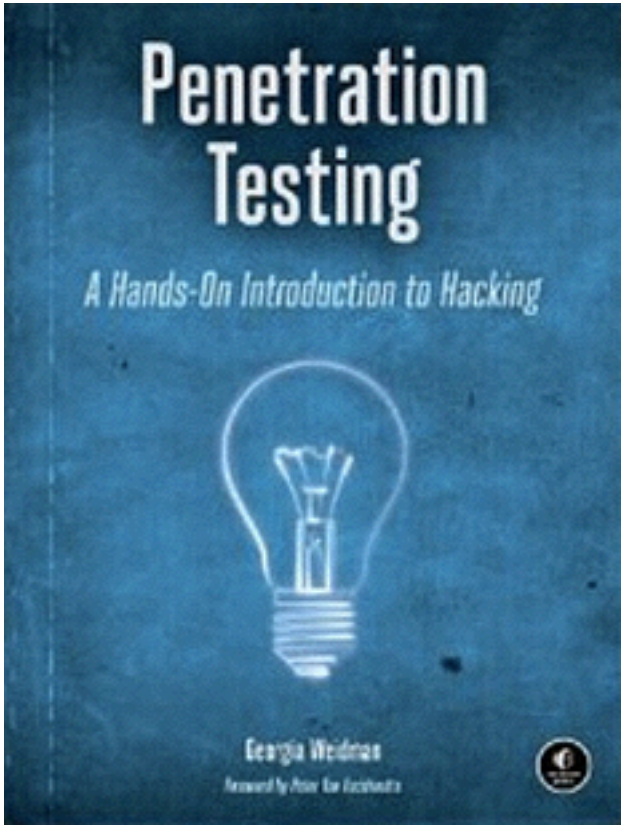
# CNIT 124: Advanced Ethical Hacking




## 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

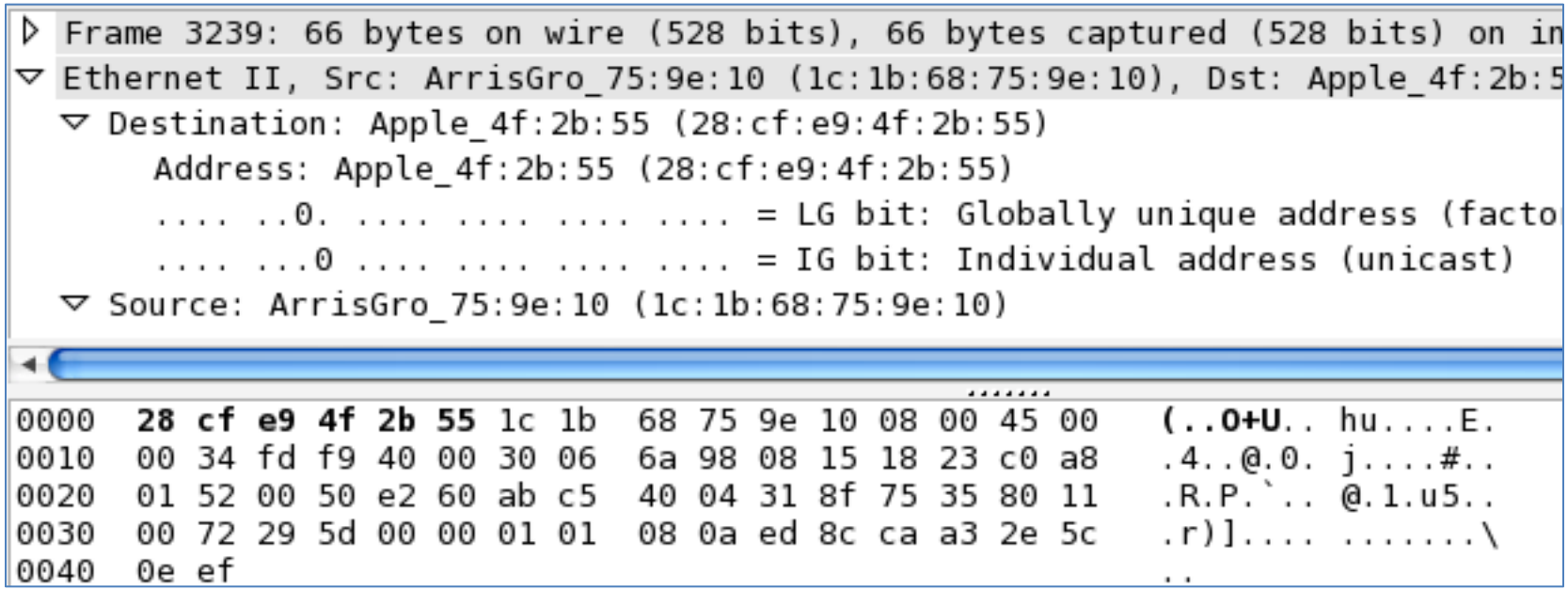
# Switches, Hubs and Wireless Networks

# 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



# Ethernet Promiscuous Mode

- If Destination MAC != 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

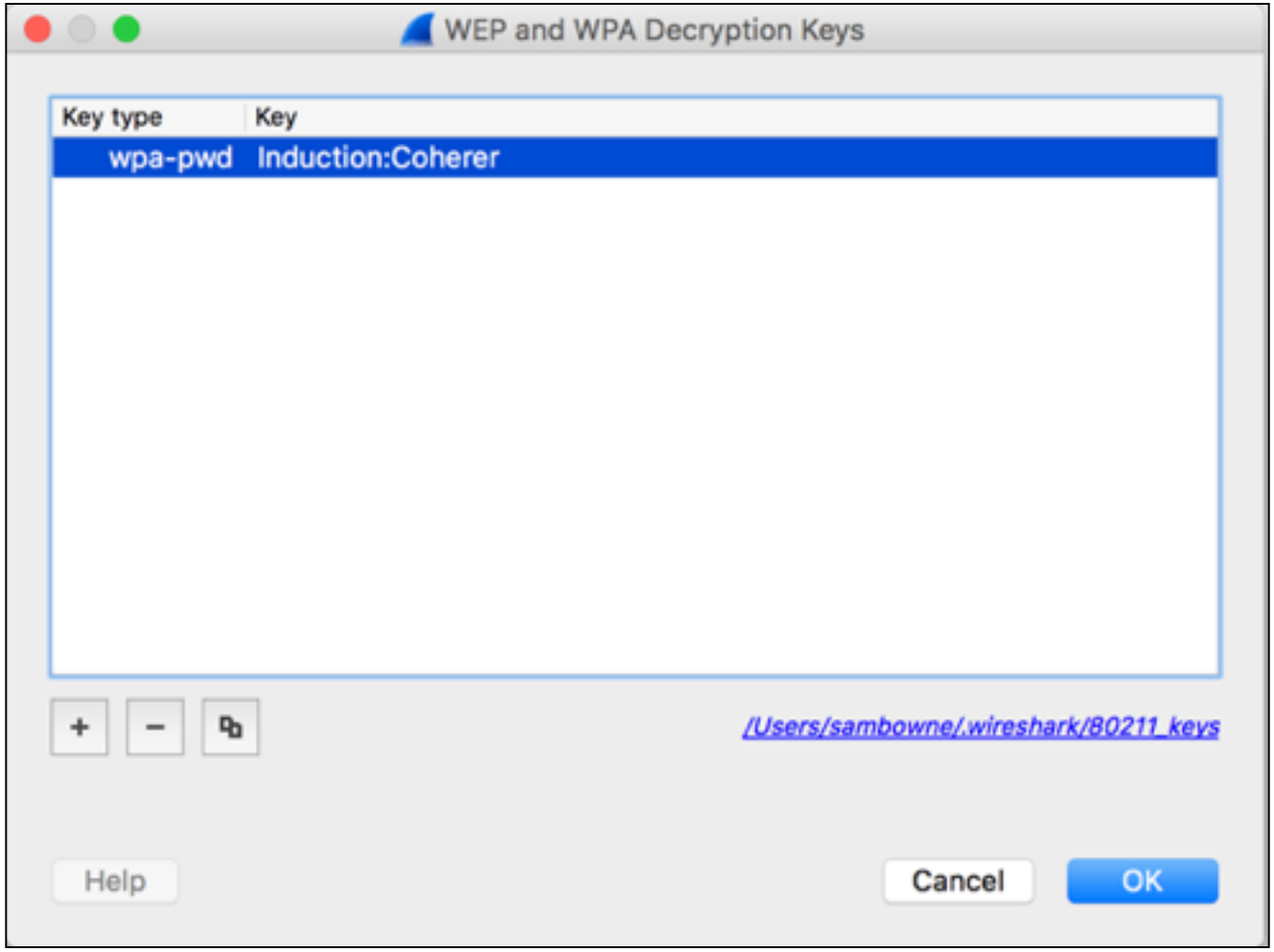
# Wireless LANs

- 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.

