

Alisha Kamat (201071010)  
Kunal Agarwal (201070074)  
Sanskruti Mahajan (201071012)

## **LAB ASSIGNMENT 6**

### **AIM:**

To perform protocol analysis using wireshark.

### **THEORY:**

#### **What is Wireshark?**

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems. Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

#### **Uses of Wireshark:**

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

#### **What is a packet?**

A packet is a unit of data which is transmitted over a network between the origin and the destination. Network packets are small, i.e., maximum 1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets. The data packets in the Wireshark can be viewed online and can be analyzed offline.

#### **What is color coding in Wireshark?**

The packets in the Wireshark are highlighted with blue, black, and green color. These colors help users to identify the types of traffic. It is also called as packet colorization. The kinds of coloring rules in the Wireshark are temporary rules and permanent rules.

- The temporary rules are there until the program is in active mode or until we quit the program.

- The permanent color rules are available until the Wireshark is in use or the next time you run the Wireshark. The steps to apply color filters will be discussed later in this topic.

## Features of Wireshark

- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
- It has sort and filter options which makes ease to the user to view the data.
- It is also useful in VoIP analysis.
- It can also capture raw USB traffic.
- Various settings, like timers and filters, can be used to filter the output.
- It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
- Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
- It is the no.1 piece of software for its purpose. It has countless applications ranging from the tracing down, unauthorized traffic, firewall settings, etc.

## Wireshark Challenge 1

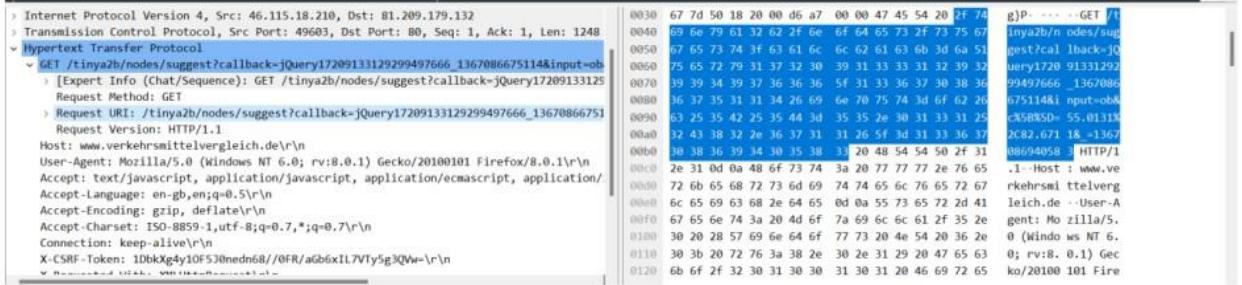
### Trouble Ticket Trace File: TroubleTicket.pcapng

- What is the application protocol used? Answer: HTTP



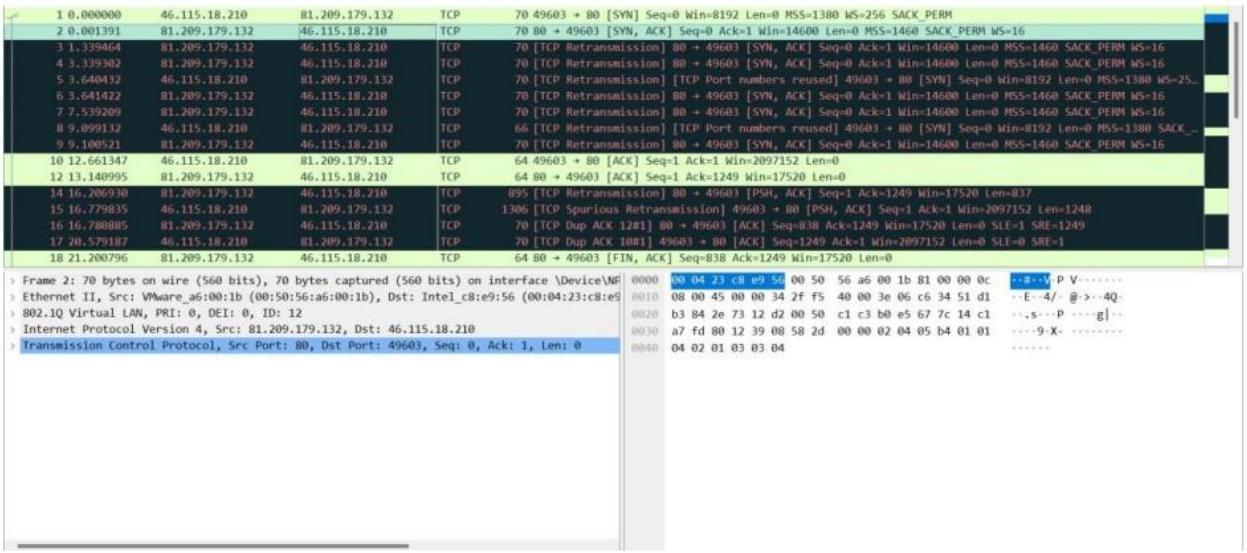
- Are all GET requests asking for the same URI?

Answer: Yes, as we can see all the GET requests have the same URI ie sr. no. 11, 15, 21 Packets.



- Based on where this trace was taken, do the packets get lost closer to the client or closer to the server?

Answer: Connection is lost near the client as it is not responding to SYN, ACK sent by server



- This trace was taken inside the infrastructure. What is the Initial Round Trip Time of the connection?

Answer: RTT refers to the time taken by a network request to reach a destination and to revert back to the original source. In case of wireshark, we can assume the time taken for a 3-way handshake is the same as RTT.

