpOnly. Notable entries include 'abs' with a value of 'http...', 'beta' with a value of '.stumbleupon.com', and 'su\_accesstoken' with a value containing '5c'. Below the cookie table, the main content of the page is visible, featuring a logo for 'REFINE THE MIND' and a title '12 Books That Destroyed and Rebuilt My Mind'.

Name	Value	Domain	Path	Expires	Session	HostOnly	Secure	HttpOnly
abs	http...	www.stumbleupon.com	/	Sat Apr 07 2018 18:31:06 ...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b		.stumbleupon.com	/	Wed Feb 06 2019 20:15:4...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
beta		.stumbleupon.com	/	Wed Feb 06 2019 20:15:4...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
beta-opt-out		.stumbleupon.com	/	Wed Feb 06 2019 20:15:4...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cmf_1	198...	.stumbleupon.com	/	Thu Mar 08 2018 17:30:01...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cmf_sp	%2Fp	.stumbleupon.com	/	Thu Mar 08 2018 17:30:01...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cmf_spr	ugg...	.stumbleupon.com	/	Thu Mar 08 2018 17:30:01...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dtCookie	E1D...	.stumbleupon.com	/	Wed Feb 06 2019 20:15:4...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G_ENABLED_IDPS	goo...	www.stumbleupon.com	/	Fri Dec 31 9999 07:00:00 ...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
luna	11	.stumbleupon.com	/	Wed Feb 06 2019 20:15:4...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ssid	uaY...	.stumbleupon.com	/	Wed Feb 06 2019 20:15:4...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
stumble%3Alast	151...	.stumbleupon.com	/	Wed Feb 06 2019 20:15:4...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
su_accesstoken	5c T5 45	.stumbleupon.com	/	Sun Feb 06 2028 17:31:14...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
su_c	9bc...	.stumbleupon.com	/	Wed Feb 06 2019 17:30:0...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SU_REMEMBER	1%...	.stumbleupon.com	/	Sun Feb 06 2028 17:31:14...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
u	cs6...	.stumbleupon.com	/	Wed Feb 06 2019 17:30:0...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 6. Adding page to cs646spring2018 account: -

- Page added with a link by UCID “ag986”

The screenshot shows a browser window displaying a post from 'REFINE THE MIND' that has been 'Liked by' 1.8k others. The post itself is titled '12 Books That Destroyed and Rebuilt My'.

```
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
```

The screenshot shows a Windows desktop environment. At the top, there's a taskbar with various icons including WhatsApp, Course: 18 S - CS 64610, StumbleUpon - StumbleUpon.com, and several browser tabs. The desktop background is black.

In the center, a StumbleUpon profile for 'Stumble' (@cs646spring...) is displayed. It shows 5 Likes, 0 Following, and 0 Followers. Below the profile, a post by 'NightFroster' (@nightfroster.com) is shown with the title 'Welcome To NightFroster' and a link to nightfroster.com. The post has 1 like and is categorized under Socialism.

Another post by 'cyber-security-and-privacy.info' (@cyber-security-and-privacy.info) titled 'Post\_For\_Stymble\_upon\_CS646\_project' is also listed, with 1 like and categorized under Education.

A third post by 'New Jersey Institute of Technology' (@njit.edu) is shown, categorized as a university with 26 likes.

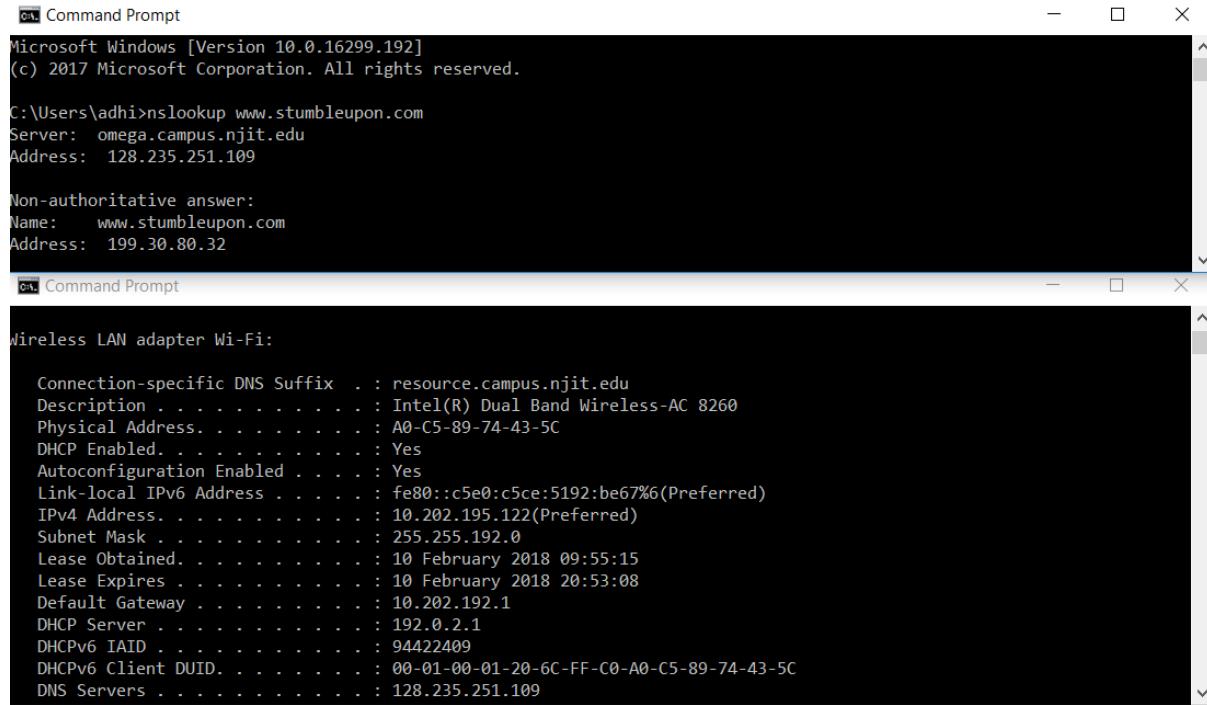
At the bottom of the screen, a command prompt window is open with the title 'C:\WINDOWS\system32\cmd.exe'. It displays network configuration information for 'Wireless LAN adapter Local Area Connection 2'. The output includes:

```
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
```

**Adhithya Sivanesh([as3423@njit.edu](mailto: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](http://www.stumbleupon.com). This was found out by using the nslookup command in cmd in my windows 10 machine.