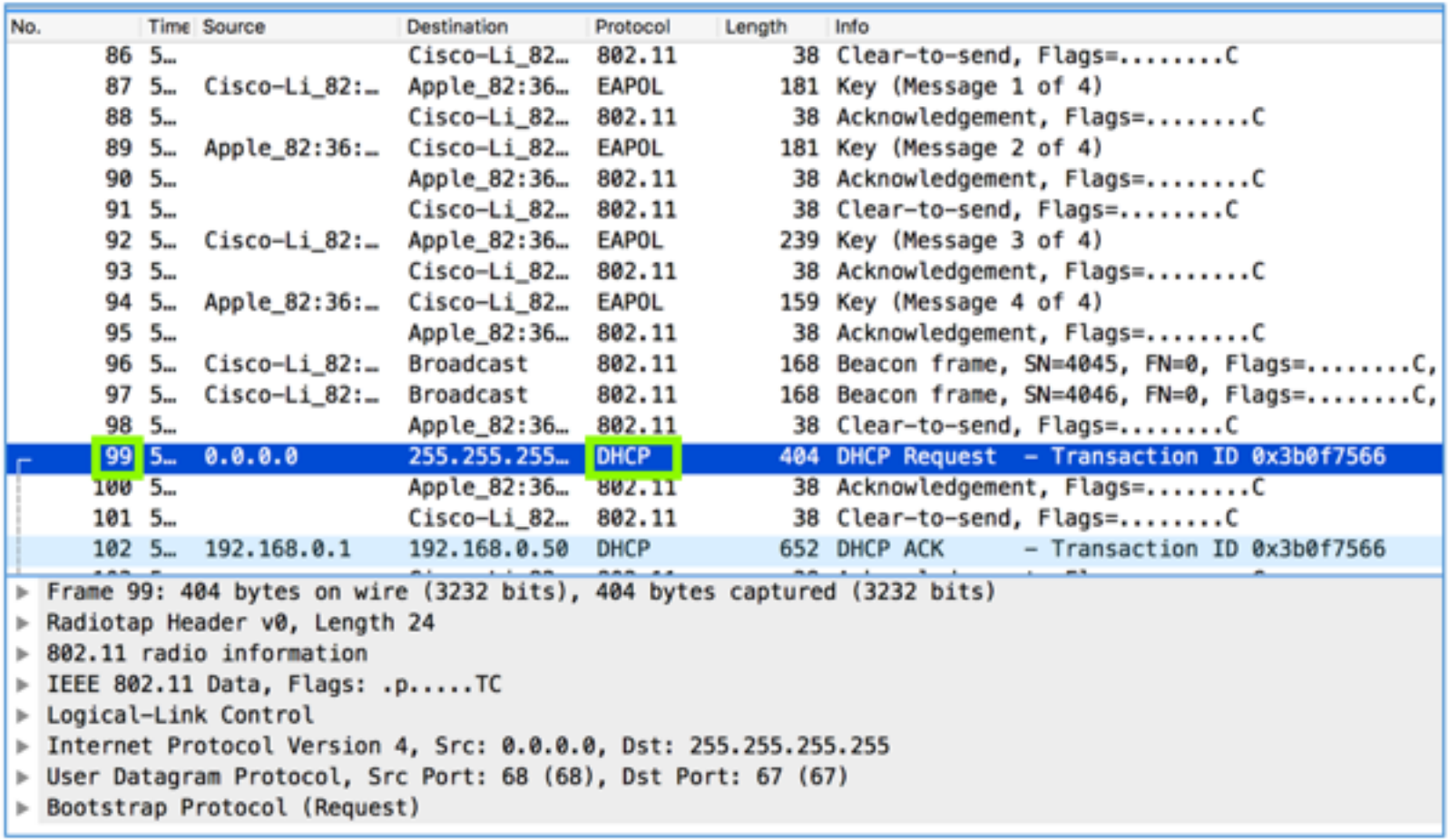
# Encrypted WPA2 Traffic

| 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]
```


WEP and WPA Decryption Keys
Key type
Key
wpa-pwd
Induction:Coherer
/Users/sambowne/.wireshark/80211_keys
Help
Cancel
OK

# 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!

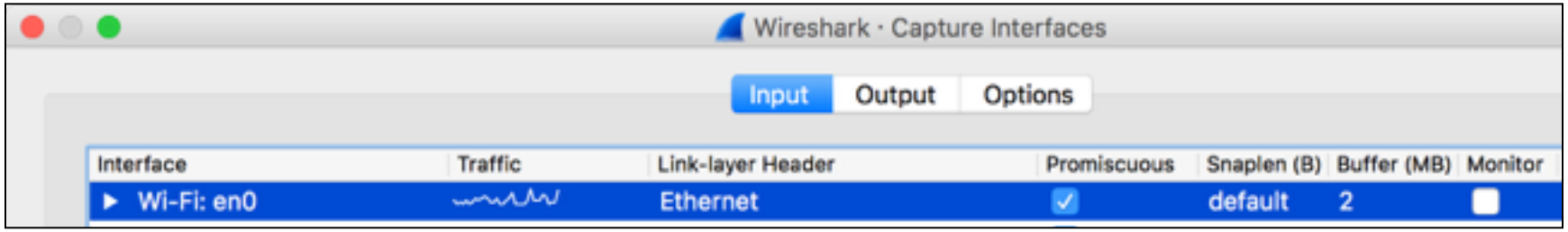