We have set the reference time as packet 8 relative time for packet 10 is 3.562215

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000		46.115.18.210	81.209.179.132	TCP	70	49603 + 80 [SYN] Seq=0 Win=8192 Len=8 MSS=1380 WS=256 SACK_PERM
2 0.001391		81.209.179.132	46.115.18.210	TCP	70	80 + 49603 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
3 1.339464		81.209.179.132	46.115.18.210	TCP	70	[TCP Retransmission] 80 + 49603 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
4 3.339302		81.209.179.132	46.115.18.210	TCP	70	[TCP Retransmission] 80 + 49603 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
5 3.640432		46.115.18.210	81.209.179.132	TCP	70	[TCP Retransmission] [TCP Port numbers reused] 49603 + 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM
6 3.641422		81.209.179.132	46.115.18.210	TCP	70	[TCP Retransmission] 80 + 49603 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
7 7.539209		81.209.179.132	46.115.18.210	TCP	70	[TCP Retransmission] 80 + 49603 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
8 9.099132		46.115.18.210	81.209.179.132	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49603 + 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 SACK_PERM
9 9.100521		81.209.179.132	46.115.18.210	TCP	70	[TCP Retransmission] 80 + 49603 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
10 12.661347		46.115.18.210	81.209.179.132	TCP	64	49603 + 80 [ACK] Seq=1 Ack=1 Win=2097152 Len=0
12 13.140995		81.209.179.132	46.115.18.210	TCP	64	80 + 49603 [ACK] Seq=1 Ack=1249 Win=17520 Len=0
14 16.206938		81.209.179.132	46.115.18.210	TCP	895	[TCP Retransmission] 80 + 49603 [PSH, ACK] Seq=1 Ack=1249 Win=17520 Len=837
15 16.779835		46.115.18.210	81.209.179.132	TCP	1386	[TCP Spurious Retransmission] 49603 + 80 [PSH, ACK] Seq=1 Ack=1 Win=2097152 Len=1248
16 16.780885		81.209.179.132	46.115.18.210	TCP	70	[TCP Dup ACK 12#] 80 + 49603 [ACK] Seq=838 Ack=1249 Win=17520 Len=0 SLE=1 SRE=1249
17 20.579187		46.115.18.210	81.209.179.132	TCP	70	[TCP Dup ACK 10#] 49603 + 80 [ACK] Seq=1249 Ack=1 Win=2097152 Len=0 SLE=0 SRE=1
18 21.200796		81.209.179.132	46.115.18.210	TCP	64	80 + 49603 [FIN, ACK] Seq=838 Ack=1249 Win=17520 Len=0

> Frame 10: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{...}

> Ethernet II, Src: Intel\_c8:e9:56 (00:04:23:c8:e9:56), Dst: VMware\_a6:00:1b (00:50:56:a6:00:00)

> 802.1Q Virtual LAN, PPI: 0, DEI: 0, ID: 12

> Internet Protocol Version 4, Src: 46.115.18.210, Dst: 81.209.179.132

> Transmission Control Protocol, Src Port: 49603, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

## 5. Who owns the server?

Answer: We set an HTTP filter for all HTTP requests in the trace file. Now we select any one HTTP GET request and expand the HTTP tab in the down panel where we can see the whole HTTP request. We found the host name in the HOST header which is www.verkehrsmittelvergleich.de

No.	Time	Source	Destination	Protocol	Length	Info
+ 11 13.139945		46.115.18.210	81.209.179.132	HTTP	1306	GET /tiny2b/nodes/suggest?callback=jQuery17209133129299497666_1367086675114&input=ob&c%58%5D=55.0131%2C8...
+ 13 13.201482		81.209.179.132	46.115.18.210	HTTP/1...	895	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)

> Frame 11: 1306 bytes on wire (10448 bits), 1306 bytes captured (10448 bits) on interface \Device\NPF\_{...}

> Ethernet II, Src: Intel\_c8:e9:56 (00:04:23:c8:e9:56), Dst: VMware\_a6:00:1b (00:50:56:a6:00:00)

> 802.1Q Virtual LAN, PPI: 0, DEI: 0, ID: 12

> Internet Protocol Version 4, Src: 46.115.18.210, Dst: 81.209.179.132

> Transmission Control Protocol, Src Port: 49603, Dst Port: 80, Seq: 1, Ack: 1, Len: 1248

▼ Hypertext Transfer Protocol

  ▼ GET /tiny2b/nodes/suggest?callback=jQuery17209133129299497666\_1367086675114&input=ob

    > [Expert Info (Chat/Sequence): GET /tiny2b/nodes/suggest?callback=jQuery17209133129299497666\_1367086675114&input=ob]

      Request Method: GET

      Request URL: /tiny2b/nodes/suggest?callback=jQuery17209133129299497666\_1367086675114&input=ob

      Request Version: HTTP/1.1

      Host: www.verkehrsmittelvergleich.de\r\n

      User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:8.0.1) Gecko/20100101 Firefox/8.0.1\r\n

      Accept: text/javascript, application/javascript, application/ecmascript, application/javascript/ecmascript, application/x-ecmascript, \*/\*

      Accept-Language: en-gb,en;q=0.5\r\n

      Accept-Encoding: gzip, deflate\r\n

0000 2e 31 0d 0a #8 6f 73 74 3a 28 77 77 77 2e 76 65 .1. Host : www.vr...  
0001 72 65 6d 72 73 6d 69 74 75 65 6c 76 65 72 67 kehsm ttelverg...  
0002 6c 65 69 63 68 2e 64 65 0d 0a 55 73 65 72 24 leich.de -User\_A...  
0003 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5...  
0004 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 0 (Windo ws NT 6...  
0005 30 3b 20 72 76 3a 38 2e 30 2e 31 29 20 47 65 63 0; rv:8. 0.1) Gec...  
0006 6b 6f 2f 32 30 31 30 30 31 30 31 28 46 69 72 65 ko/20100 101 Fire...  
0007 66 6f 78 2f 38 2e 30 2e 31 0d 0a 41 63 63 65 70 fox/8.0. 1.-Accp...  
0008 74 3a 20 74 65 78 74 2f 6a 61 76 61 73 63 72 69 ti text/ javascri...  
0009 70 74 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f pt, appl ication/...  
0010 6a 61 76 61 73 63 72 69 70 74 2c 20 61 70 70 6c javascri pt, appl...  
0011 69 63 61 74 69 6f 6e 2f 65 63 6d 61 73 63 72 69 ication/ ecmasc...  
0012 70 74 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f pt, appl ication/...  
0013 78 2d 65 63 6d 61 73 63 72 69 70 74 2c 20 2a 2f x-ecmasc ript, /\*/  
0014 2a 3b 20 71 3d 30 2e 30 31 0d 0a 41 63 63 65 70 "; q=0.0 1--Accp...  
0015 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 67 t-Langu ge: en-g...