The image shows two separate Command Prompt windows side-by-side. The top window displays the output of the 'nslookup www.stumbleupon.com' command, which shows the server as omega.campus.njit.edu and the address as 128.235.251.109. The bottom window shows detailed network configuration for the 'Wireless LAN adapter Wi-Fi' interface, including connection-specific DNS suffix, description (Intel(R) Dual Band Wireless-AC 8260), physical address (A0-C5-89-74-43-5C), DHCP status (Enabled Yes), auto-configuration (Enabled Yes), link-local IPv6 address (fe80::c5e0:c5ce:5192:be67%6(Preferred)), IPv4 address (10.202.195.122(Preferred)), subnet mask (255.255.192.0), lease obtained (10 February 2018 09:55:15), lease expires (10 February 2018 20:53:08), default gateway (10.202.192.1), DHCP server (192.0.2.1), DHCPv6 IAID (94422409), DHCPv6 Client DUID (00-01-00-01-20-6C-FF-C0-A0-C5-89-74-43-5C), and DNS servers (128.235.251.109).

```
Microsoft Windows [Version 10.0.16299.192]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\adhi>nslookup www.stumbleupon.com
Server:  omega.campus.njit.edu
Address: 128.235.251.109

Non-authoritative answer:
Name:  www.stumbleupon.com
Address: 199.30.80.32

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : resource.campus.njit.edu
Description . . . . . : Intel(R) Dual Band Wireless-AC 8260
Physical Address. . . . . : A0-C5-89-74-43-5C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c5e0:c5ce:5192:be67%6(Preferred)
IPv4 Address. . . . . : 10.202.195.122(Preferred)
Subnet Mask . . . . . : 255.255.192.0
Lease Obtained. . . . . : 10 February 2018 09:55:15
Lease Expires . . . . . : 10 February 2018 20:53:08
Default Gateway . . . . . : 10.202.192.1
DHCP Server . . . . . : 192.0.2.1
DHCPv6 IAID . . . . . : 94422409
DHCPv6 Client DUID. . . . . : 00-01-00-01-20-6C-FF-C0-A0-C5-89-74-43-5C
DNS Servers . . . . . : 128.235.251.109
```

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

The Wireshark interface shows a list of network packets. A green vertical bar highlights the first few packets. The packet details pane shows the following:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.59.128	199.30.80.32	TCP	74	40228 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
2	0.055259	192.168.59.128	199.30.80.32	TCP	74	40230 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
4	0.084217	192.168.59.128	199.30.80.32	TCP	54	40228 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
6	0.139225	192.168.59.128	199.30.80.32	TCP	54	40230 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
7	5.078819	192.168.59.128	199.30.80.32	TCP	74	40232 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
18	5.168479	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
19	5.168827	192.168.59.128	199.30.80.32	HTTP	1590	GET / HTTP/1.1
23	5.350501	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=1537 Ack=1461 Win=32120 Len=0
25	5.351210	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=1537 Ack=7591 Win=43800 Len=0
30	5.697492	192.168.59.128	199.30.80.32	TCP	54	40230 → 80 [FIN, ACK] Seq=1 Ack=1 Win=29200 Len=0
31	5.697704	192.168.59.128	199.30.80.32	TCP	54	40228 → 80 [FIN, ACK] Seq=1 Ack=1 Win=29200 Len=0
35	5.782079	192.168.59.128	199.30.80.32	TCP	54	40230 → 80 [ACK] Seq=2 Ack=2 Win=29200 Len=0
37	5.782104	192.168.59.128	199.30.80.32	TCP	54	40228 → 80 [ACK] Seq=2 Ack=2 Win=29200 Len=0
48	6.256794	192.168.59.128	199.30.80.32	HTTP	1661	GET /p?f=9a8d1df207a37bfc1d327e0b588fc0369f74e31a HTTP/1...
64	6.519149	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=3144 Ack=8164 Win=46720 Len=0
65	6.814825	192.168.59.128	199.30.80.32	HTTP	1676	GET /p?f=9a8d1df207a37bfc1d327e0b588fc0369f74e31a HTTP/1...
76	7.063628	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=4766 Ack=8696 Win=49640 Len=0
78	9.303489	192.168.59.128	199.30.80.32	HTTP	1655	GET /su HTTP/1.1
84	9.476687	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=6367 Ack=10156 Win=52560 Len=0
86	9.476942	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=6367 Ack=14536 Win=61320 Len=0
88	9.486943	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=6367 Ack=16294 Win=64240 Len=0
93	9.884179	192.168.59.128	199.30.80.32	HTTP	1681	GET /p?f=3083f80f22f76c737c056c9e15ea169917c1fb85 HTTP/1...