# Wireshark

# Promiscuous Mode in Wireshark

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

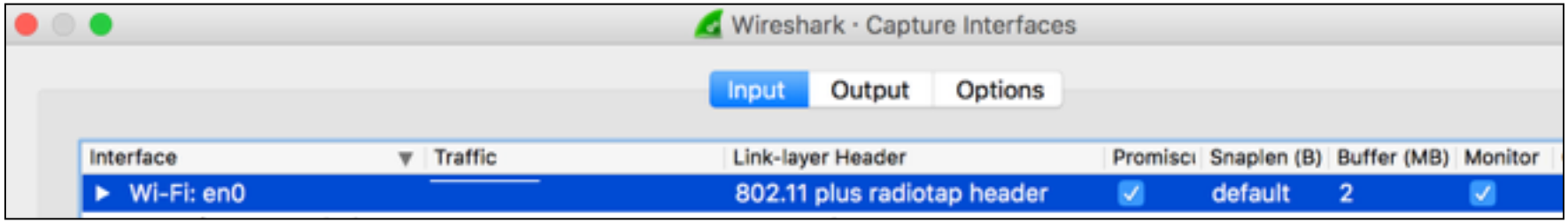
# Monitor Mode in Wireshark

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



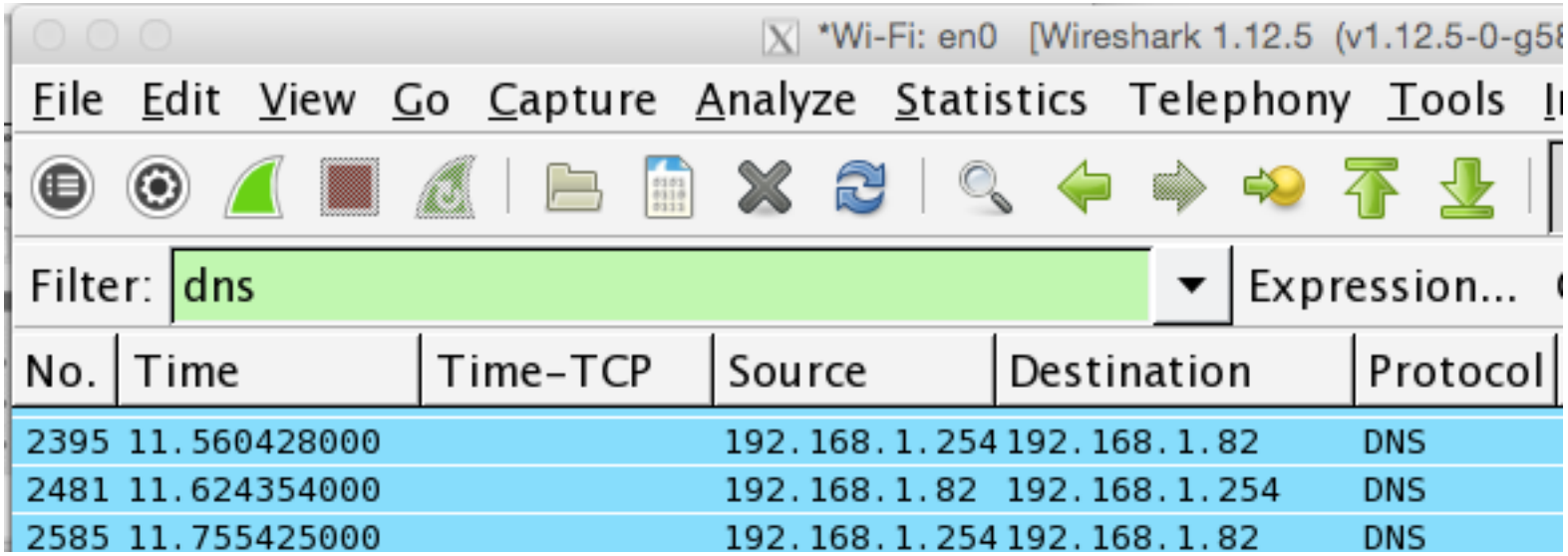
# Monitor Mode in Wireshark

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



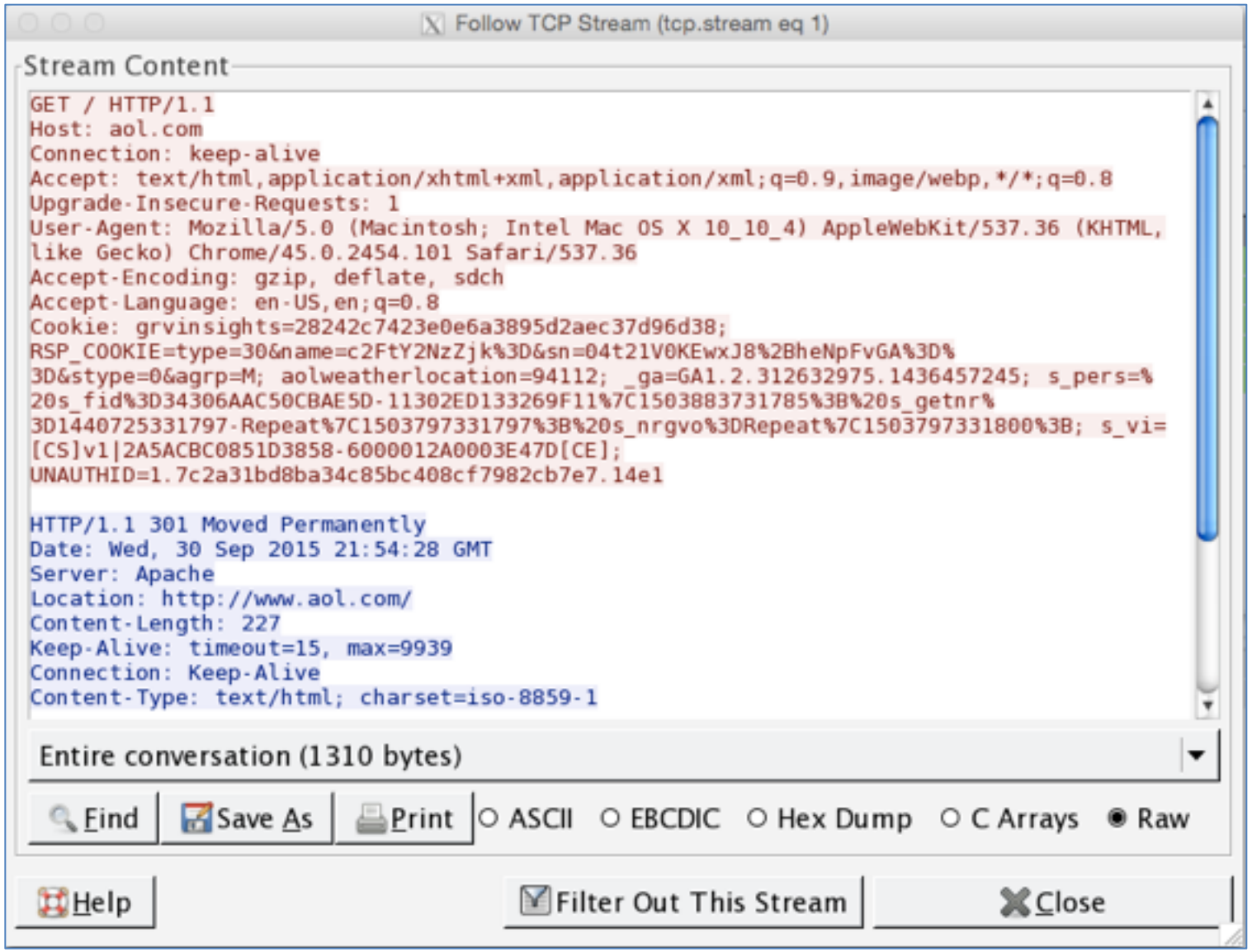

