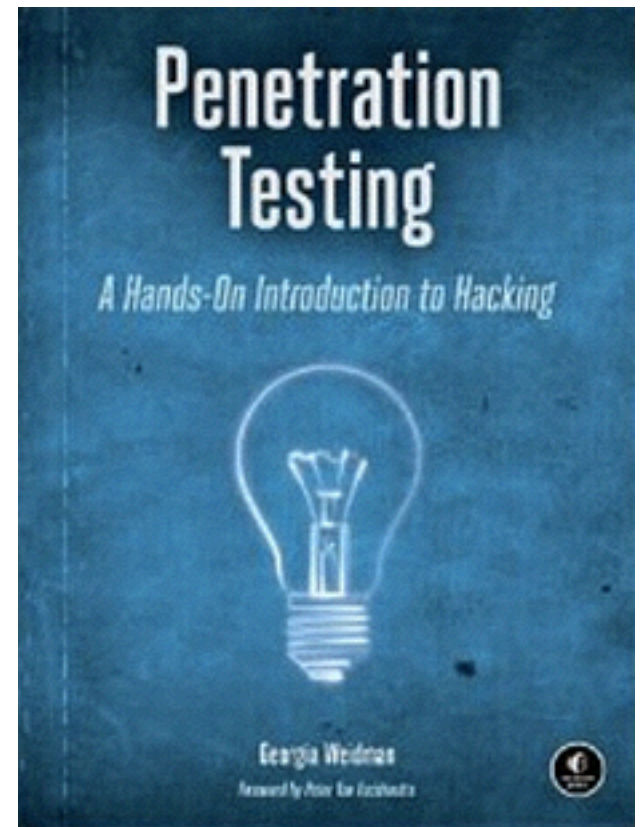


CNIT 124: Advanced Ethical Hacking



Ch 7: Capturing Traffic

Updated 10-5-17

Topics

- Switches, Hubs and Wireless networks
- Wireshark
 - Promiscuous mode and Monitor mode
 - Filters
 - Following a Stream
- ARP Cache Poisoning
- DNS Cache Poisoning
- SSLstrip

Switches, Hubs and Wireless Networks

Hubs

- Operate at OSI layer 1
- Repeat every bit out all ports
 - Except the receiving port
- Don't read addresses or any other content
- Ethernet NICs were designed for hubs

Ethernet

- NIC reads Destination MAC address
- First 6 bytes of frame

```
▶ Frame 3239: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on in
▼ Ethernet II, Src: ArrisGro_75:9e:10 (1c:1b:68:75:9e:10), Dst: Apple_4f:2b:5
  ▼ Destination: Apple_4f:2b:55 (28:cf:e9:4f:2b:55)
    Address: Apple_4f:2b:55 (28:cf:e9:4f:2b:55)
      .... ..0. .... = LG bit: Globally unique address (facto
      .... ..0 .... = IG bit: Individual address (unicast)
  ▼ Source: ArrisGro_75:9e:10 (1c:1b:68:75:9e:10)
```

```
0000  28 cf e9 4f 2b 55 1c 1b 68 75 9e 10 08 00 45 00  (...0+U.. hu....E.
0010  00 34 fd f9 40 00 30 06 6a 98 08 15 18 23 c0 a8  .4..@.0. j....#..
0020  01 52 00 50 e2 60 ab c5 40 04 31 8f 75 35 80 11  .R.P.`.. @.1.u5..
0030  00 72 29 5d 00 00 01 01 08 0a ed 8c ca a3 2e 5c  .r)].... \
0040  0e ef ..
```

Ethernet Promiscuous Mode

- If Destination MAC \neq NIC's hardware address
 - Packet is discarded
- Unless NIC is in "Promiscuous mode"
 - Every packet passed on to higher levels, regardless of MAC address
- Also applies to outgoing traffic

Wireless LANs

- No Encryption is just like Hubs
- WEP uses same key for every packet
- WPA generates a different key for each device
 - WPA and WPA2 use keys derived from an EAPOL handshake, which occurs when a machine joins a Wi-Fi network, to encrypt traffic. Unless all four handshake packets are present for the session you're trying to decrypt, Wireshark won't be able to decrypt the traffic.

Encrypted WPA2 Traffic

No.	Time	Source	Destination	Protocol	Length	Info
85	5_		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
86	5_		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
87	5_	Cisco-Li_82:b2:55	Apple_82:36...	EAPOL	181	Key (Message 1 of 4)
88	5_		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
89	5_	Apple_82:36:3a	Cisco-Li_82...	EAPOL	181	Key (Message 2 of 4)
90	5_		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
91	5_		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
92	5_	Cisco-Li_82:b2:55	Apple_82:36...	EAPOL	239	Key (Message 3 of 4)
93	5_		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
94	5_	Apple_82:36:3a	Cisco-Li_82...	EAPOL	159	Key (Message 4 of 4)
95	5_		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
96	5_	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=...
97	5_	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=...
98	5_		Apple_82:36...	802.11	38	Clear-to-send, Flags=.....C
99	5_	Apple_82:36:3a	Broadcast	802.11	404	Data, SN=27, FN=0, Flags=.p.....TC
100	5_		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
101	5_		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C

▶ Frame 99: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits)