c:\ Command Prompt

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : resource.campus.njit.edu
Description . . . . . : Intel(R) Dual Band Wireless-AC 8260
Physical Address . . . . . : A0-C5-89-74-43-5C
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c5e0:c5ce:5192:be67%6(Preferred)
IPv4 Address . . . . . : 10.202.192.122(Preferred)
Subnet Mask . . . . . : 255.255.192.0
Lease Obtained . . . . . : 10 February 2018 09:55:15
Lease Expires . . . . . : 10 February 2018 20:53:08
Default Gateway . . . . . : 10.202.192.1
DHCP Server . . . . . : 192.0.2.1
DHCPv6 IAID . . . . . : 94422409
DHCPv6 Client DUID . . . . . : 00-01-00-01-20-6C-FF-C0-A0-C5-89-74-43-5C
DNS Servers . . . . . : 128.235.251.109
```

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](http://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.

The Wireshark interface shows a list of network packets. A green vertical bar highlights the first few packets. The packet details pane shows the following:

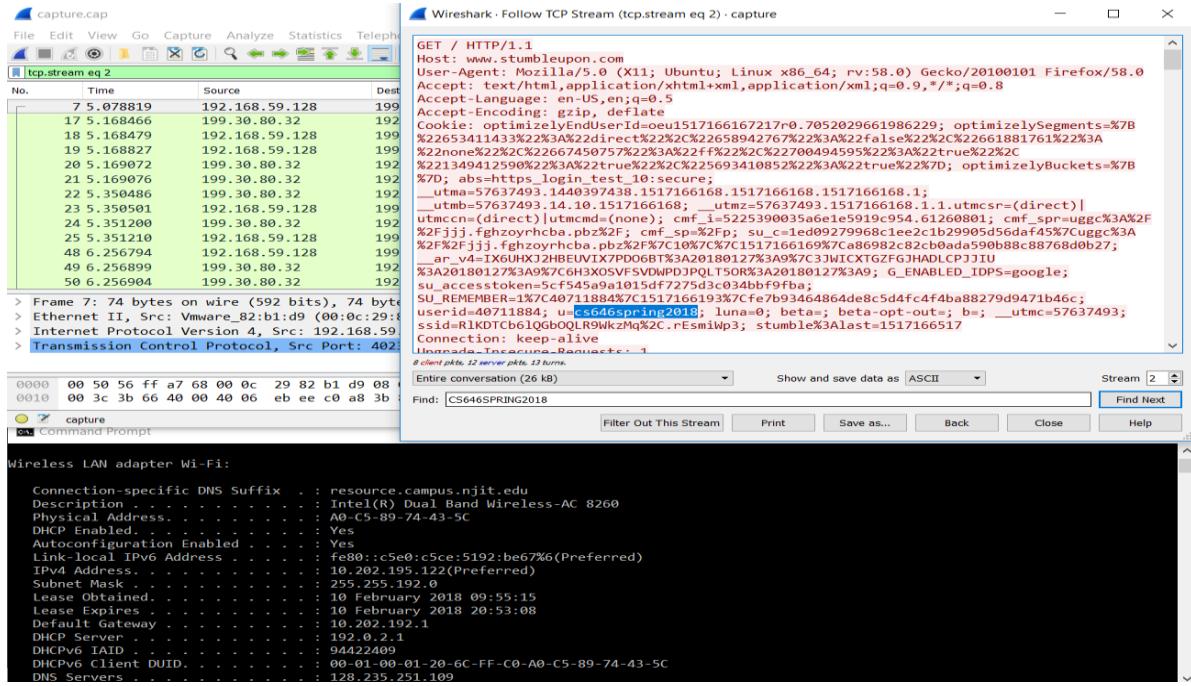
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.59.128	199.30.80.32	TCP	74	40228 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
2	0.055259	192.168.59.128	199.30.80.32	TCP	74	40230 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
4	0.084217	192.168.59.128	199.30.80.32	TCP	54	40228 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
6	0.139225	192.168.59.128	199.30.80.32	TCP	54	40230 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
7	5.078819	192.168.59.128	199.30.80.32	TCP	74	40232 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
18	5.168479	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
19	5.168827	192.168.59.128	199.30.80.32	HTTP	1590	GET / HTTP/1.1
23	5.350501	192.168.59.128	199.30.80.32	TCP	54	40232 → 80 [ACK] Seq=1537 Ack=1461 Win=32120 Len=0
25	5.351210	192.168.59.128	199.30.80.32	TCP	54	40230 → 80 [FIN, ACK] Seq=1 Ack=1 Win=29200 Len=0
30	5.697492	192.168.59.128	199.30.80.32	TCP	54	40228 → 80 [FIN, ACK] Seq=1 Ack=1 Win=29200 Len=0
31	5.697704	192.168.59.128	199.30.80.32	TCP	54	40230 → 80 [ACK] Seq=2 Ack=2 Win=29200 Len=0
35	5.782079	192.168.59.128	199.30.80.32	TCP	54	40228 → 80 [ACK] Seq=2 Ack=2 Win=29200 Len=0
37	5.782104	192.168.59.128	199.30.80.32	TCP	54	40228 → 80 [ACK] Seq=2 Ack=2 Win=29200 Len=0

The context menu for the selected packet (Frame 7) is open, with "TCP Stream" highlighted under the "Follow" submenu. Other options in the menu include Mark/Unmark Packet, Ignore/Unignore Packet, Set/Unset Time Reference, Time Shift..., Packet Comment..., Edit Resolved Name, Apply as Filter, Prepare a Filter, Conversation Filter, Colorize Conversation, SCTP, Follow (with TCP Stream selected), Copy, Protocol Preferences, Decode As..., and Show Packet in New Window.

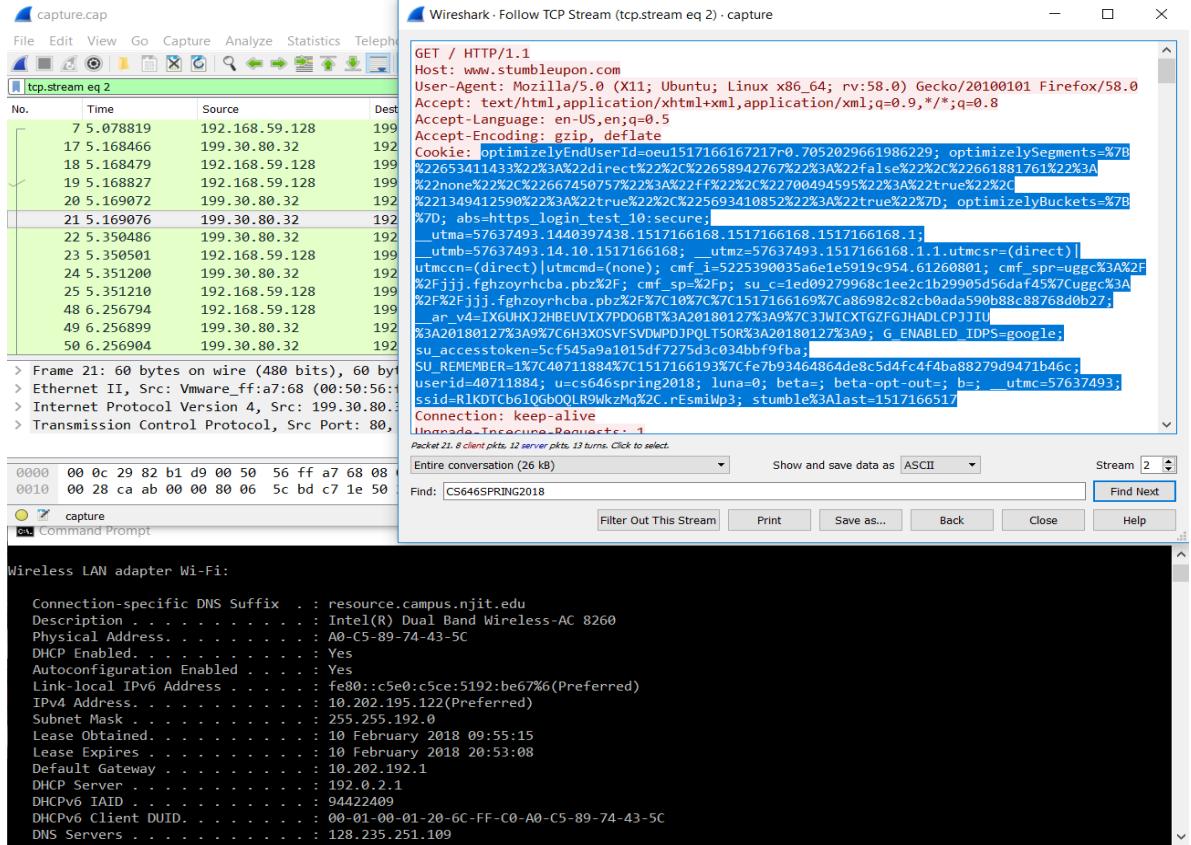
Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : resource.campus.njit.edu
Description . . . . . : Intel(R) Dual Band Wireless-AC 8260
Physical Address . . . . . : A0-C5-89-74-43-5C
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c5e0:c5ce:5192:be67%6(Preferred)
IPv4 Address . . . . . : 10.202.192.122(Preferred)
Subnet Mask . . . . . : 255.255.192.0
Lease Obtained . . . . . : 10 February 2018 09:55:15
Lease Expires . . . . . : 10 February 2018 20:53:08
Default Gateway . . . . . : 10.202.192.1
DHCP Server . . . . . : 192.0.2.1
DHCPv6 IAID . . . . . : 94422409
DHCPv6 Client DUID . . . . . : 00-01-00-01-20-6C-FF-C0-A0-C5-89-74-43-5C
DNS Servers . . . . . : 128.235.251.109
```

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.