| | | | | | | |
|---|---|---|---|---|---|---|
| 10 | 0.004002 | 8a:15:14:90:a6:ab | IntelCor_93:ad:… | 802.11 | 55 | QoS Null function (No data), SN=298, F… |
| 11 | 0.025634 | 20:c0:d4:85:98:31… | 82:cf:62:17:c4:… | 802.11 | 350 | Request-to-send, Flags=o..PR.F.. |
| 12 | 0.043326 | 8a:15:14:90:a6:af | 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



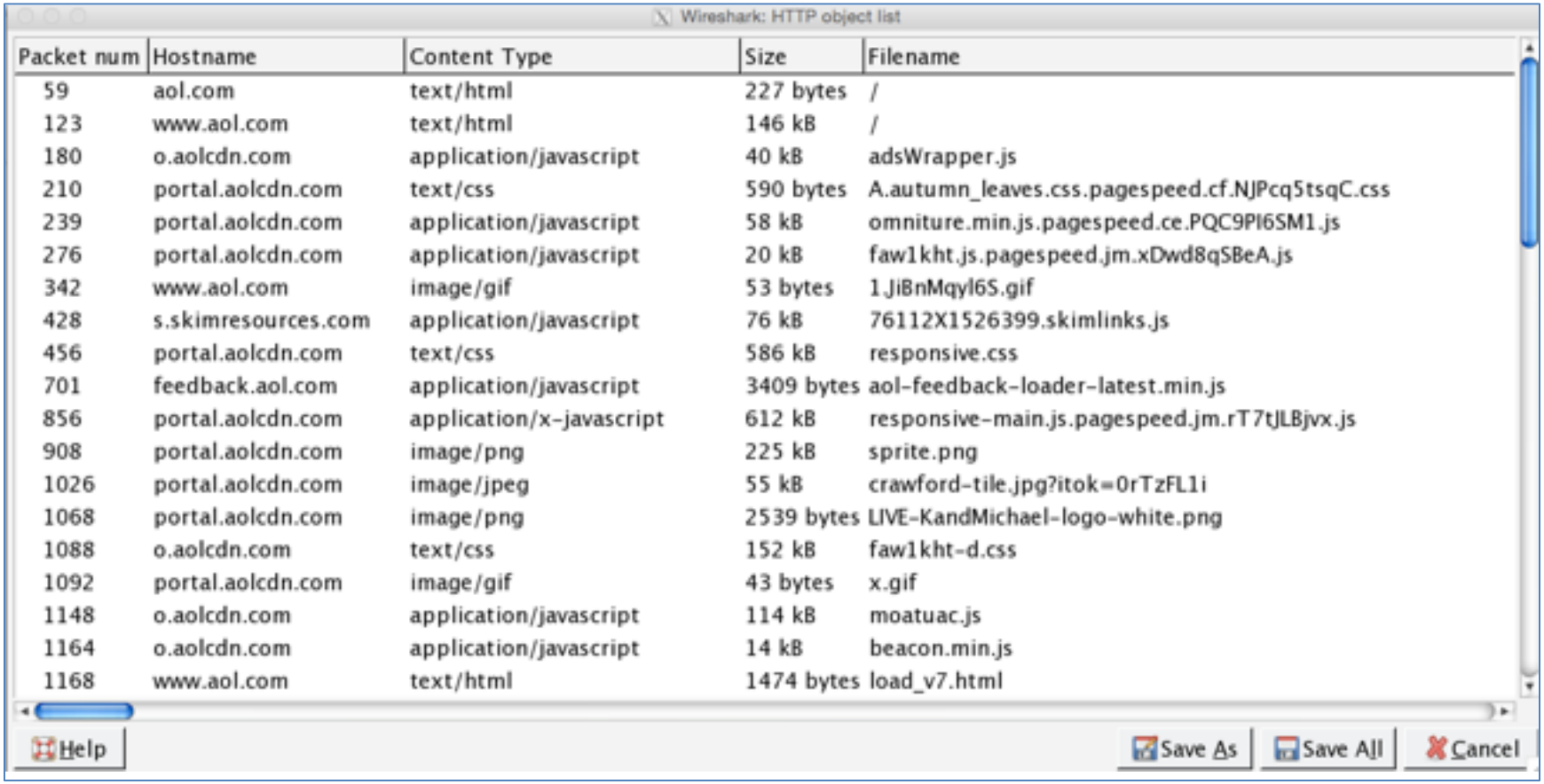

- frame contains attack
- Expression... button

# Following a Stream



# Extracting Files

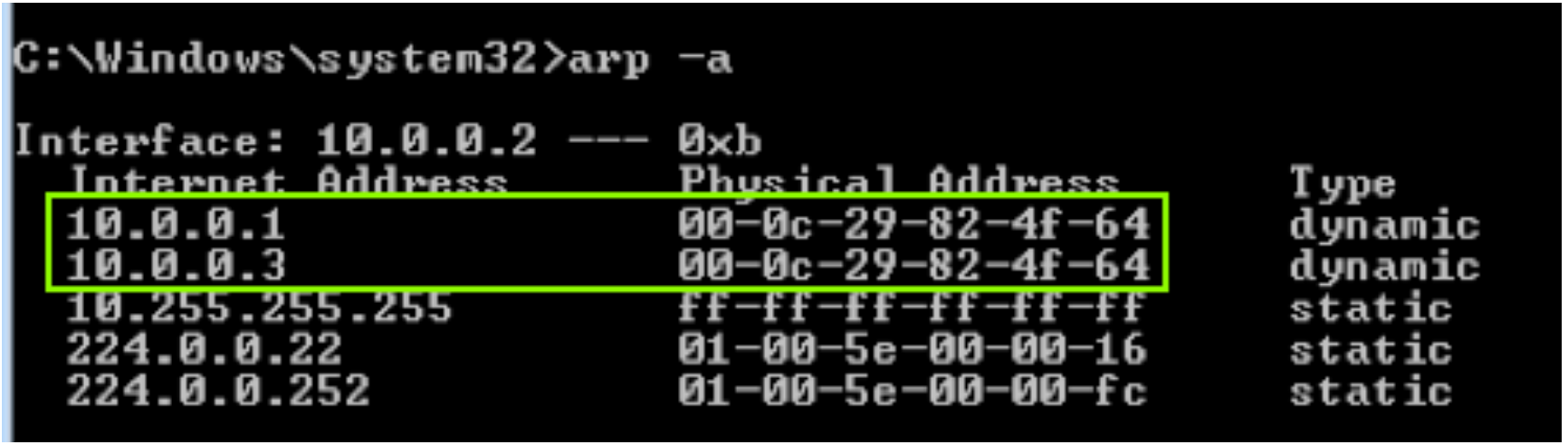
- File, Export Objects, HTTP



# ARP Cache Poisoning

# ARP Cache Poisoning

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



# DNS Cache Poisoning

# DNS Cache Poisoning (Client)

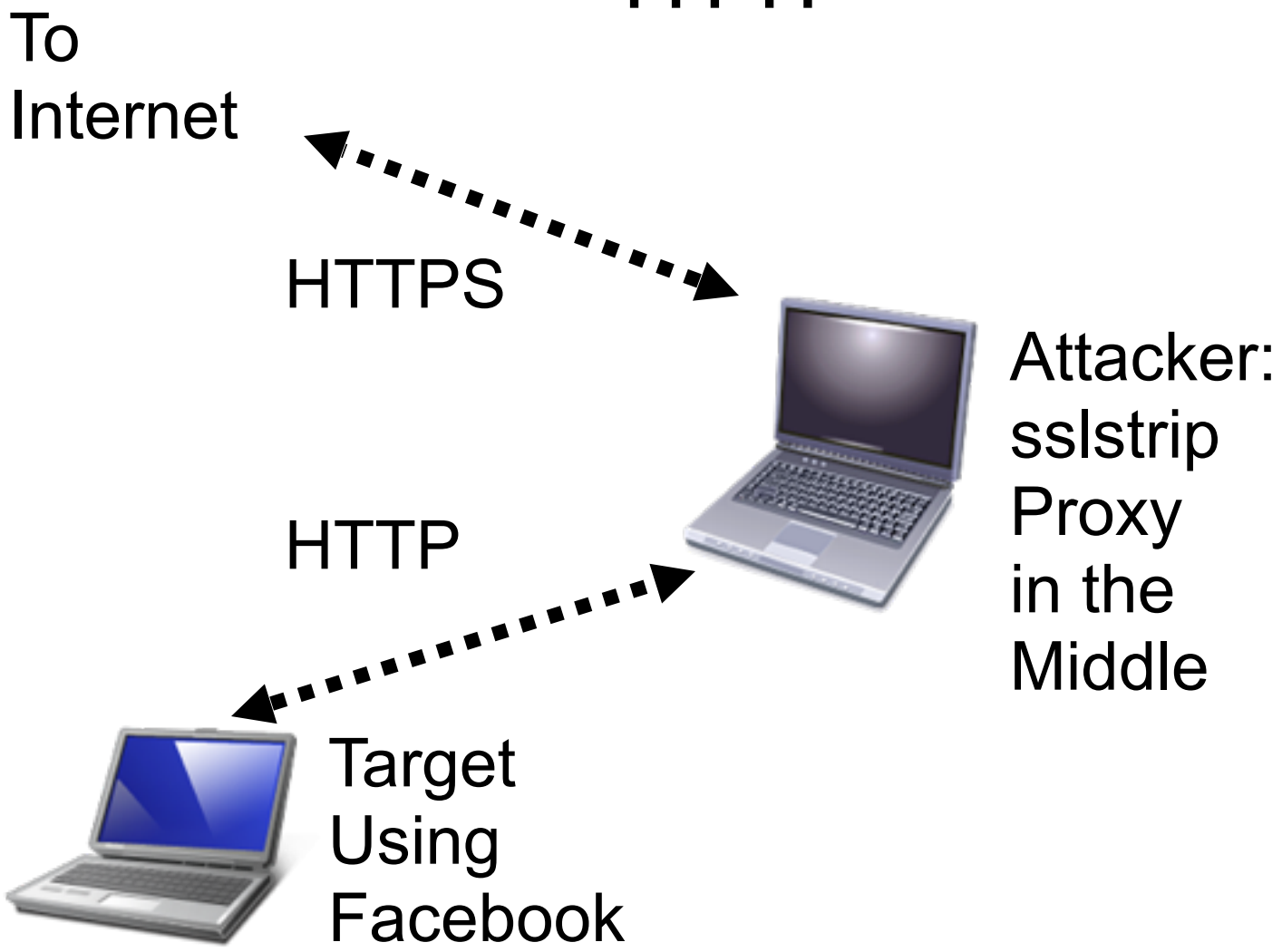