Home > Whois Lookup > VerkehrsmittelVergleich.de

## Whois Record for VerkehrsmittelVergleich.de

### — Domain Profile

Registrar Status	connect
Dates	Updated on 2021-03-04
Name Servers	NS1.DOMAINDISCOUNT24.NET (has 279,498 domains) NS2.DOMAINDISCOUNT24.NET (has 279,498 domains) NS3.DOMAINDISCOUNT24.NET (has 279,498 domains)
Tech Contact	—
Hosting History	2 changes on 3 unique name servers over 6 years

### — Website

Website Title	None given.
---------------	-------------

Whois Record (last updated on 2022-10-14)

```
Domain: verkehrsmittelvergleich.de
Nserver: ns1.domaindiscount24.net
Nserver: ns2.domaindiscount24.net
Nserver: ns3.domaindiscount24.net
Status: connect
Changed: 2021-03-04T13:11:37+01:00
```

```

root@LAPTOP-K61BR036:/mnt/c/users/aryan# whois verkehrsmittelvergleich.de
% Restricted rights.
%
% Terms and Conditions of Use
%
% The above data may only be used within the scope of technical or
% administrative necessities of Internet operation or to remedy legal
% problems.
% The use for other purposes, in particular for advertising, is not permitted.
%
% The DENIC whois service on port 43 doesn't disclose any information concerning
% the domain holder, general request and abuse contact.
% This information can be obtained through use of our web-based whois service
% available at the DENIC website:
% http://www.denic.de/en/domains/whois-service/web-whois.html
%
%

Domain: verkehrsmittelvergleich.de
Nserver: ns1.domaindiscount24.net
Nserver: ns2.domaindiscount24.net
Nserver: ns3.domaindiscount24.net
Status: connect
Changed: 2021-03-04T13:11:37+01:00
root@LAPTOP-K61BR036:/mnt/c/users/aryan#

```

### BIG FTP Trace File: BigFTP.pcapng

- On which host was Wireshark running when this trace file was taken?

Answer: The first packet we saw in the trace file is a FTP request in 0.00000 seconds and the second packet comes with the response in 0.036454000 seconds later, again the third packet is going with FTP command in 0.000505000 seconds, the request time is too fast, which means Wireshark is running on client's system.

1 0.000000	24.6.173.220	198.66.239.146	FTP	85 Request: CWD /www/htdocs/uploadtesting
2 0.036454	198.66.239.146	24.6.173.220	FTP	82 Response: 250 CWD command successful
3 0.036959	24.6.173.220	198.66.239.146	FTP	81 Request: PORT 24,6,173,220,155,127
4 0.053553	198.66.239.146	24.6.173.220	FTP	83 Response: 200 PORT command successful
5 0.053664	24.6.173.220	198.66.239.146	FTP	62 Request: TYPE I

- If this network does not support jumbo frames, why do we see 16,450 byte packets in the trace file?

Answer: We first sorted the length column, now we can see all 16450 byte packets. This, size of packet is supported by something called Large Segment Offload. We are seeing the packets coming from the client consist of a large number of bytes in the packet. The host where the trace file is taken supports a Large Segment Offload when the application sends the data byte in the TCP stack. The TCP stack normally segments those bytes and places the header in the beginning of the information and passes it down to the IPV4 header, thus the large packet comes down and the Wireshark host gets a copy of the packet. Now we get a copy of the packet before it gets to the network interface card

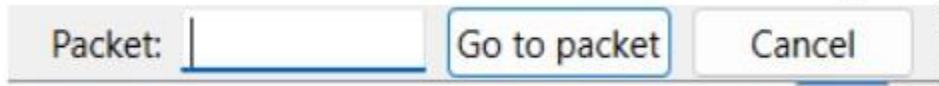
(NIC) driver and the driver passes the 16450 bytes down to the NIC card, and it actually creates the TCP segments and sends them out on the network. Only for this process we are seeing here the jumbo packets in the trace file

No.	Time	Source	Destination	Protocol	Length	Info
6091	24.489410	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6082	24.423773	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6074	24.365967	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6065	24.308880	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6056	24.243788	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6047	24.179063	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6038	24.121292	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6029	24.051233	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6020	23.986978	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6012	23.929454	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6003	23.865034	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
5994	23.800004	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
5986	23.742435	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
5977	23.677241	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
5968	23.619700	24.6.173.220	198.66.239.146	FTP-D..	16450	FTP Data: 16384 bytes (PORT) (TYPE I)

### 3. What data packet is being acknowledged in frames 314-321?

Answer: Data packet 304 is acknowledged between 314-321

Select Go and then Go to Packet for jumping into packet number 314.



Given the packet number as can be seen below, we gave 314. Now we can see all packets between 314-321.

314 1.278165	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=542121 Win=66608 Len=0 TSval=3182269235 TSecr=198..
315 1.278938	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=545017 Win=65160 Len=0 TSval=3182269236 TSecr=198..
316 1.278941	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=546465 Win=66608 Len=0 TSval=3182269236 TSecr=198..
317 1.278944	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=549361 Win=65160 Len=0 TSval=3182269237 TSecr=198..
318 1.279761	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=550809 Win=66608 Len=0 TSval=3182269238 TSecr=198..
319 1.279763	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=553705 Win=65160 Len=0 TSval=3182269239 TSecr=198..
320 1.333211	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=555153 Win=66608 Len=0 TSval=3182269292 TSecr=198..
321 1.333995	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=557057 Win=64704 Len=0 TSval=3182269292 TSecr=198..