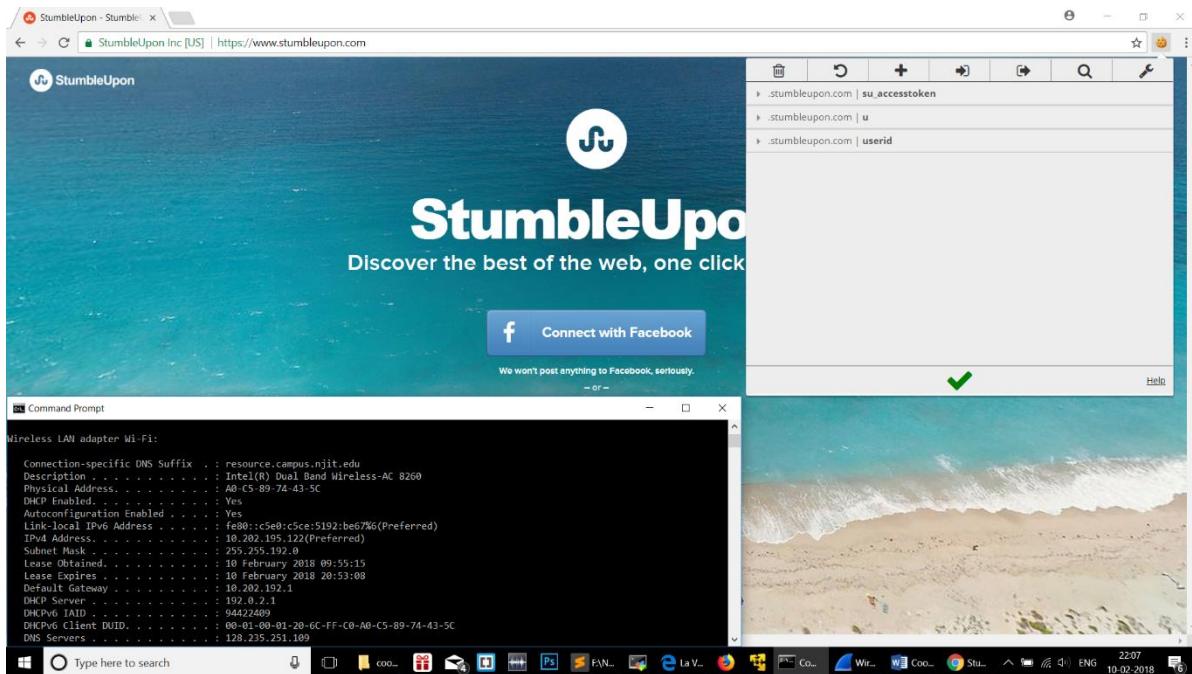
6] The next step is to go to [www.stumbleupon.com](https://www.stumbleupon.com) in your chrome browser, and then open EditThisCookie to edit the cookie. Remove all the present cookies that are shown in the below screenshot.



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.

The screenshot shows a hijacked StumbleUpon profile for "George Barnard's Photographic Views of Sherman's Campaign - Image Gallery Essay". A context menu is open on the right, with "My Profile" selected. A command prompt window is overlaid, showing network configuration details:

```
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : resource.campus.njit.edu
Description . . . . . : Intel(R) Dual Band Wireless-AC 8260
Physical Address . . . . . : A0-C5-89-74-43-5C
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c9e0:c5ce:5192:be67%6(Preferred)
IPv4 Address . . . . . : 10.202.195.122(Preferred)
Subnet Mask . . . . . : 255.255.192.0
Lease Obtained . . . . . : 10 February 2018 09:55:15
Lease Expires . . . . . : 10 February 2018 20:53:08
Default Gateway . . . . . : 10.202.1.1
DHCP Server . . . . . : 192.0.2.1
DHCPv6 T1/D1 . . . . . : 94427409
DHCPv6 Client DUID . . . . . : 00-01-00-01-20-6C-FF-C0-A0-C5-89-74-43-5C
DNS Servers . . . . . : 128.235.251.109
```

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”.

The screenshot shows a StumbleUpon profile page for user "@cs646spring2018". A modal dialog box is open, prompting to add the page "https://www.launchora.com". The dialog includes fields for "Safe for Work?", "What is this page about?", "Search Interests", "Add one or more tags", and a "Save" button. The "Add one or more tags" field contains the tag "as3423".

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

The screenshot shows a web browser window with the URL <https://www.stumbleupon.com/stumbler/cs646spring2018>. The page displays a user profile for '@cs646spring2018' with 8 likes and 0 followers. Below the profile are several thumbnail links to various websites, including Launchora, MIT, Amazon.com, and Kali Linux. To the right of the profile is a sidebar for 'NightFroster' with a welcome message and a post titled 'Post\_For\_Stumble\_upon\_CS646\_project'. At the bottom of the browser window is a command prompt titled 'Command Prompt' showing network configuration details for a 'Wireless LAN adapter Wi-Fi'.

```
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : resource.campus.njit.edu
Description . . . . . : Intel(R) Dual Band Wireless-AC 8260
Physical Address . . . . . : A0-C5-89-74-43-5C
DHCP Enabled . . . . . : Yes
Automatic Location Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c5e:5ce:5192:be67%{Preferred}
IPv4 Address . . . . . : 10.202.191.122{Preferred}
Subnet Mask . . . . . : 255.255.192.0
Lease Obtained . . . . . : 10 February 2018 09:55:15
Lease Expires . . . . . : 10 February 2018 20:53:08
Default Gateway . . . . . : 10.202.192.1
DHCP Server . . . . . : 192.0.2.1
DHCPv6 IID . . . . . : 9242:400
DHCPv6 Client DUID . . . . . : 00:01:00:01:20:6C:FF:C0:A0-C5-89-74-43-5C
DNS Servers . . . . . : 128.235.251.109
```