- Attacker sends false DNS replies
- Target is tricked into storing the wrong IP address for a domain name
- Attacker is usually on the same LAN
  - May not always be required
- DNSSEC might stop this someday
  - But not today

# 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

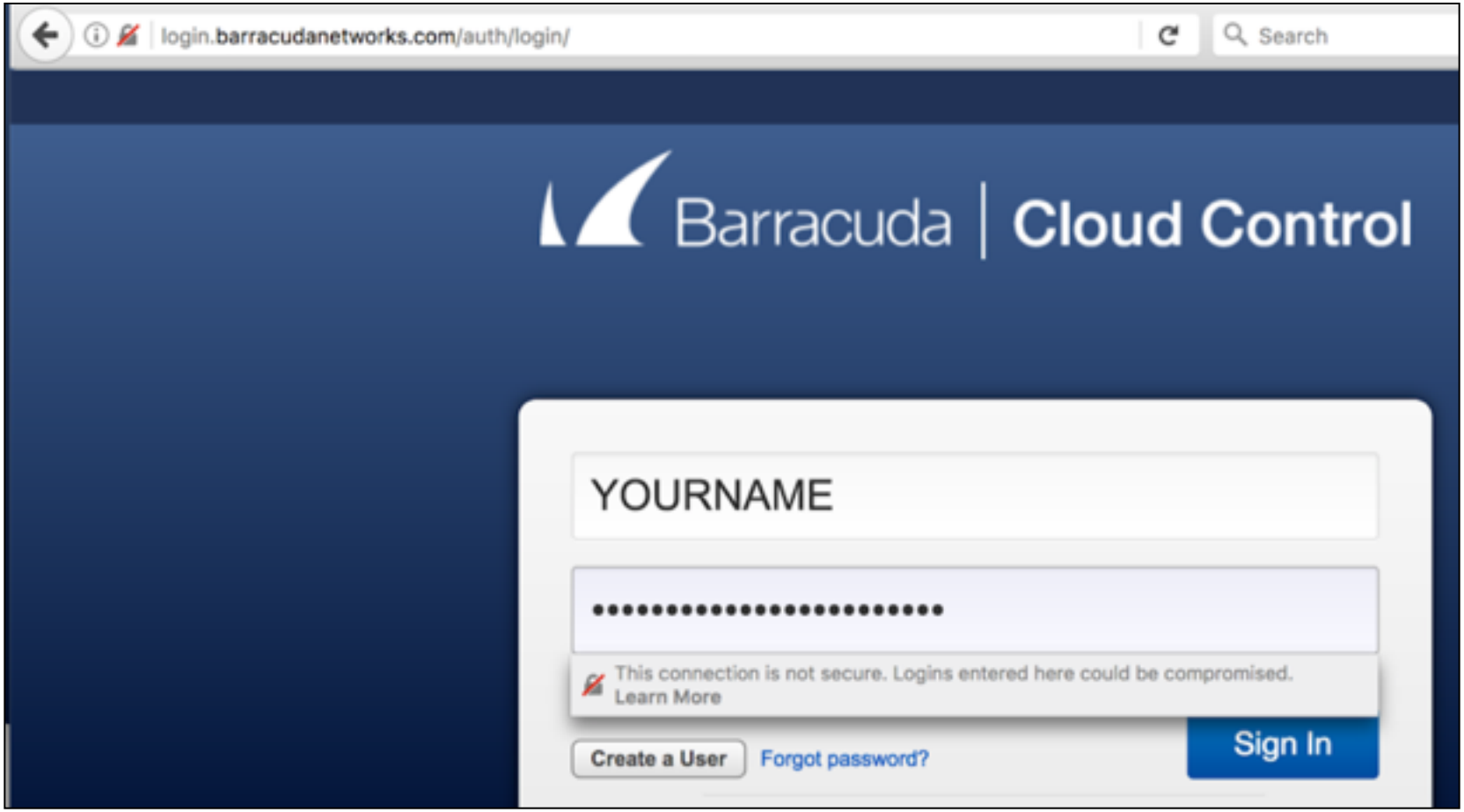