▶ Radiotap Header v0, Length 24

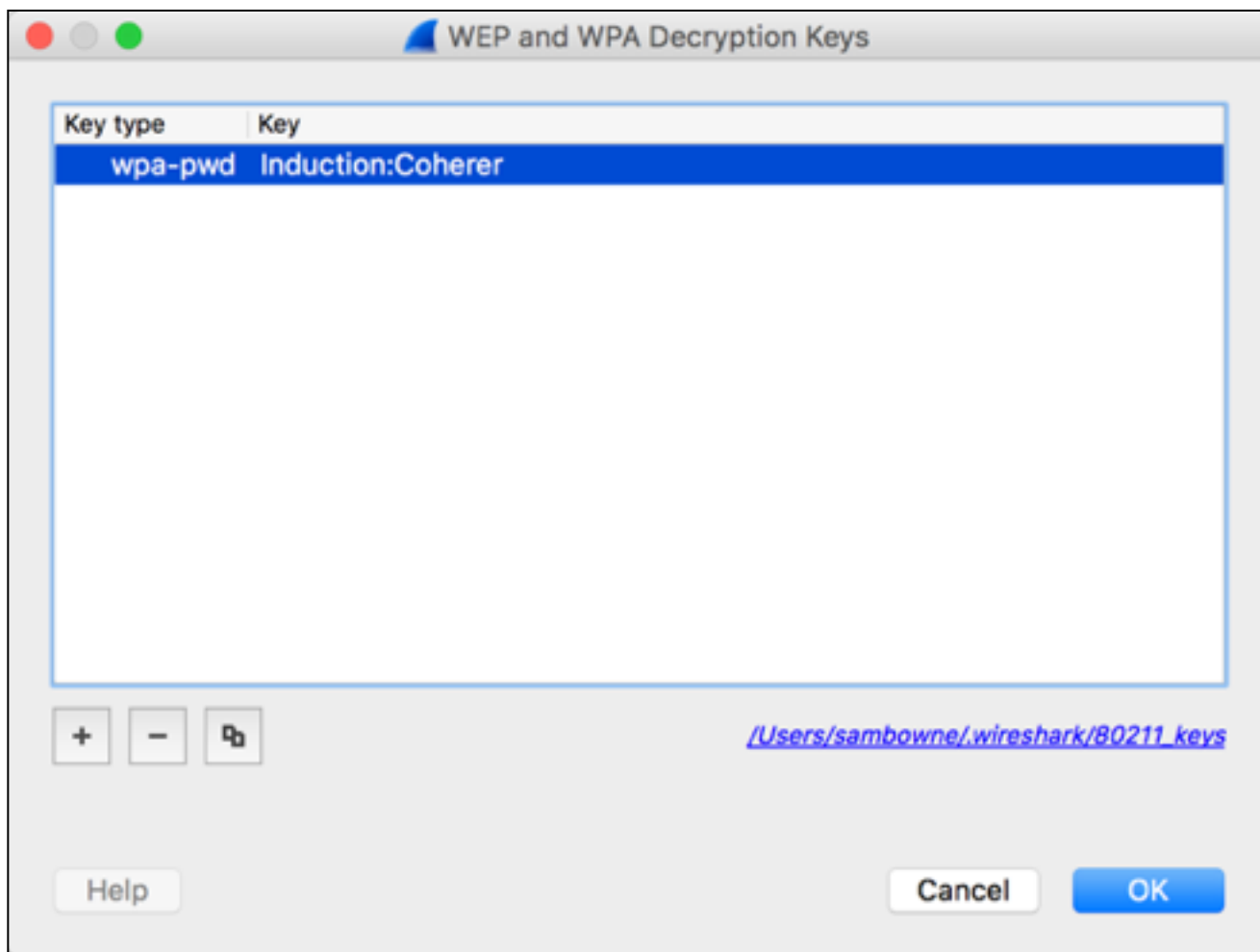
▶ 802.11 radio information

▶ IEEE 802.11 Data, Flags: .p.....TC

▼ Data (344 bytes)

Data: 7eccf60ac1ddffb04796c30ba19c92c6121e800390f5ef4a...

[Length: 344]



Decrypted Traffic

No.	Time	Source	Destination	Protocol	Length	Info
86	5...		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
87	5...	Cisco-Li_82:...	Apple_82:36...	EAPOL	181	Key (Message 1 of 4)
88	5...		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
89	5...	Apple_82:36:...	Cisco-Li_82...	EAPOL	181	Key (Message 2 of 4)
90	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
91	5...		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
92	5...	Cisco-Li_82:...	Apple_82:36...	EAPOL	239	Key (Message 3 of 4)
93	5...		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
94	5...	Apple_82:36:...	Cisco-Li_82...	EAPOL	159	Key (Message 4 of 4)
95	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
96	5...	Cisco-Li_82:...	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=.....C,
97	5...	Cisco-Li_82:...	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=.....C,
98	5...		Apple_82:36...	802.11	38	Clear-to-send, Flags=.....C
99	5...	0.0.0.0	255.255.255...	DHCP	404	DHCP Request - Transaction ID 0x3b0f7566
100	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
101	5...		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
102	5...	192.168.0.1	192.168.0.50	DHCP	652	DHCP ACK - Transaction ID 0x3b0f7566

▶ Frame 99: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▶ IEEE 802.11 Data, Flags: .p....TC
▶ Logical-Link Control
▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
▶ Bootstrap Protocol (Request)

Kahoot!