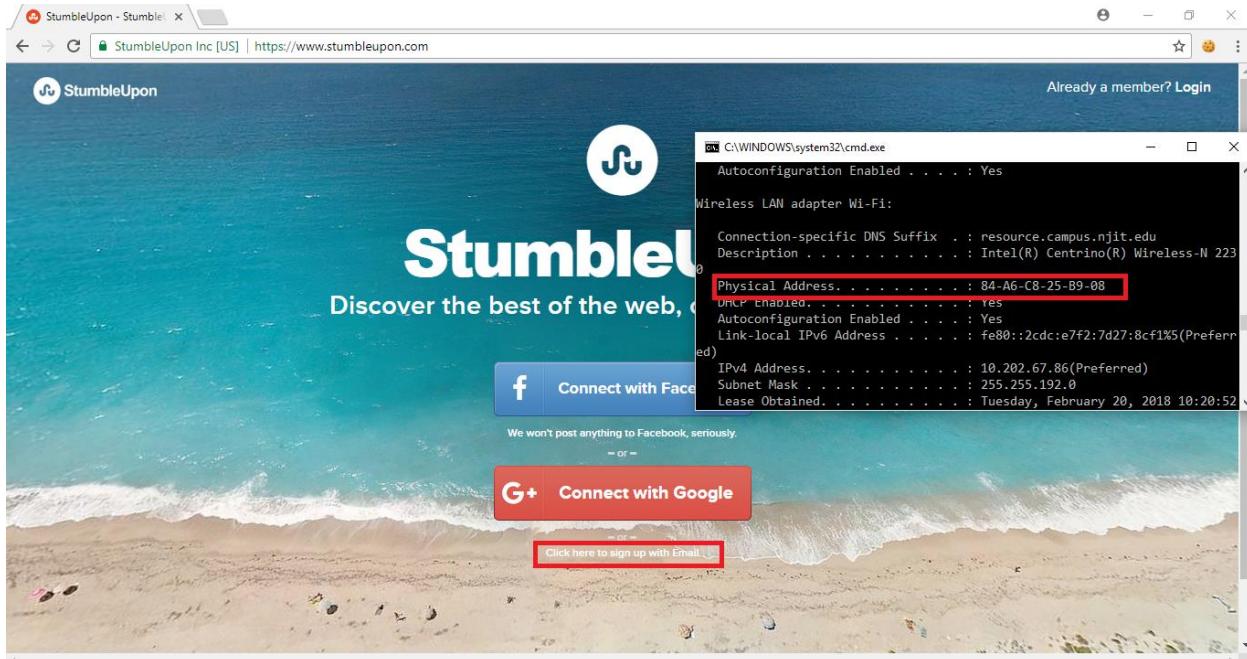
This shows that an account could be hijacked if the cookies are send in plain text and were captured by an eavesdropper.

Ketaki Kakade([kk524@njit.edu](mailto:kk524@njit.edu))