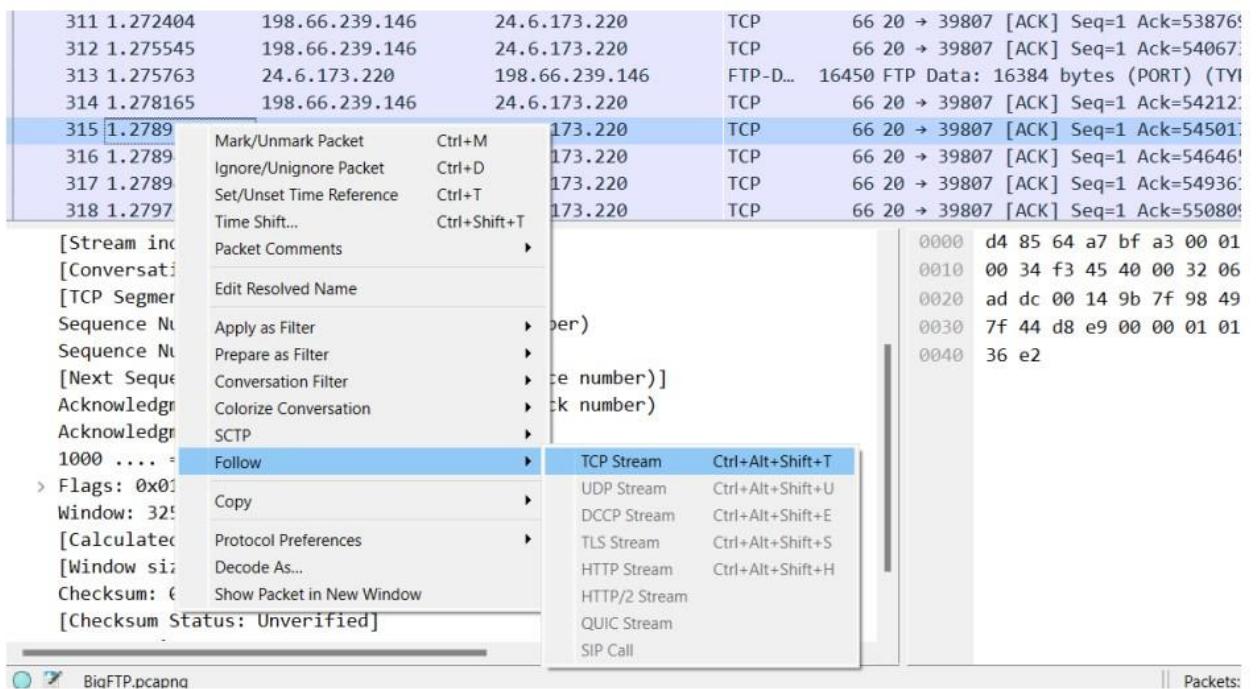
We selected the last packet 321 and expanded the TCP header for checking the ACK sequence number, which is showing 557057. Now we have to find which data packet is sending this ACK number to 321.

No.	Time	Source	Destination	Protocol	Length	Info
313	1.275763	24.6.173.220	198.66.239.146	FTP-D...	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
314	1.278165	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=542121 Win=66608 Len=0 TSval=3182269235 TSecr=198...
315	1.278938	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=545017 Win=65160 Len=0 TSval=3182269236 TSecr=198...
316	1.278941	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=546465 Win=66608 Len=0 TSval=3182269236 TSecr=198...
317	1.278944	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=549361 Win=65160 Len=0 TSval=3182269237 TSecr=198...
318	1.279761	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=550809 Win=66608 Len=0 TSval=3182269238 TSecr=198...
319	1.279763	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=553705 Win=65160 Len=0 TSval=3182269239 TSecr=198...
320	1.333211	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=555153 Win=66608 Len=0 TSval=3182269292 TSecr=198...
321	1.333995	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=557057 Win=64704 Len=0 TSval=3182269292 TSecr=198...
322	1.334381	24.6.173.220	198.66.239.146	FTP-D...	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
323	1.341907	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=559953 Win=63712 Len=0 TSval=3182269300 TSecr=198...
324	1.342705	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=561401 Win=66608 Len=0 TSval=3182269301 TSecr=198...
325	1.342707	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=564297 Win=65160 Len=0 TSval=3182269301 TSecr=198...
326	1.343460	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=565745 Win=66608 Len=0 TSval=3182269301 TSecr=198...
327	1.344273	198.66.239.146	24.6.173.220	TCP	66	20 → 39807 [ACK] Seq=1 Ack=568641 Win=65160 Len=0 TSval=3182269302 TSecr=198...
<pre>[Stream index: 1] [Conversation completeness: Incomplete (30)] [TCP Segment Len: 0] Sequence Number: 1 (relative sequence number) Sequence Number (raw): 2554975040 [Next Sequence Number: 1 (relative sequence number)] Acknowledgment Number: 557057 (relative ack number) Acknowledgment number (raw): 3029041827 1000 .... = Header Length: 32 bytes (8) &gt; Flags: 0x010 (ACK) Window: 32352 [Calculated window size: 64704] [Window size scaling factor: 2] Checksum: 0xaabd [unverified] [Checksum Status: Unverified]</pre>						

We started to check all the first data packet numbers, which are sending the main FTP-DATA. We found that packet number 304's TCP header has the next sequence number for 557057. This means data packet 304 is acknowledged between 314-321.

```
[Stream index: 1]
[Conversation completeness: Incomplete (30)]
[TCP Segment Len: 16384]
Sequence Number: 540673 (relative sequence number)
Sequence Number (raw): 3029025443
[Next Sequence Number: 557057 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2554975040
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)
Window: 260
[Calculated window size: 66560]
[Window size scaling factor: 256]
Checksum: 0x7bbe [unverified]
[Checksum Status: Unverified]
```

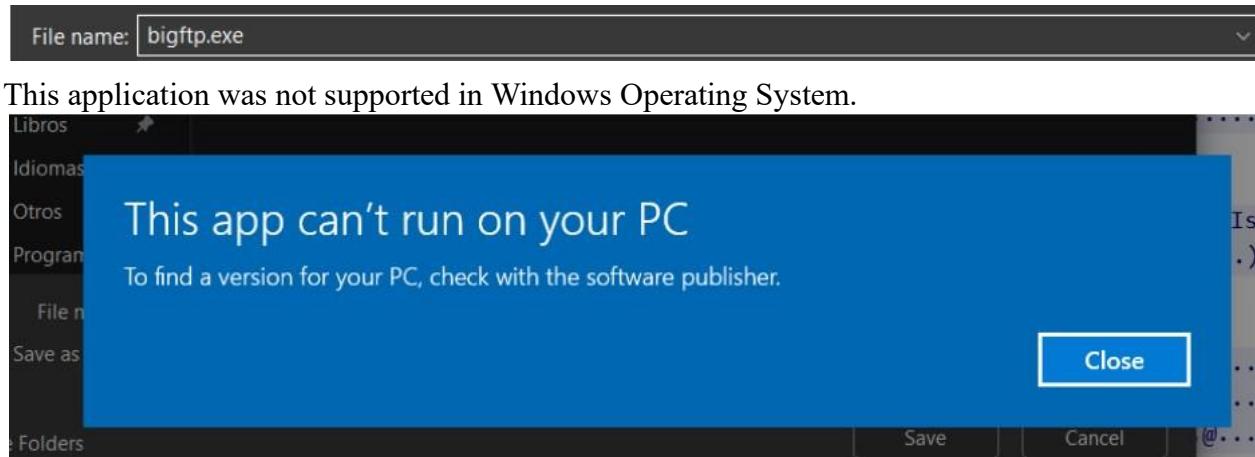
- Why can't you view the reassembled .jpg file that is uploaded in this trace file?
- Answer: We selected a data packet and right clicked on it then selected Follow TCP stream.