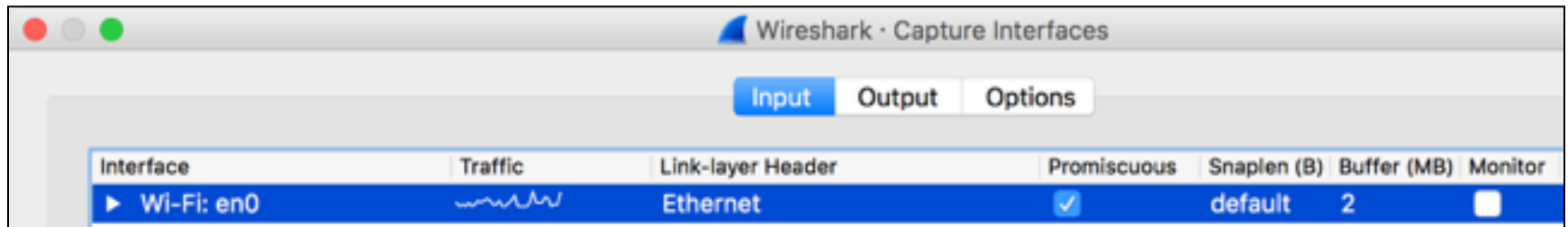
Wireshark

Promiscuous Mode in Wireshark

- Edit, Preferences
- Click "Capture" on left side
- "Capture packets in promiscuous mode on all network cards" on right side