## Problem 2: Cookie Hijacking Attack

### Step 1:

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



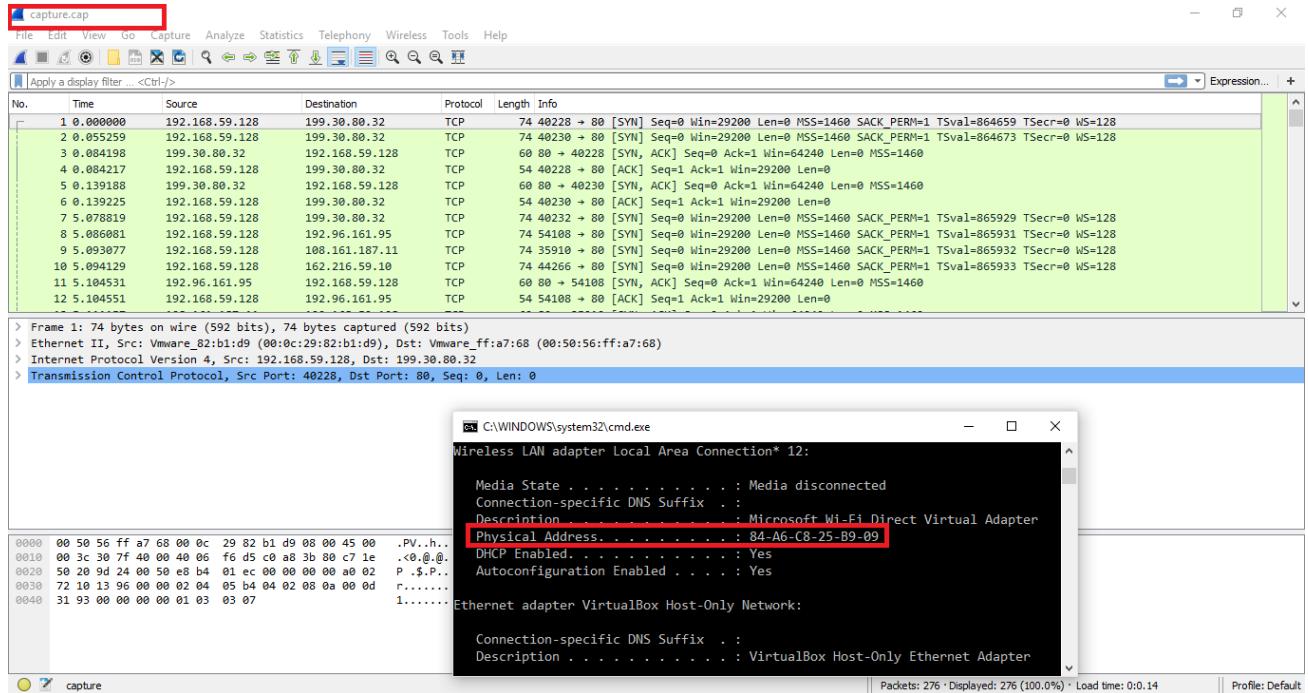
Screenshot – 1



Screenshot – 2

## Step 2:

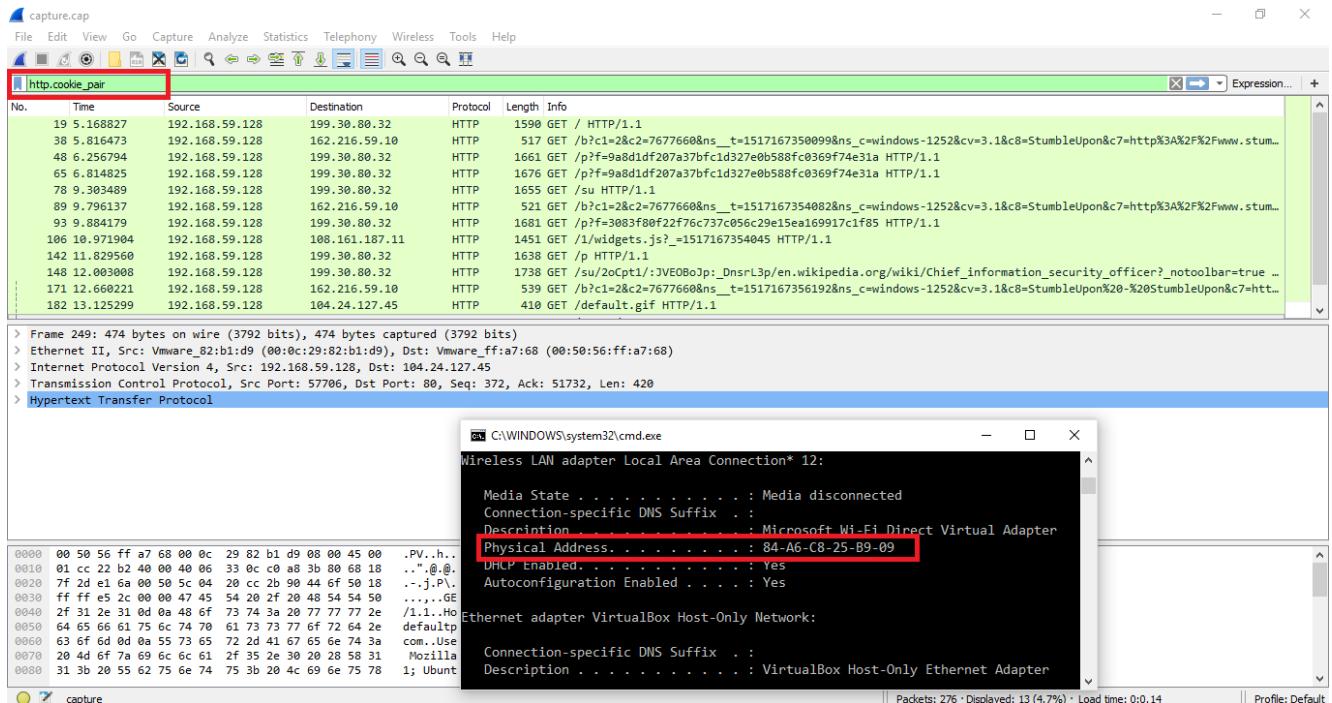
Open the capture.cap file in wireshark which contains wireless traffic captured when a client connected to the website www.stumbleupon.com over an insecure wireless connection.



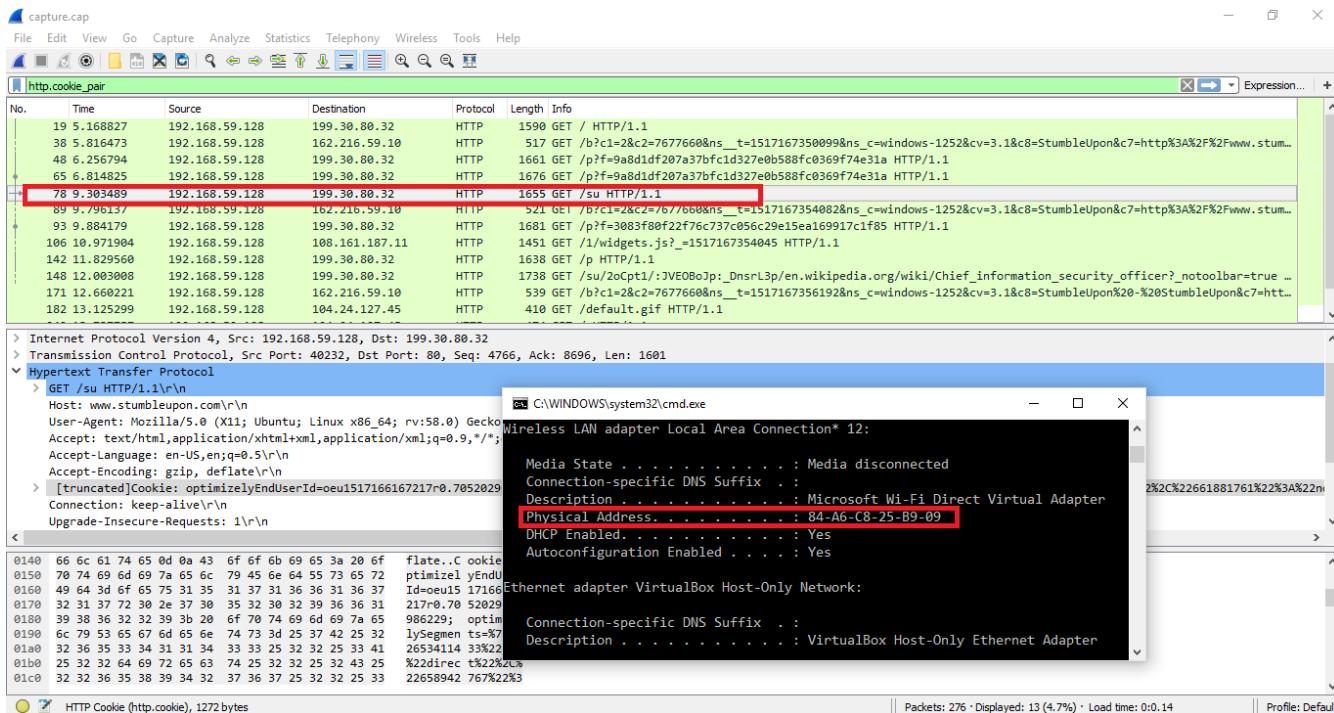
Screenshot – 3

## Step 3:

Apply the wireshark filter for analyzing only http cookies- http.cookie\_pair.