Inside the TCP stream it is showing the RAW data and it doesn't look like an image file. There is a message showing that this program must be run under win32 and also some kind of source code is showing. It means it is a Windows executable program.

5. What is the true purpose of kidsatbeach.jpg?

Answer: In the previous challenge we saw that the jpg file was actually an exe file. So we saved the file in exe format. Then we executed it



## PAID TO PLAY Trace File: AllPlayNoWork.pcapng

1. For what server did the client try to resolve an IPv6 address?

The IPv6 resolution process tries to look for AAAA in the DNS query type

Answer: ws12.gti.mcafee.com

No.	Time	Source	Destination	Protocol	Length	Info
7	0.807328	192.168.1.254	192.168.1.71	DNS	176	Standard query response 0x1450 A login.live.com CNAME login.live.com.nsatc.n...
8	0.960492	192.168.1.71	192.168.1.254	DNS	140	Standard query 0x979b A c-0.19-a7000489.2.15ea.7cd.3ea3.210.0.me41ifbcr7aub...
9	0.984965	192.168.1.254	192.168.1.71	DNS	156	Standard query response 0x979a A c-0.19-a7000489.2.15ea.7cd.3ea3.210.0.me41...
10	1.027210	192.168.1.71	192.168.1.254	DNS	81	Standard query 0xa1a9a A cdf-anon.xboxlive.com
11	1.057721	192.168.1.71	192.168.1.254	DNS	81	Standard query 0xa1a9a A cdf-anon.xboxlive.com
12	1.116915	192.168.1.254	192.168.1.71	DNS	258	Standard query response 0xa1a9a A cdf-anon.xboxlive.com CNAME cdf-anon.gtm.xb...
13	1.131298	192.168.1.71	192.168.1.254	DNS	79	Standard query 0xa0d8 A ws12.gti.mcafee.com
14	1.131298	192.168.1.71	192.168.1.254	DNS	79	Standard query 0xa482 AAAA ws12.gti.mcafee.com
15	1.161825	192.168.1.71	192.168.1.254	DNS	79	Standard query 0xa0d8 A ws12.gti.mcafee.com
16	1.161825	192.168.1.71	192.168.1.254	DNS	79	Standard query 0xa482 AAAA ws12.gti.mcafee.com
17	1.174870	192.168.1.254	192.168.1.71	DNS	79	Standard query response 0xa482 AAAA ws12.gti.mcafee.com
18	1.176713	192.168.1.254	192.168.1.71	DNS	95	Standard query response 0xa0d8 A ws12.gti.mcafee.com A 8.18.25.6
19	1.607327	192.168.1.71	192.168.1.254	DNS	77	Standard query response 0x891d A commerce.zune.net
20	1.630695	192.168.1.254	192.168.1.71	DNS	161	Standard query response 0x891d A commerce.zune.net CNAME commerce.zune.net.n...
21	1.727271	192.168.1.71	192.168.1.254	DNS	81	Standard query 0xd59 A eds-anon.xboxlive.com

Frame 14: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface  
 > Ethernet II, Src: Micro-St\_a6:43:6f (d4:3d:7e:a6:43:6f), Dst: PaceAmer\_11:e2:b  
 > Internet Protocol Version 4, Src: 192.168.1.71, Dst: 192.168.1.254  
 > User Datagram Protocol, Src Port: 53873, Dst Port: 53  
 > Domain Name System (query)  
 Transaction ID: 0xa482  
 > Flags: 0x0100 Standard query  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 0  
 > Queries  
 > ws12.gti.mcafee.com: type AAAA, class IN  
 [Response In: 17]

Packets: 2357 · Displayed: 2357 (100.0%) Profile: Default

2. What operating system do you think the client is running?

Answer: Windows 8

No.	Time	Source	Destination	Protocol	Length	Info
31	2.003160	192.168.1.71	8.254.61.254	TCP	66	3994 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
32	2.003164	192.168.1.71	8.254.61.254	TCP	66	3990 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
33	2.003189	192.168.1.71	8.254.61.254	TCP	66	3991 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
34	2.010721	192.168.1.71	8.254.61.254	TCP	66	3996 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
35	2.050201	8.254.61.254	192.168.1.71	TCP	66	80 → 3993 [SVN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
36	2.050370	192.168.1.71	8.254.61.254	TCP	54	3993 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
37	2.050443	192.168.1.71	8.254.61.254	HTTP	336	GET /assets/za/dd/2add7b43-6022-4253-ab9a-cccee205ddd8.jpg?n=03_06_2013_game...
38	2.051855	8.254.61.254	192.168.1.71	TCP	66	80 → 3992 [SVN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
39	2.051914	192.168.1.71	8.254.61.254	TCP	54	3992 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
40	2.051950	192.168.1.71	8.254.61.254	HTTP	318	GET /assets/53/79/5379179d-139b-4b1-b647-4a160c25a677.jpg?n=slot-ty-01-295x...
41	2.054699	8.254.61.254	192.168.1.71	TCP	66	80 → 3994 [SVN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
42	2.054823	192.168.1.71	8.254.61.254	TCP	54	3994 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
43	2.054856	192.168.1.71	8.254.61.254	HTTP	323	GET /assets/00/bc/00bccce83-f8c4-440e-bdc4-05fd50211078.png?n=7_30_2013_class...
44	2.055570	8.254.61.254	192.168.1.71	TCP	66	80 → 3991 [SVN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
45	2.055638	192.168.1.71	8.254.61.254	TCP	54	3991 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0