# SSLstrip

# sslstrip Proxy Changes HTTPS to HTTP

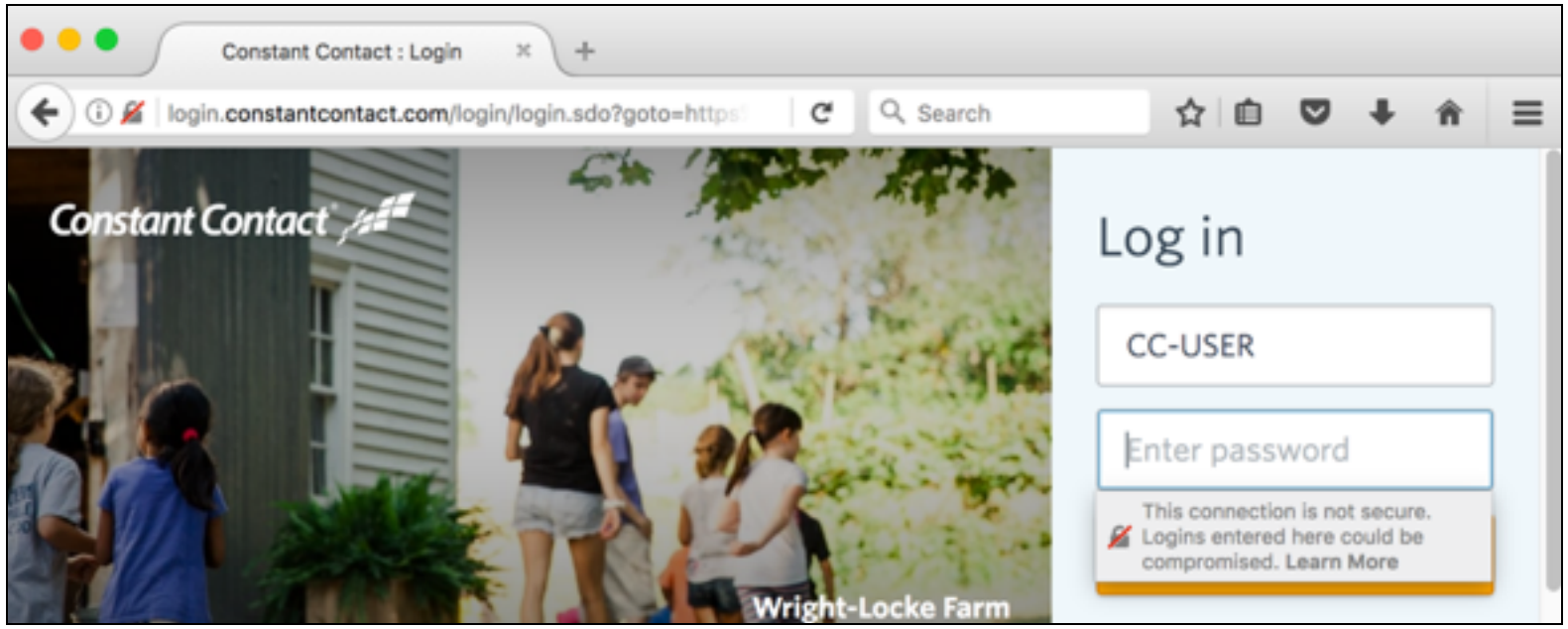


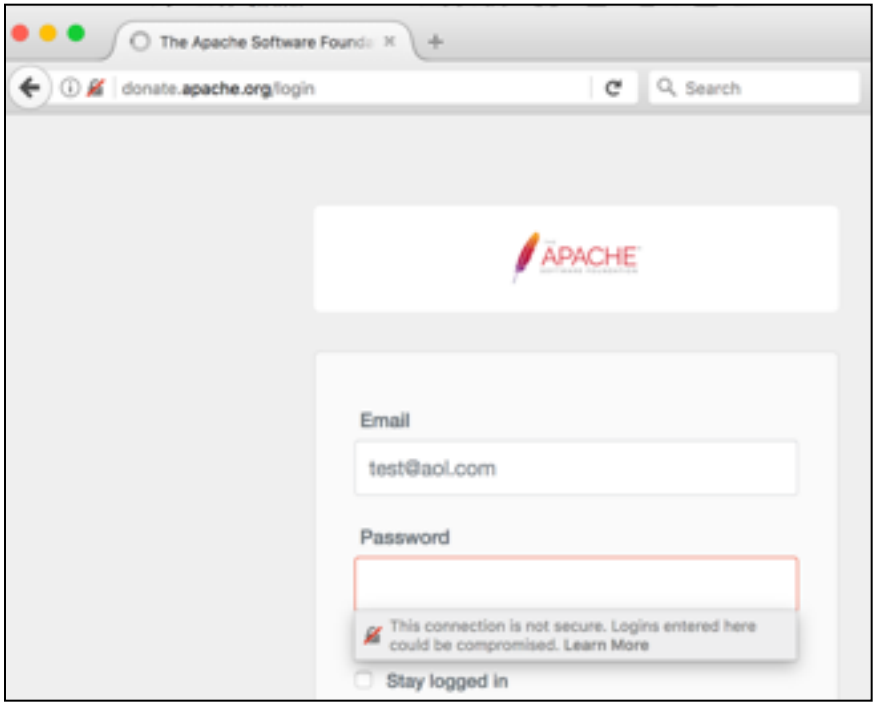
# Sslstrip Vulnerability

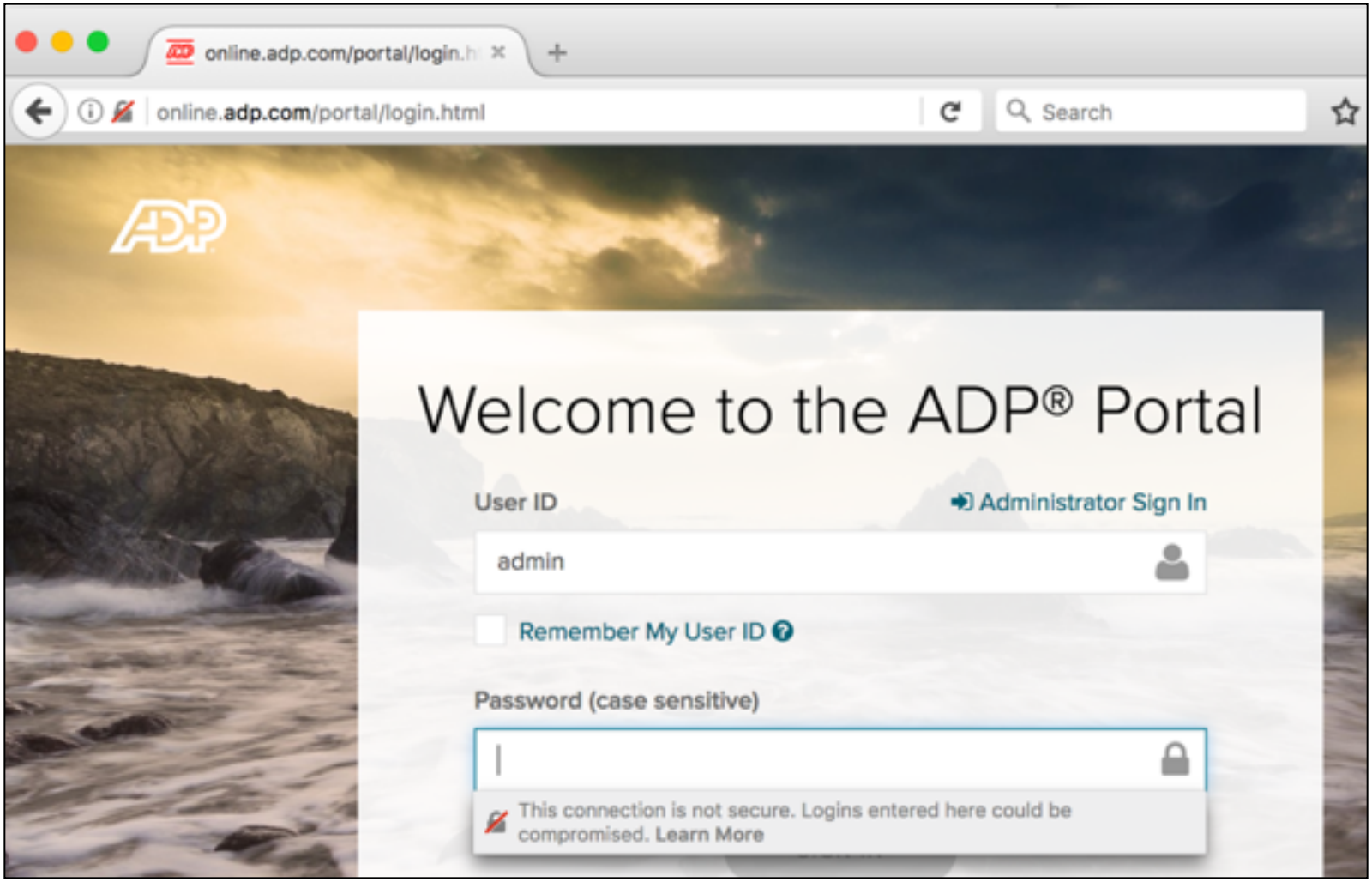
- If you go directly to an HTTPS URL, you are not vulnerable
- But many sites use a 302 redirect from HTTP to HTTPS, rendering them vulnerable



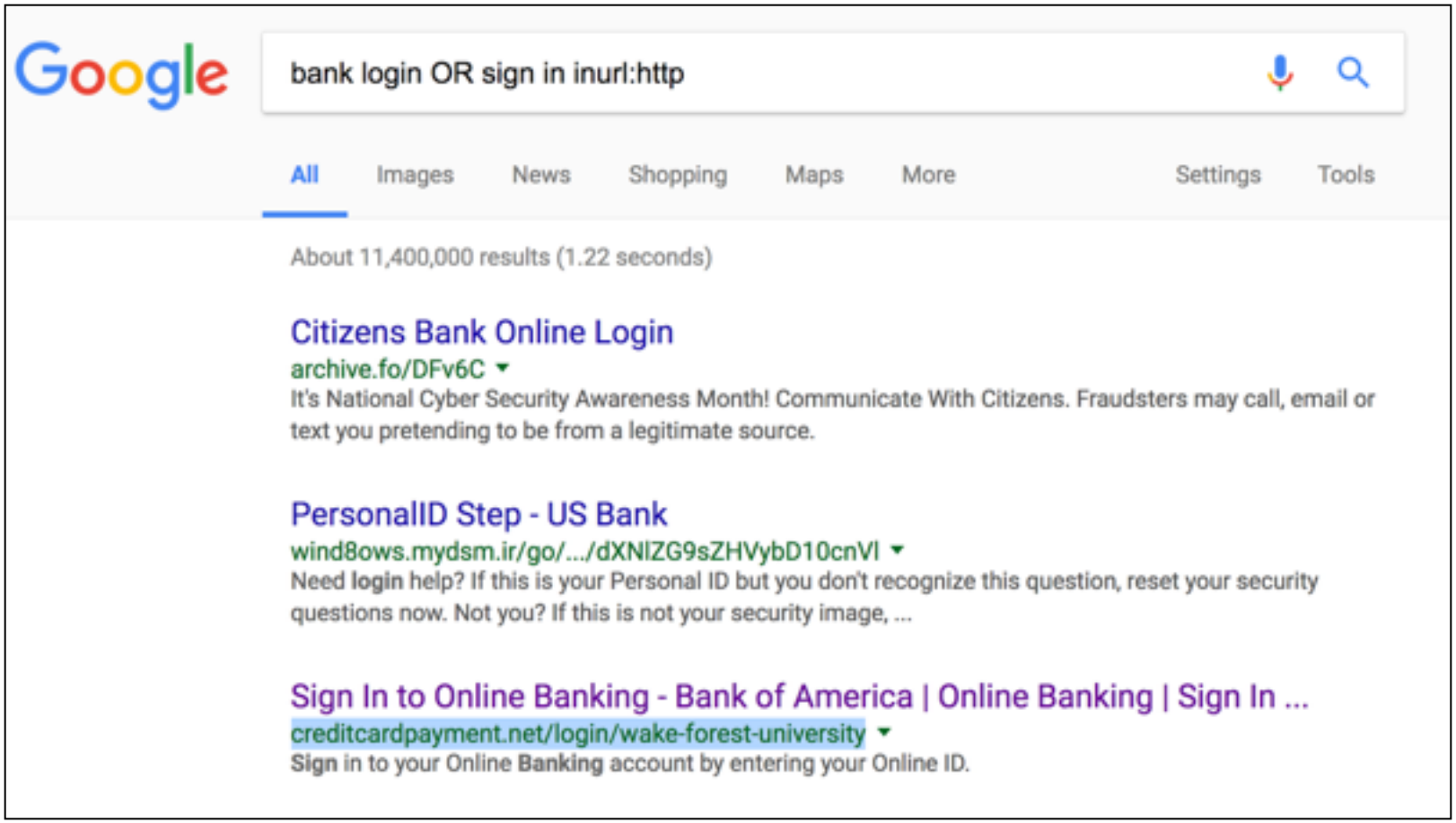