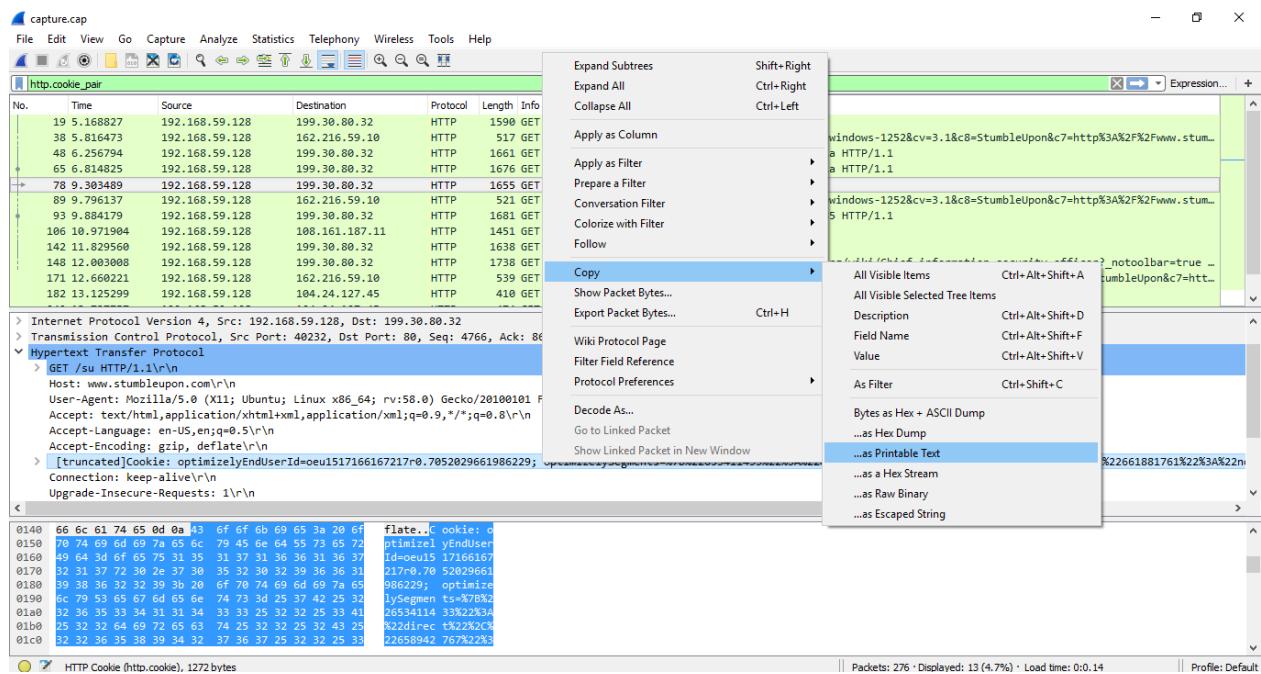
Screenshot – 4



Screenshot – 5

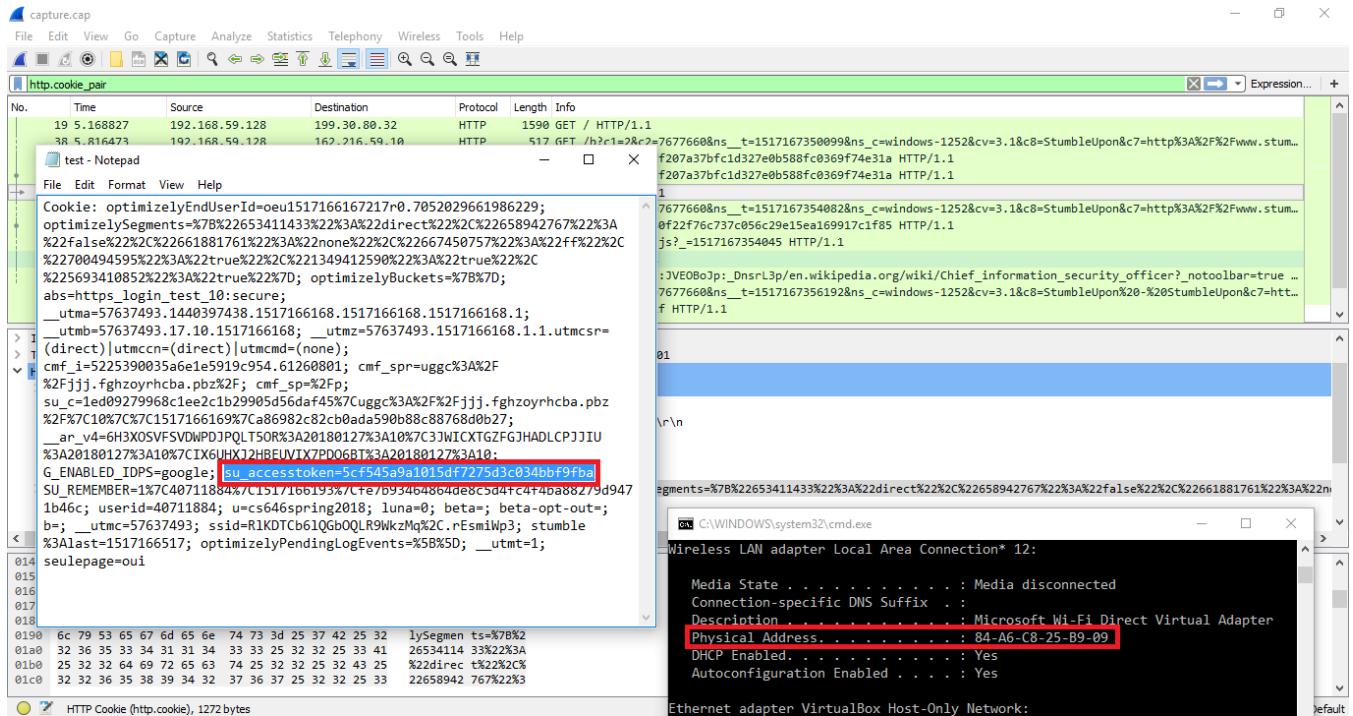
## Step 4:

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.