Frame 37: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits) on interface  
 > Ethernet II, Src: Micro-St\_a6:43:6f (d4:3d:7e:a6:43:6f), Dst: PaceAmer\_11:e2:  
 > Internet Protocol Version 4, Src: 192.168.1.71, Dst: 8.254.61.254  
 > Transmission Control Protocol, Src Port: 3993, Dst Port: 80, Seq: 1, Ack: 1,  
 > Hypertext Transfer Protocol  
 > GET /assets/za/dd/2add7b43-6022-4253-ab9a-cccee205ddd8.jpg?n=03\_06\_2013\_ga...  
 Accept: \*/\*\r\nUser-Agent: XBLWIN2.0\r\nAccept-Language: en-US,en;q=0.5\r\nUA-CPU: AMD64\r\nAccept-Encoding: gzip, deflate\r\nHost: compass.xboxlive.com\r\nConnection: Keep-Alive\r\nV\r\n[Full request URI: http://compass.xboxlive.com/assets/za/dd/2add7b43-6022-4253-ab9a-cccee205ddd8.jpg?n=03\_06\_2013\_game...]  
 0000 ac 5d 10 11 e2 b9 d3 7e a3 43 6f 08 00 45 00 .].....= ~Co-E.  
 0010 01 42 6d 69 40 00 80 06 00 00 c0 a8 01 47 08 fe -Bm@.....G..  
 0020 3d fe 09 00 50 06 68 4b 7d 8a f1 d9 50 18 =....P-hT<-P.  
 0030 04 00 2a 00 20 00 47 45 54 20 2f 61 73 65 74 ...GE T /asset...  
 0040 73 2f 32 61 2f 64 64 2f 32 61 64 64 37 62 34 33 s/za/dd/ 2add7b43  
 0050 2d 36 30 32 32 2d 34 32 35 33 2d 61 62 39 61 2d -6022-42 53-ab9a-  
 0060 63 63 65 65 32 30 35 64 64 64 38 2e 6a 70 67 cccee205 ddd8.jpg  
 0070 3f 6e 3d 30 33 5f 30 36 5f 32 30 31 33 5f 67 61 ?n=03\_06\_2013\_ga...  
 0080 6d 65 73 5f 72 6f 79 61 6c 65 6e 76 6f 79 32 5f mes\_roya lenvoy2\_...  
 0090 32 39 35 5f 31 36 35 2e 6a 70 67 20 48 54 50 50 295\_165. jpg HTTP  
 00a0 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f /1.1..Ac cept: /\*  
 00b0 2a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 58 \*.User-Agent: XBLWIN2.0 ..Accept  
 00c0 42 4c 57 49 4e 32 2e 30 0d 0a 41 63 65 70 74 BLWIN2.0 ..Accept  
 00d0 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 -Langua...e: en-US  
 00e0 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 55 41 2d 43 50 ,en;q=0.5 ..UA-CP

Packets: 2357 · Displayed: 2357 (100.0%) Profile: Default

Right click on the user agent and click “apply as column”

No.	Time	Source	Destination	Protocol	Length	User-Agent	Info
579	2.311735	192.168.1.71	8.254.61.254	HTTP	351	XBLWIN2.0	GET /assets/76/7a/767aa37c-2362-48d3-e97-3c3a1820ce09.jpg?n=03_12
496	2.279873	192.168.1.71	8.254.61.254	HTTP	343	XBLWIN2.0	GET /assets/58/34/58343fe8-327b-4d9f-a6d7-1e2b6cf3aca6.jpg?n=03_12
485	2.273854	192.168.1.71	8.254.61.254	HTTP	323	XBLWIN2.0	GET /assets/c2/52/c252fe11-bc47-4dae-8930-8e0cb9d96e110.jpg?n=b1g_b
263	2.199376	192.168.1.71	8.254.61.254	HTTP	326	XBLWIN2.0	GET /assets/37/eb/37ebdd85-e00e-43b4-b9ed-692b76071f2c.png?n=uno-a
250	2.186253	192.168.1.71	8.254.61.254	HTTP	336	XBLWIN2.0	GET /assets/d4/8d/d48d4cc1-39ce-481b-af22-6c1fab909eca.jpg?n=06_05
226	2.164109	192.168.1.71	8.254.61.254	HTTP	318	XBLWIN2.0	GET /assets/24/c2/c24c2b5e3-95f0-4b67-96ce-8b762f0431c.png?n=1itt1
52	2.060308	192.168.1.71	8.254.61.254	HTTP	328	XBLWIN2.0	GET /assets/e9/5c/e95ce79a-fb26-494b-a2c2-9eae5c9d9f66.jpg?n=05_02
49	2.056471	192.168.1.71	8.254.61.254	HTTP	335	XBLWIN2.0	GET /assets/5d/00/5d008588-f17d-45de-9afa-8be2c250c376.jpg?n=05_01
46	2.055671	192.168.1.71	8.254.61.254	HTTP	336	XBLWIN2.0	GET /assets/30/b0/30b06a70-6657-429a-9ce1-02ef040d6262.jpg?n=03_12
43	2.054856	192.168.1.71	8.254.61.254	HTTP	323	XBLWIN2.0	GET /assets/00/bc/00bcc83-f8c4-440e-bdc4-05fd50211078.jpg?n=7_30
40	2.051950	192.168.1.71	8.254.61.254	HTTP	318	XBLWIN2.0	GET /assets/53/79/5379179d-119b-44b1-b647-4a160c25a677.jpg?n=slot-1
37	2.050443	192.168.1.71	8.254.61.254	HTTP	336	XBLWIN2.0	GET /assets/2a/dd/2add7b43-6022-4253-ab9a-ccce205ddd8.jpg?n=03_06
2323	1058.879480	192.168.1.71	208.71.187.24	HTTP	328	G1WebToo...	GET /config/1534:51718:1.0.41:ios:appstore HTTP/1.1
2062	158.914003	192.168.1.71	208.71.187.24	HTTP	328	G1WebToo...	GET /config/1534:51718:1.0.41:ios:appstore HTTP/1.1

### 3. What is the color of the mermaid's hair?

Answer: Reddish-orange

The screenshot shows a browser window with the URL <https://drive.google.com/drive/u/1/folders/1HjR0nYzAaAmThMvZDf6UAgQO>. The search bar contains "ip.arc=>192.168.1.71". The NetworkMiner tool is overlaid on the browser, displaying a list of network traffic. The traffic list includes several entries for XBLWIN2.0 GET requests to various asset URLs, such as /assets/76/7a/767aa37c-2362-48d3-e97-3c3a1820ce09.jpg?n=03\_12 and /assets/58/34/58343fe8-327b-4d9f-a6d7-1e2b6cf3aca6.jpg?n=03\_12. The main content area of the browser shows a large image of Ariel from Disney's The Little Mermaid.