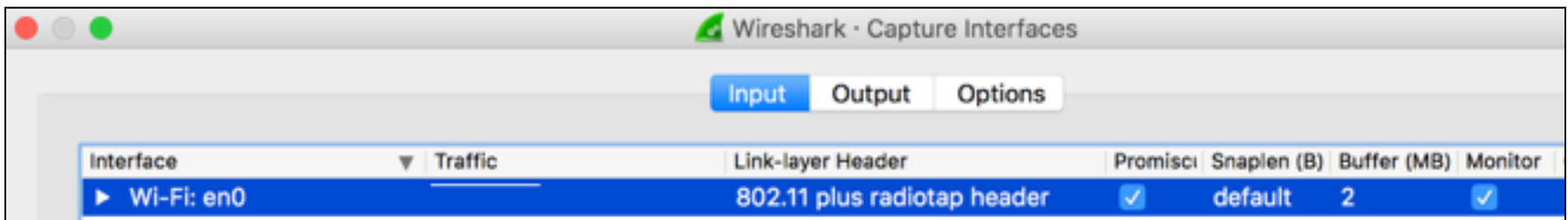
Monitor Mode in Wireshark

- On a Mac
 - Capture, Options
 - Normal: Promiscuous but not Monitor



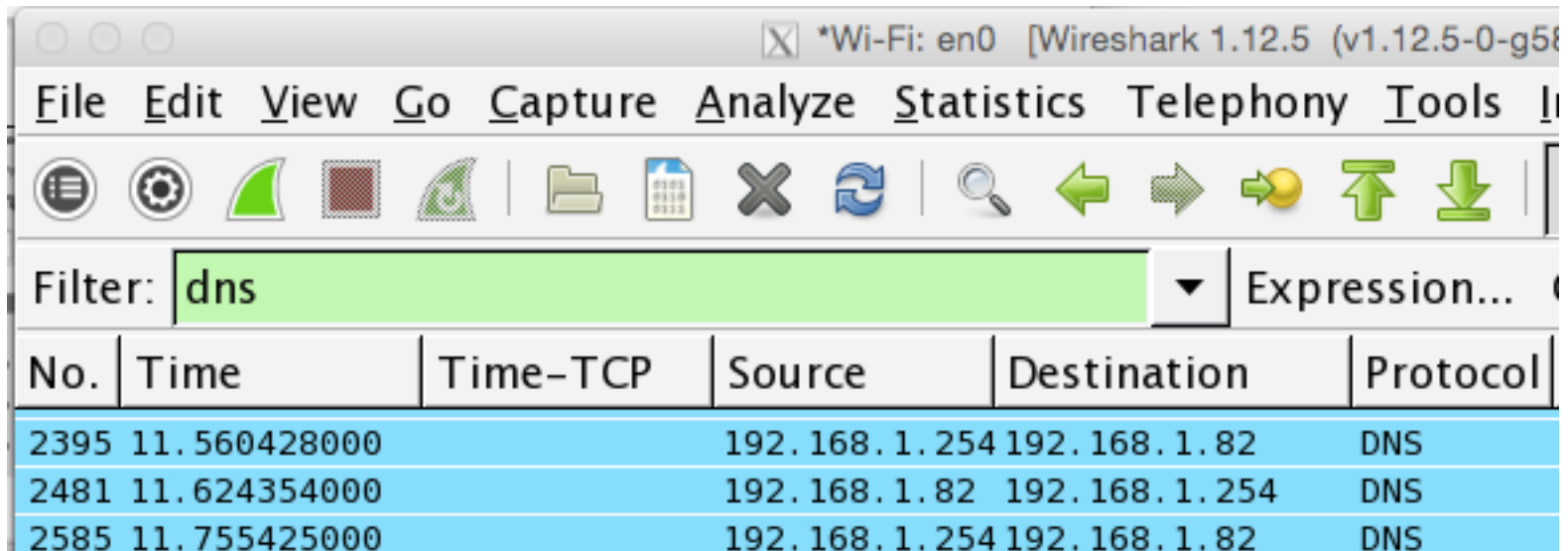
Monitor Mode in Wireshark

- Shows 802.11 management frames, like "Beacon"
- Not all NICs allow this



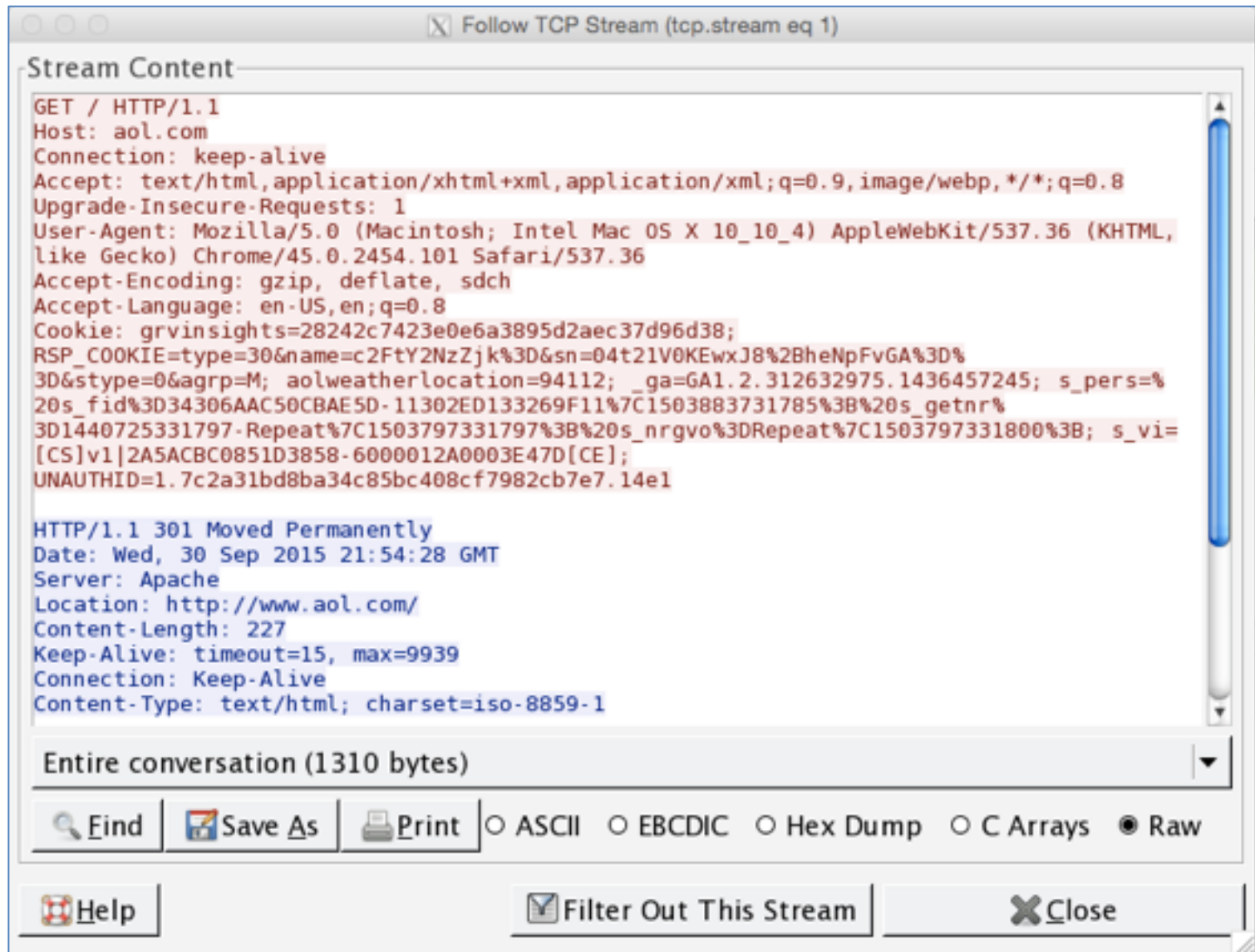
10	0.004002	8a:15:14:90:a6:ab	IntelCor_93:ad:...	802.11	55	QoS Null function (No data), SN=298, F...
11	0.025634	20:c0:d4:85:98:31...	82:cf:62:17:c4:...	802.11	350	Request-to-send, Flags=o..PR.F..
12	0.043326	8a:15:14:90:a6:af	Broadcast	802.11	296	Beacon frame, SN=299, FN=0, Flags=.....
13	0.043433	8a:15:14:90:a6:a3	Broadcast	802.11	332	Beacon frame, SN=300, FN=0, Flags=.....
14	0.043558	8a:15:14:90:a6:a9	Broadcast	802.11	385	Beacon frame, SN=301, FN=0, Flags=.....
15	0.043802	8a:15:14:90:a6:ab	Broadcast	802.11	387	Beacon frame, SN=302, FN=0, Flags=.....
16	0.043941	Meraki_19:1c:30	Broadcast	802.11	127	Data, SN=303, FN=0, Flags=.pm...F.C
17	0.044025	Meraki_19:1c:30	Broadcast	802.11	127	Data, SN=304, FN=0, Flags=.pm...F.C
18	0.044133	Meraki_19:1c:30	Broadcast	ARP	107	Who has 147.144.208.12? Tell 0.0.0.0
19	0.044217	Apple_d1:3f:89	Broadcast	802.11	131	Data, SN=306, FN=0, Flags=.p....F.C
20	0.044395	Apple_d1:3f:89	Broadcast	802.11	131	Data, SN=307, FN=0, Flags=.p....F.C

Display Filters



- frame contains attack
- Expression... button

Following a Stream



The screenshot shows a window titled "Follow TCP Stream (tcp.stream eq 1)". The main content area displays the following text:

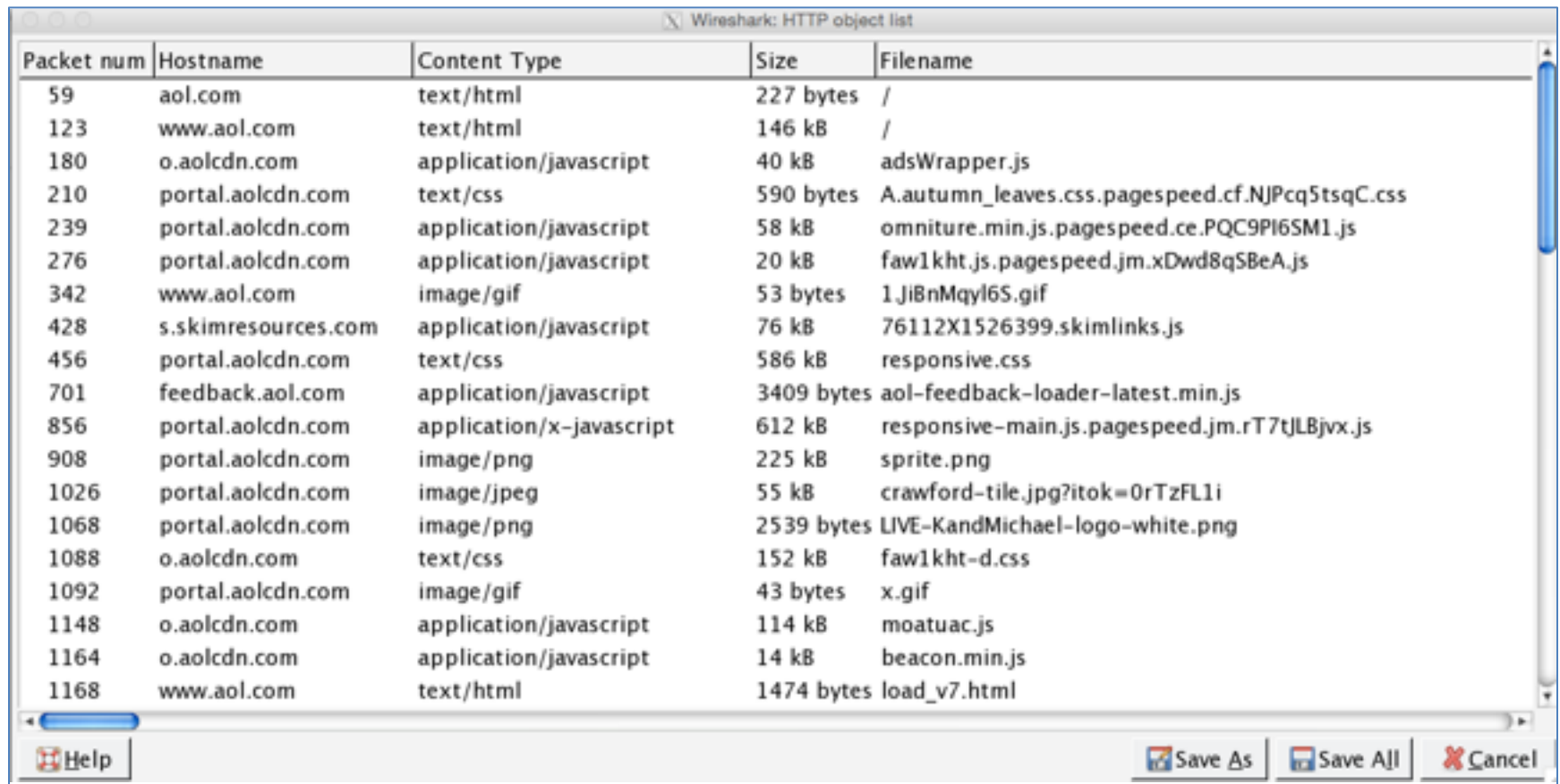
```
Stream Content
GET / HTTP/1.1
Host: aol.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/45.0.2454.101 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: grvinsights=28242c7423e0e6a3895d2aec37d96d38;
RSP_COOKIE=type=30&name=c2FtY2NzZjk%3D&sn=04t21V0KEwxJ8%2BheNpFvGA%3D%
3D&stype=0&agrp=M; aolweatherlocation=94112; _ga=GA1.2.312632975.1436457245; s_pers=%
20s_fid%3D34306AAC50CBAE5D-11302ED133269F11%7C1503883731785%3B%20s_getnr%
3D1440725331797-Repeat%7C1503797331797%3B%20s_nrgvo%3DRepeat%7C1503797331800%3B; s_vi=
[CS]v1|2A5ACBC0851D3858-6000012A0003E47D[CE];
UNAUTHID=1.7c2a31bd8ba34c85bc408cf7982cb7e7.14e1

HTTP/1.1 301 Moved Permanently
Date: Wed, 30 Sep 2015 21:54:28 GMT
Server: Apache
Location: http://www.aol.com/
Content-Length: 227
Keep-Alive: timeout=15, max=9939
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

Below the main content area, there is a dropdown menu showing "Entire conversation (1310 bytes)". At the bottom, there is a toolbar with the following options: Find, Save As, Print, ASCII, EBCDIC, Hex Dump, C Arrays, and Raw (selected). At the very bottom, there are buttons for Help, Filter Out This Stream, and Close.

Extracting Files

- File, Export Objects, HTTP



Wireshark: HTTP object list

Packet num	Hostname	Content Type	Size	Filename
59	aol.com	text/html	227 bytes	/
123	www.aol.com	text/html	146 kB	/
180	o.aolcdn.com	application/javascript	40 kB	adsWrapper.js
210	portal.aolcdn.com	text/css	590 bytes	A.autumn_leaves.css.pagespeed.cf.NJPcq5tsqC.css
239	portal.aolcdn.com	application/javascript	58 kB	omniture.min.js.pagespeed.ce.PQC9PI6SM1.js
276	portal.aolcdn.com	application/javascript	20 kB	faw1kht.js.pagespeed.jm.xDwd8q5BeA.js
342	www.aol.com	image/gif	53 bytes	1JiBnMqyl6S.gif
428	s.skimresources.com	application/javascript	76 kB	76112X1526399.skimlinks.js
456	portal.aolcdn.com	text/css	586 kB	responsive.css
701	feedback.aol.com	application/javascript	3409 bytes	aol-feedback-loader-latest.min.js
856	portal.aolcdn.com	application/x-javascript	612 kB	responsive-main.js.pagespeed.jm.rT7tJLBjvx.js
908	portal.aolcdn.com	image/png	225 kB	sprite.png
1026	portal.aolcdn.com	image/jpeg	55 kB	crawford-tile.jpg?itok=0rTzFL1i
1068	portal.aolcdn.com	image/png	2539 bytes	LIVE-KandMichael-logo-white.png
1088	o.aolcdn.com	text/css	152 kB	faw1kht-d.css
1092	portal.aolcdn.com	image/gif	43 bytes	x.gif
1148	o.aolcdn.com	application/javascript	114 kB	moatuac.js
1164	o.aolcdn.com	application/javascript	14 kB	beacon.min.js
1168	www.aol.com	text/html	1474 bytes	load_v7.html

Help Save As Save All Cancel

ARP Cache Poisoning

ARP Cache Poisoning

- Client tricked into sending packets to the wrong MAC Address
- Attacker must be on target's LAN