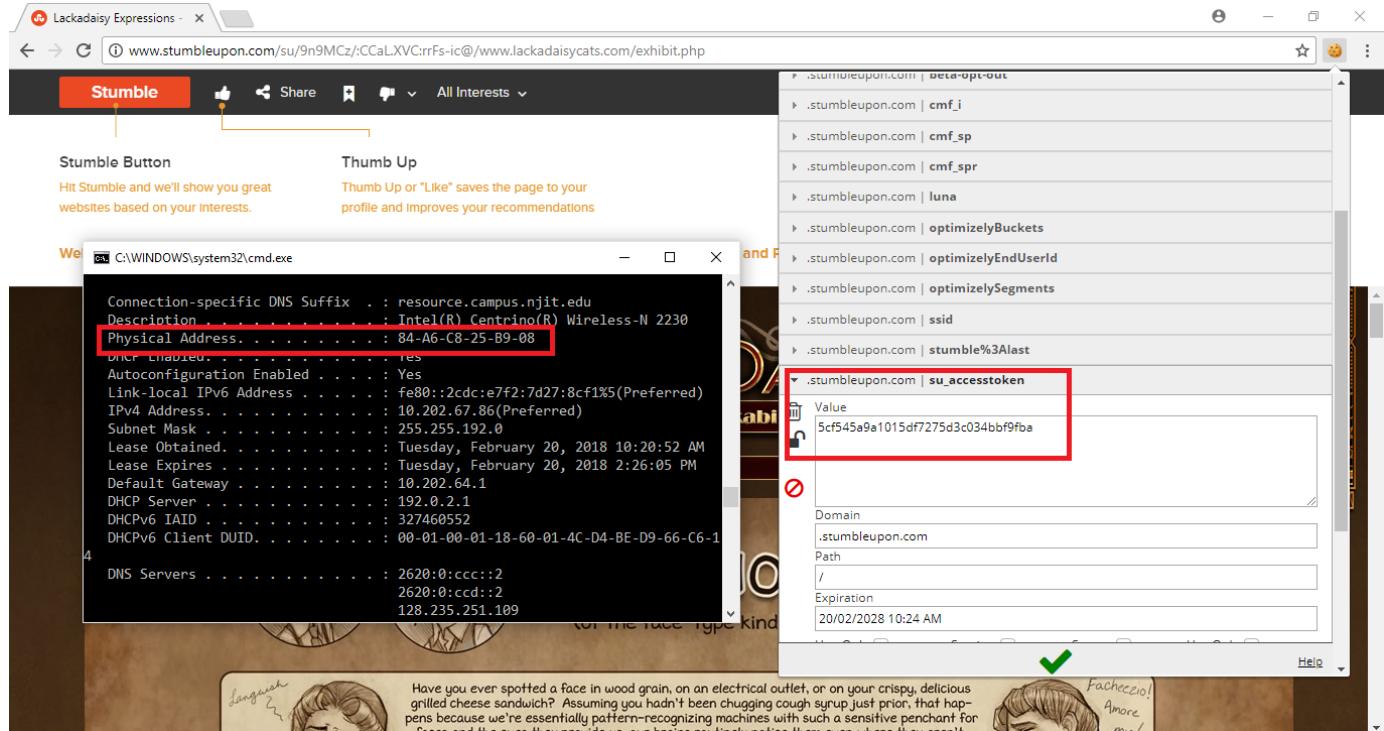
The screenshot shows a browser window with the URL [www.stumbleupon.com/su/9n9MCz/CcALXVCrrFs-ic@/www.lackadaisycats.com/exhibit.php](http://www.stumbleupon.com/su/9n9MCz/CcALXVCrrFs-ic@/www.lackadaisycats.com/exhibit.php). The page displays a StumbleUpon interface with a “Stumble” button and a “Thumb Up” section. To the right, a sidebar lists various cookies for the domain. A “.stumbleupon.com | su\_accesstoken” cookie is selected, showing its value as `76687097c2935db685197d03cc4a0b2`.

Below the browser, a command prompt window is open, showing network configuration details. The Physical Address is highlighted as `84-A6-C8-25-B9-09`.

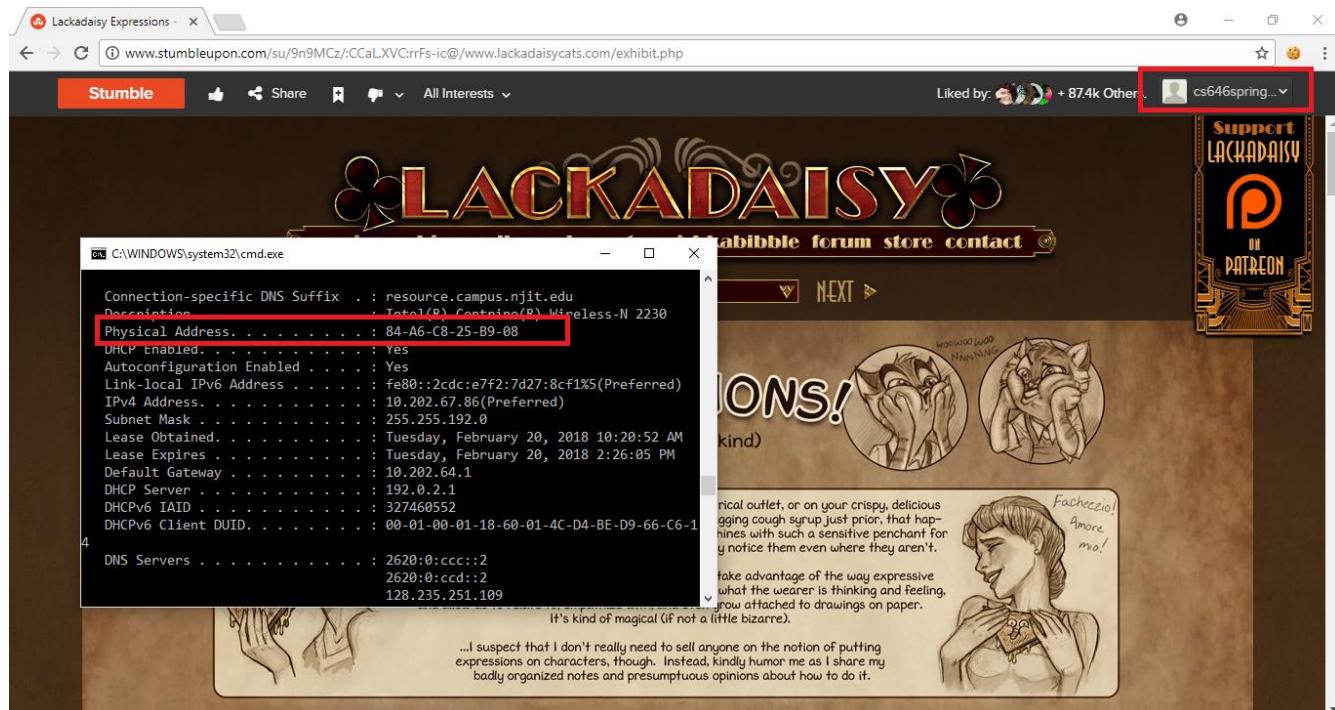
Screenshot – 8

## 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.

The screenshot shows a web browser window for StumbleUpon. In the center, a modal dialog box is open with the title "Submit this page to StumbleUpon and add it to your Likes." It contains a text input field with the URL "https://www.cisco.com/", a "Safe for Work?" radio button set to "Yes", and a dropdown menu "What is this page about? (choose one)" with "Network Security" selected. Below these are sections for "Search Interests" and "Add one or more tags", with "ketaki-kakade" and "kk524" listed. At the bottom are "Cancel" and "Save" buttons. The background shows the user's profile (@cs646spring2...) and a command prompt window showing network configuration details, with the "Physical Address" line highlighted.

Screenshot – 11

This screenshot shows the StumbleUpon interface after saving the page. The main area displays a list of pages the user has liked, including "World's Largest Professional Network" (LinkedIn), "Sachin Tendulkar - Wikipedia", "Amirs Modi" (ibelieve147.wordpress.com), "Watch The Big Bang Theory Online" (123movies.cafe), and "MS Dhoni - Wikipedia". The "Add a Page" dialog box from the previous screenshot is still visible on the right side of the screen. The command prompt window at the bottom continues to show network configuration details, with the "Physical Address" line highlighted.

Screenshot -12