### 4. What classic games did the user learn about?

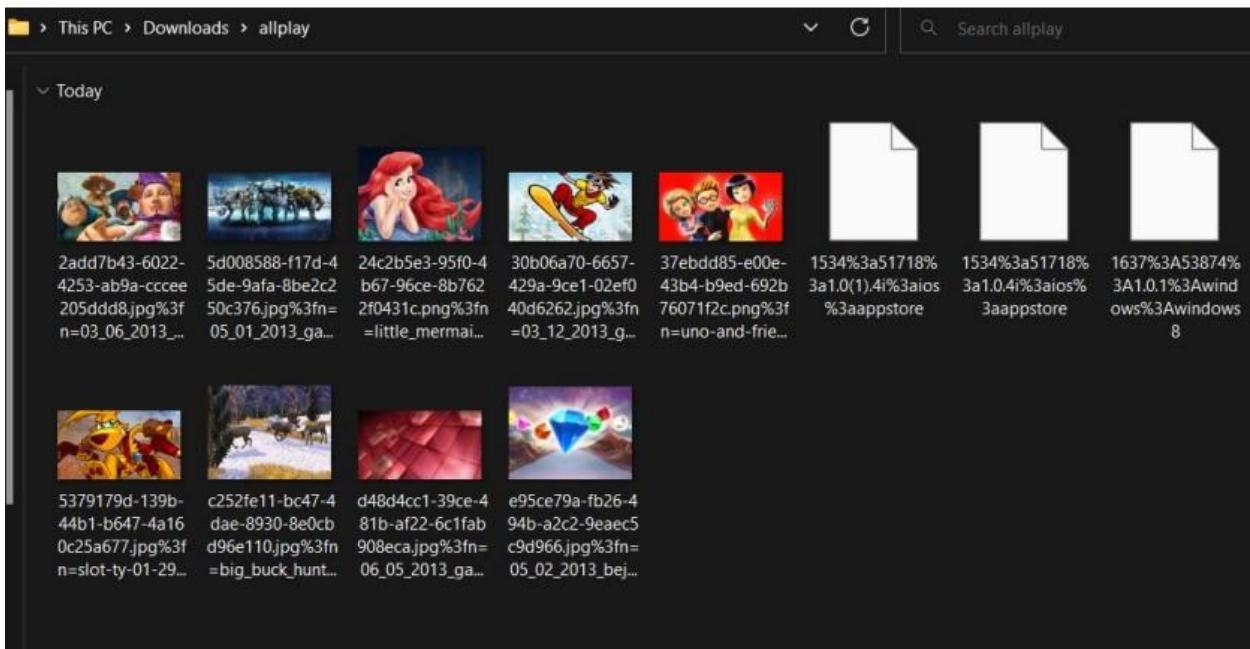
Answer: Games: Solitaire, Pac-Man, Mahjong, BigBuck etc:

Wireshark - Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
224	compass.xboxlive.com	image/jpeg	23 kB	5d008588-f17d-45de-9afa-8be2c250c376.jpg?n=05_01_2013_games_h
248	compass.xboxlive.com	image/jpeg	31 kB	2add7b43-6022-4253-ab9a-cccee205ddd8.jpg?n=03_06_2013_games_
261	compass.xboxlive.com	image/jpeg	43 kB	5379179d-139b-44b1-b647-4a160c25a677.jpg?n=slot-ty-01-295x165.j
483	compass.xboxlive.com	image/jpeg	72 kB	e95ce79a-fb26-494b-a2c2-9eaec5c9d966.jpg?n=05_02_2013_bejewele
494	compass.xboxlive.com	image/jpeg	23 kB	d48d4cc1-39ce-481b-af22-6c1fab908eca.jpg?n=06_05_2013_games_al
576	compass.xboxlive.com	image/jpeg	34 kB	30b06a70-6657-429a-9ce1-02ef040d6262.jpg?n=03_12_2013_games_i
946	compass.xboxlive.com	image/png	75 kB	37ebdd85-e00e-43b4-b9ed-692b76071f2c.png?n=uno-and-friends_29
1469	compass.xboxlive.com	image/png	391 kB	24c2b5e3-95f0-4b67-96ce-8b7622f0431c.png?n=little_mermaid_wgs.p
1555	compass.xboxlive.com	image/jpeg	29 kB	58343fe8-327b-4d9f-a6d7-1e2b6cf3aca6.jpg?n=03_12_2013_games_ar
1840	compass.xboxlive.com	image/jpeg	419 kB	c252fe11-bc47-4dae-8930-8e0cbd96e110.jpg?n=big_buck_hunter_635
1975	uno.eve.gameloft.com:20001	application/json	881 bytes	1637%3A53874%3A1.0.1%3Awindows%3Awindows8
2064	uno.eve.gameloft.com:20001	application/json	767 bytes	1534:51718:1.0.4:iios:appstore
2325	uno.eve.gameloft.com:20001	application/json	767 bytes	1534:51718:1.0.4:iios:appstore