```
C:\Windows\system32>arp -a
```

```
Interface: 10.0.0.2 --- 0xb
```

Internet Address	Physical Address	Type
10.0.0.1	00-0c-29-82-4f-64	dynamic
10.0.0.3	00-0c-29-82-4f-64	dynamic
10.255.255.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static

DNS Cache Poisoning

DNS Cache Poisoning (Client)

- Attacker sends false DNS replies
- Target is tricked into storing the wrong IP address for a domain name
- Attacker is usually on the same LAN
 - May not always be required
- DNSSEC might stop this someday
 - But not today

DNS Cache Poisoning (Server)

- Attacker can poison remote, shared DNS servers
 - Like Comcast DNS servers
- Affects many users
- Dan Kaminsky figured this out
- Patched in 2008
- DNSSEC will patch it more thoroughly

SSLstrip

sslstrip Proxy Changes HTTPS to HTTP

To
Internet

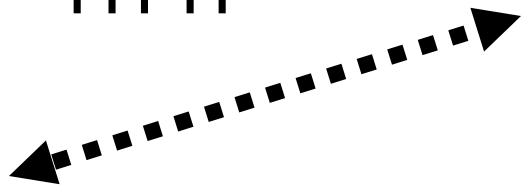


HTTPS



Attacker:
sslstrip
Proxy
in the
Middle

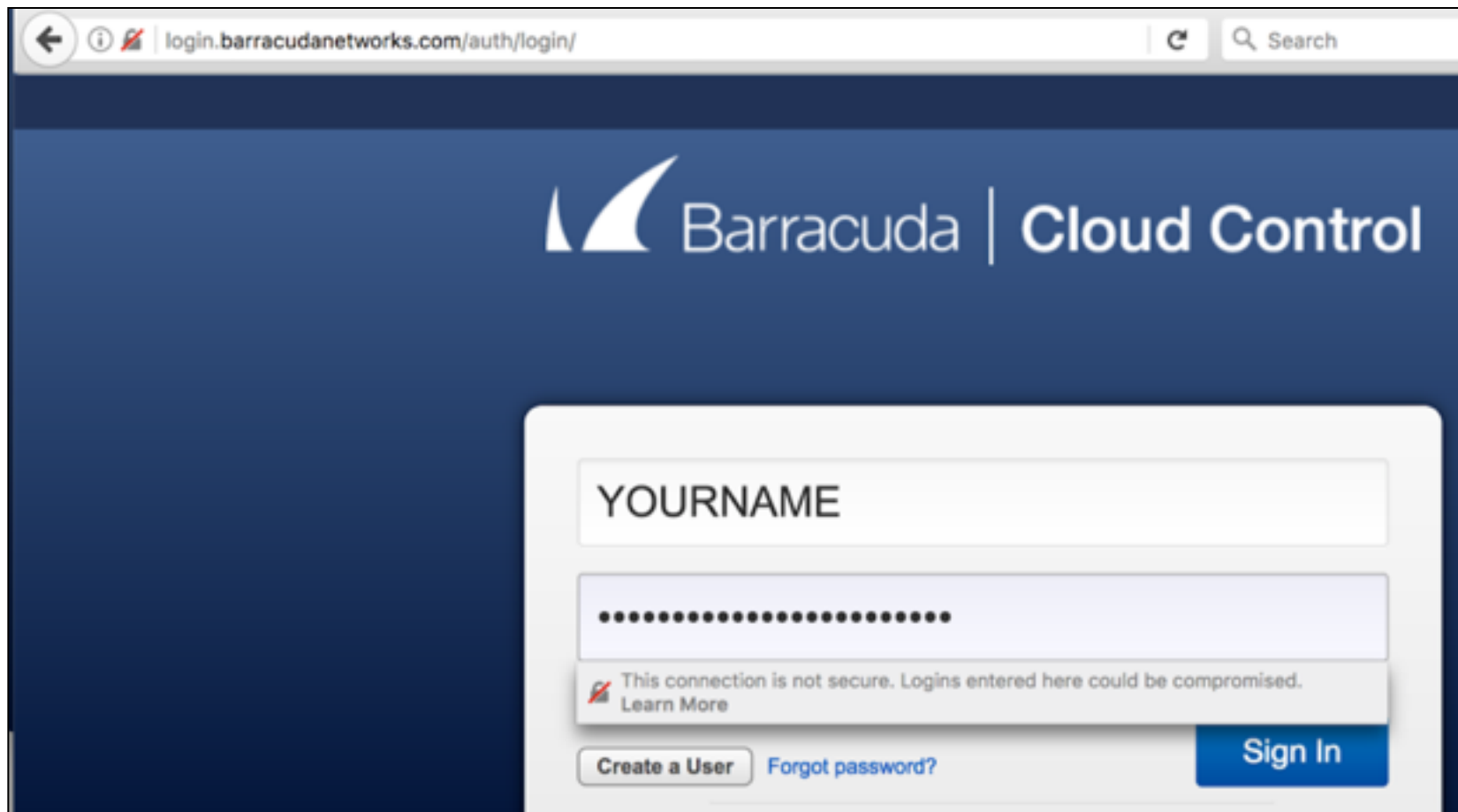
HTTP



Target
Using
Facebook

Sslstrip Vulnerability


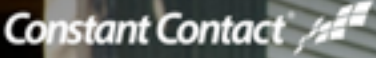
- If you go directly to an HTTPS URL, you are not vulnerable
- But many sites use a 302 redirect from HTTP to HTTPS, rendering them vulnerable