```
2017-10-05 12:59:52,407 Sending header: cookie : CLOUD_LOCALE=en_US; BNI
00; cloud_session=iospd0di7gdq4k87a9pkr3rsl1
2017-10-05 12:59:52,407 Sending header: content-type : application/x-www
2017-10-05 12:59:52,407 SECURE POST Data (login.barracudanetworks.com):
username=YOURNAME&password=YOURNAME-SECRET-PASSWORD&mfa_input=&login_tok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


Constant Contact : Login
login.constantcontact.com/login/login.sdo?goto=https
Search
Constant Contact
Wright-Locke Farm
Log in
CC-USER
Enter password
This connection is not secure. Logins entered here could be compromised. Learn More

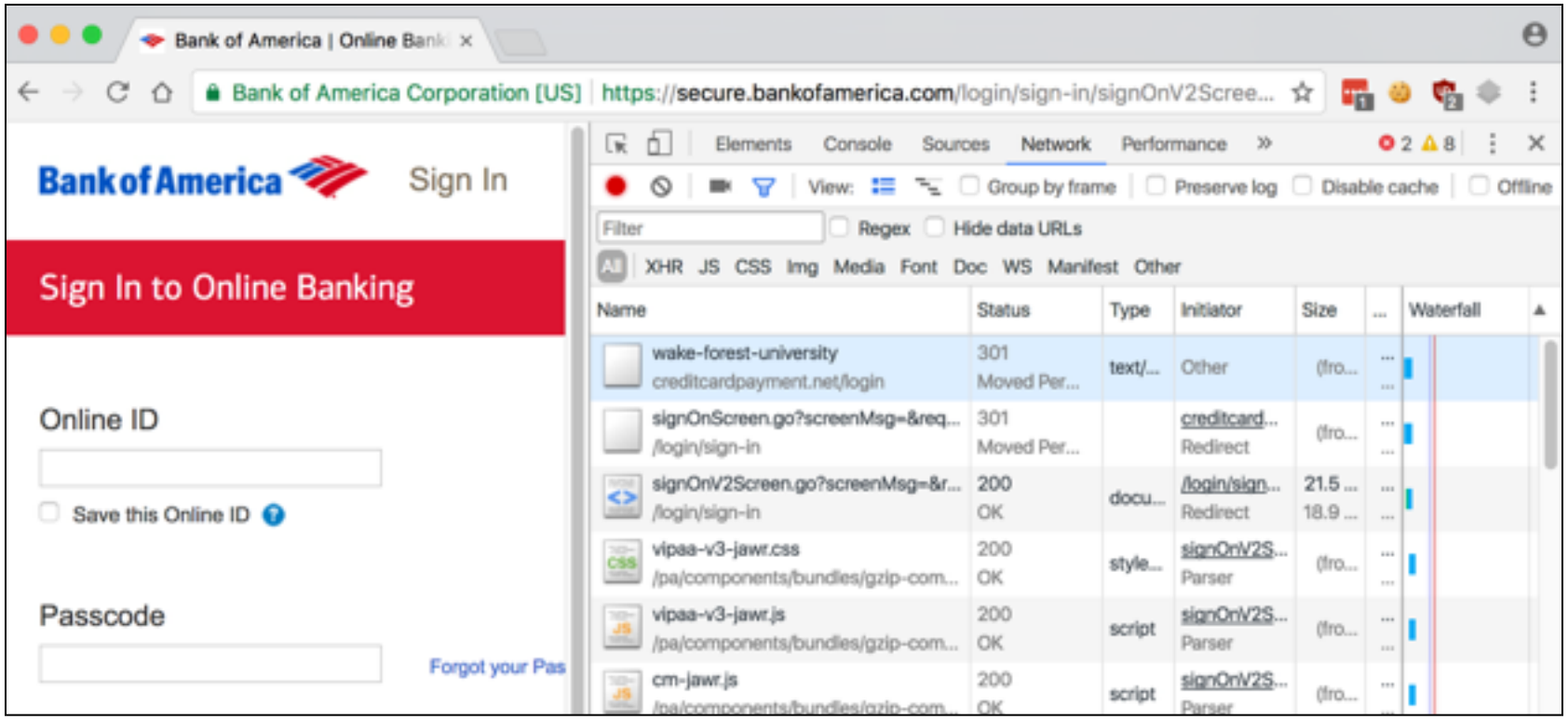

The Apache Software Founda
donate.apache.org/login
Search
APACHE
Email
test@aol.com
Password
This connection is not secure. Logins entered here could be compromised. Learn More
Stay logged in


online.adp.com/portal/login.h
online.adp.com/portal/login.html
Search
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

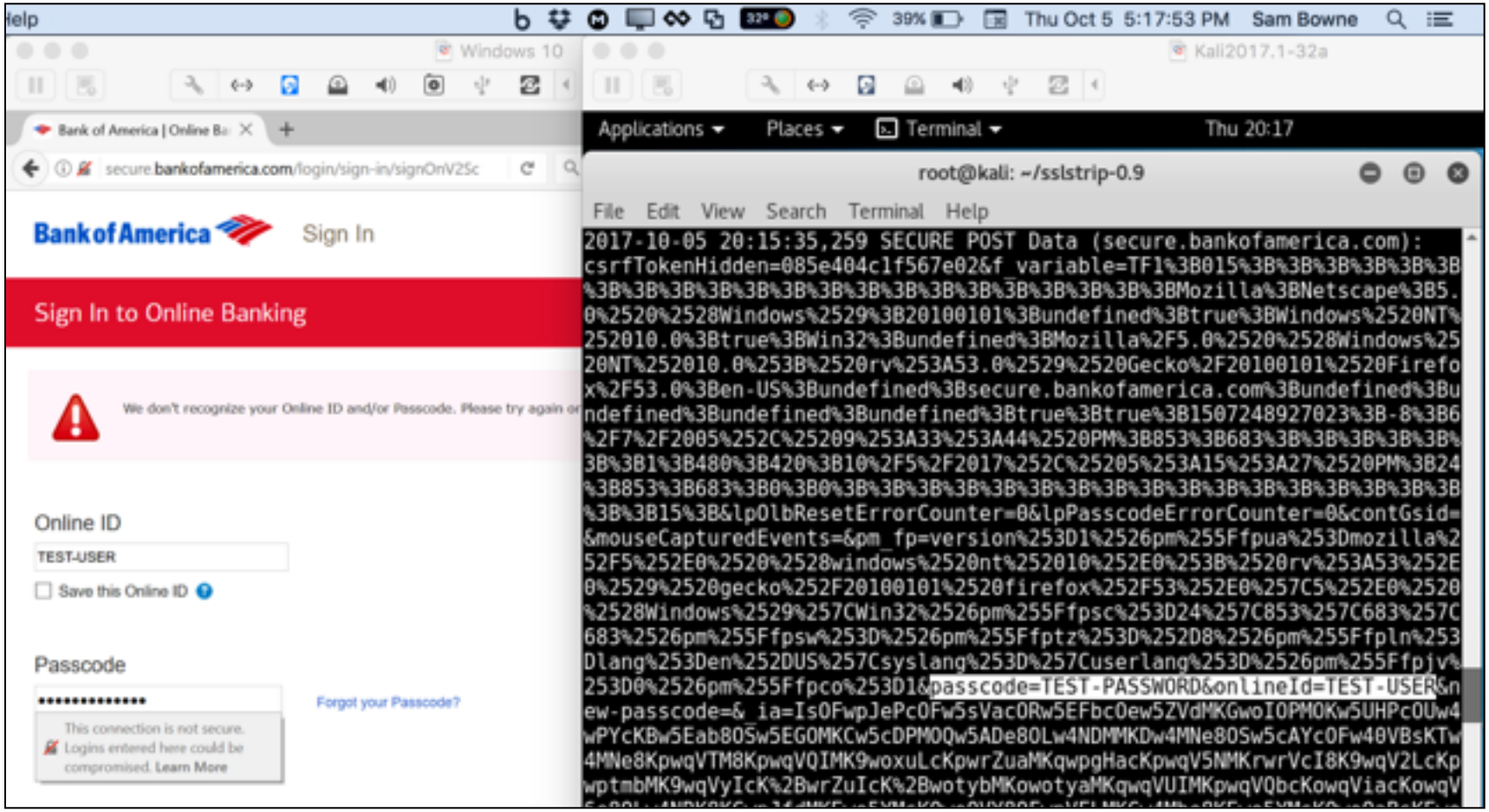
# Dork for sslstrip Vulnerability



# HTTP 301 Redirect



# Stealing Password




Kahoot!