```
2017-10-05 12:59:52,407 Sending header: cookie : CLOUD_LOCALE=en_US; BNI00; cloud_session=iospd0di7gdq4k87a9pkr3rsl1
2017-10-05 12:59:52,407 Sending header: content-type : application/x-www
2017-10-05 12:59:52,407 SECURE POST Data (login.barracudanetworks.com):
username=YOURNAME&password=YOURNAME-SECRET-PASSWORD&mfa_input=&login_tok
1981e5e8ae54948743a8569f60b48f4&service=&csrf_token=3d555136a0047a731a83
75a269be66752-1507222627&form=&csrf_token=2d855bdde39638868c686e4ba65dee
```

Constant Contact : Login

login.constantcontact.com/login/login.sdo?goto=https? Search



Wright-Locke Farm

Log in


CC-USER

Enter password

This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

The Apache Software Found: X

donate.apache.org/login Search



Email

test@aol.com

Password

This connection is not secure. Logins entered here could be compromised. [Learn More](#)

Stay logged in

online.adp.com/portal/login.html

Welcome to the ADP® Portal

User ID [Administrator Sign In](#)

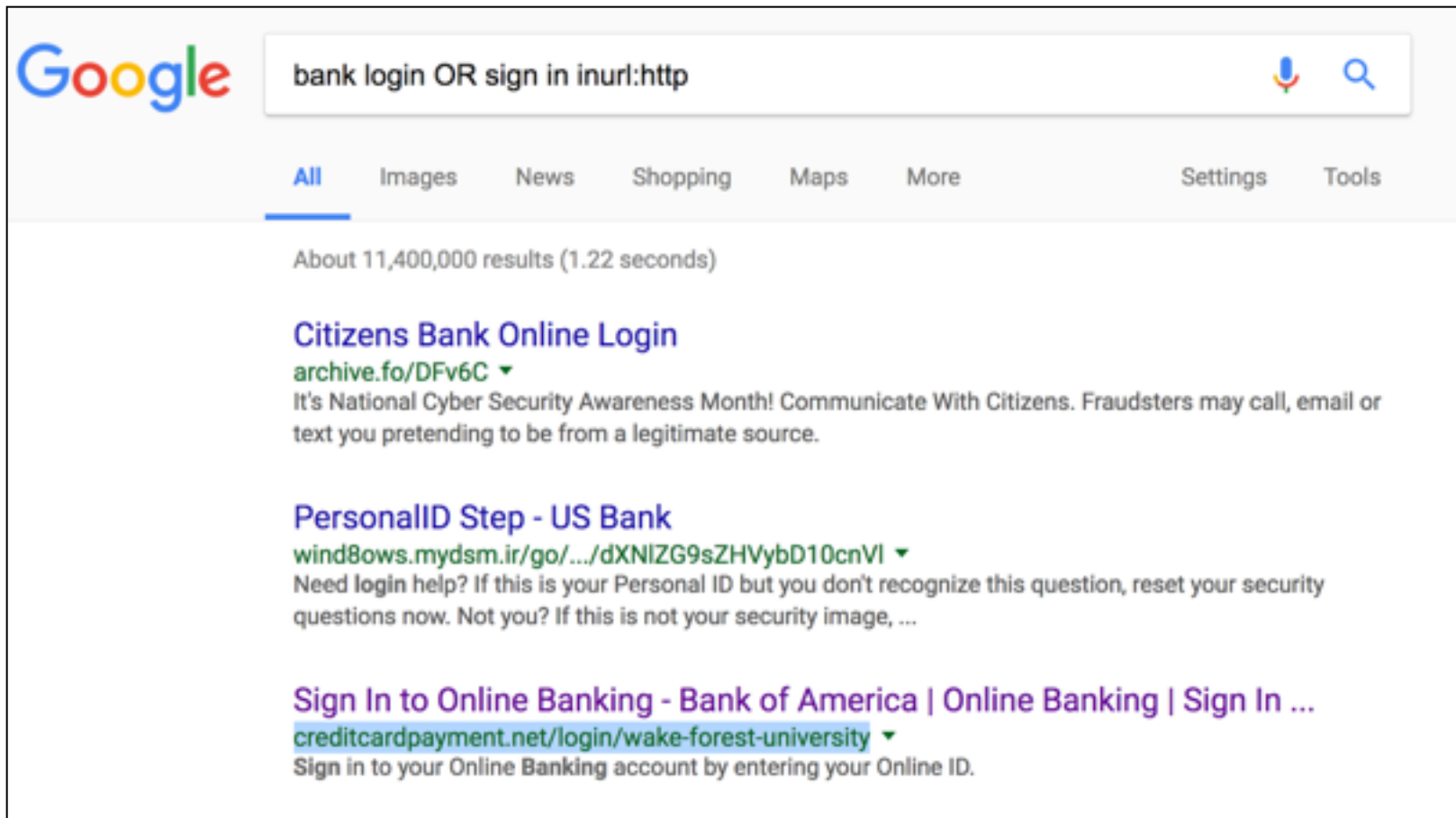
admin

Remember My User ID

Password (case sensitive)

This connection is not secure. Logins entered here could be compromised. [Learn More](#)

Dork for sslstrip Vulnerability



The image shows a Google search results page. The search bar contains the query "bank login OR sign in inurl:http". The search results are displayed below the navigation tabs. The first result is "Citizens Bank Online Login" with a snippet about National Cyber Security Awareness Month. The second result is "PersonalID Step - US Bank" with a snippet about login help. The third result is "Sign In to Online Banking - Bank of America | Online Banking | Sign In ..." with a snippet about signing in to an account.

Google bank login OR sign in inurl:http

[All](#) [Images](#) [News](#) [Shopping](#) [Maps](#) [More](#) [Settings](#) [Tools](#)

About 11,400,000 results (1.22 seconds)

Citizens Bank Online Login
archive.fo/DFv6C ▾
It's National Cyber Security Awareness Month! Communicate With Citizens. Fraudsters may call, email or text you pretending to be from a legitimate source.

PersonalID Step - US Bank
wind8ows.mydsm.ir/go/.../dXNIZG9sZHVybD10cnVI ▾
Need login help? If this is your Personal ID but you don't recognize this question, reset your security questions now. Not you? If this is not your security image, ...

Sign In to Online Banking - Bank of America | Online Banking | Sign In ...
creditcardpayment.net/login/wake-forest-university ▾
Sign in to your Online Banking account by entering your Online ID.

HTTP 301 Redirect

The screenshot shows a web browser window with the Bank of America login page. The address bar displays the URL: `https://secure.bankofamerica.com/login/sign-in/signOnV2Screen...`. The browser's developer tools are open to the Network tab, showing a list of network requests. The first request, `wake-forest-university creditcardpayment.net/login`, has a status of 301 (Moved Permanently) and a type of `text/...`. The second request, `signOnScreen.go?screenMsg=&req... /login/sign-in`, also has a status of 301 and a type of `Redirect`. The third request, `signOnV2Screen.go?screenMsg=&r... /login/sign-in`, has a status of 200 (OK) and a type of `docu... Redirect`. The remaining requests are for CSS and JavaScript files, all with a status of 200 (OK).

Name	Status	Type	Initiator	Size	Waterfall
wake-forest-university creditcardpayment.net/login	301 Moved Per...	text/...	Other	(fro...)	
signOnScreen.go?screenMsg=&req... /login/sign-in	301 Moved Per...	Redirect	creditcard...	(fro...)	
signOnV2Screen.go?screenMsg=&r... /login/sign-in	200 OK	docu... Redirect	/login/sign...	21.5 ...	
vipaa-v3-jawr.css /pa/components/bundles/gzip-com...	200 OK	style...	signOnV2S...	(fro...)	
vipaa-v3-jawr.js /pa/components/bundles/gzip-com...	200 OK	script	signOnV2S...	(fro...)	
cm-jawr.js /pa/components/bundles/gzip-com...	200 OK	script	signOnV2S...	(fro...)	

Stealing Password

The screenshot displays a Windows 10 desktop environment. In the foreground, a Kali Linux terminal window is open, showing the output of a `ssllstrip` command. The terminal output is a long, dense string of hexadecimal data, which is the captured SSL traffic for the login page. In the background, the Bank of America login page is visible. The page title is "Bank of America | Online Banking". The URL in the address bar is `secure.bankofamerica.com/login/sign-in/signOnV25c`. The page contains a "Sign In" button, a "Sign In to Online Banking" link, and a warning message: "We don't recognize your Online ID and/or Passcode. Please try again or". Below the warning, there are input fields for "Online ID" (containing "TEST-USER") and "Passcode" (containing "*****"). A "Forgot your Passcode?" link is also present. A security warning at the bottom of the page states: "This connection is not secure. Logins entered here could be compromised. Learn More".

Kahoot!