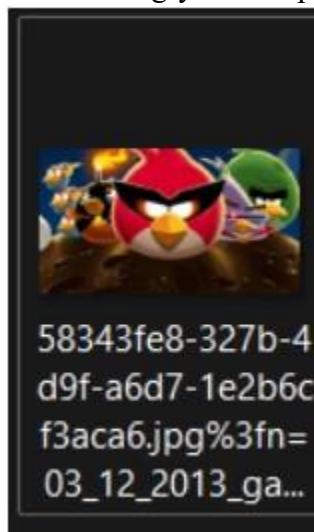
Save Save All Preview Close Help





5. Which Angry Birds edition did the user learn about?

Answer: Angry Birds Space Edition

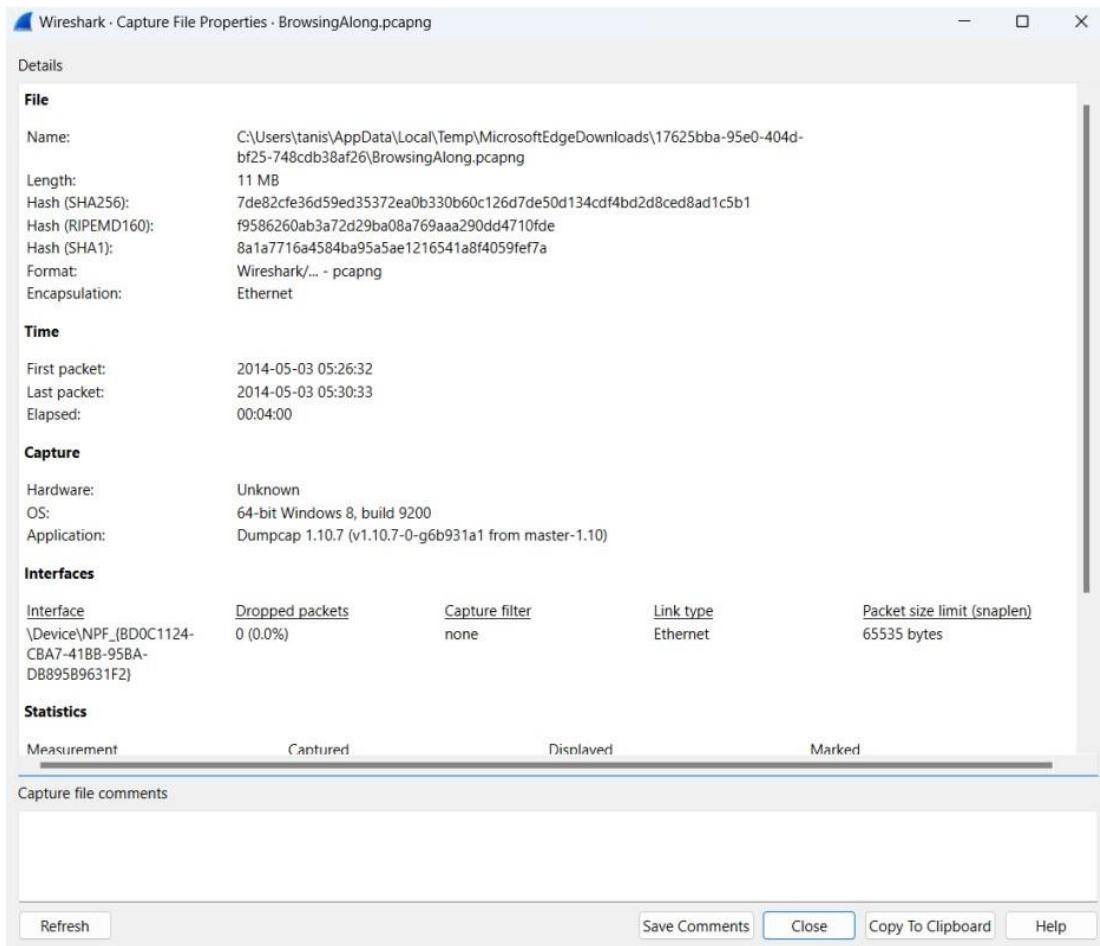


58343fe8-327b-4  
d9f-a6d7-1e2b6c  
f3aca6.jpg%3fn=  
03\_12\_2013\_ga...

### BROWSING BUDDY Trace File: BrowsingAlong.pcapng

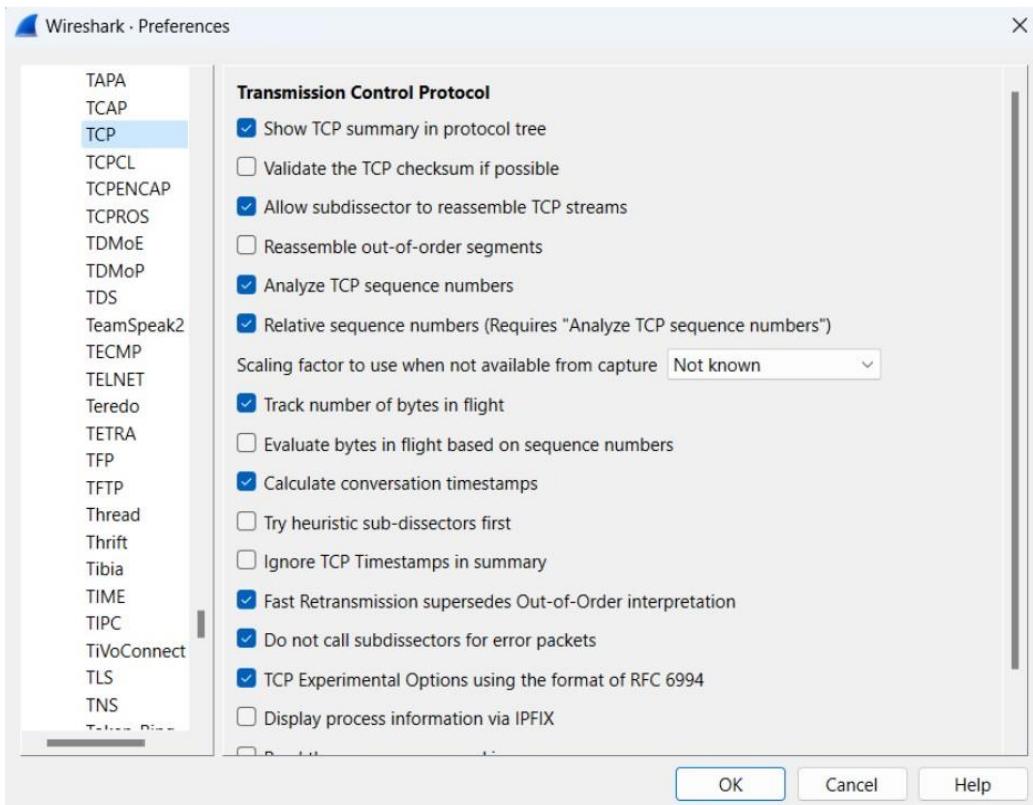
1. What version of dumpcap was used to capture this trace file?

Answer: Dumpcap 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)



2. Which frame contains the 200 OK response to the GET request for /scripts/AC\_OETags.js?

Answer: 266



```
> GET /scripts/AC_OETags.js HTTP/1.1\r\n
Host: www.coolcows.com.au\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0\r\n
Accept: */*\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://www.coolcows.com.au/Infrastructure\r\n
> Cookie: visitorDeviceClass=desktop; ASP.NET_SessionId=1234567890\r\n
Connection: keep-alive\r\n
\r\n
[Full request URI: http://www.coolcows.com.au/scripts/AC_OETags.js]
[HTTP request 2/7]
[Prev request in frame: 171]
[Response in frame: 271]
[Next request in frame: 282]
```

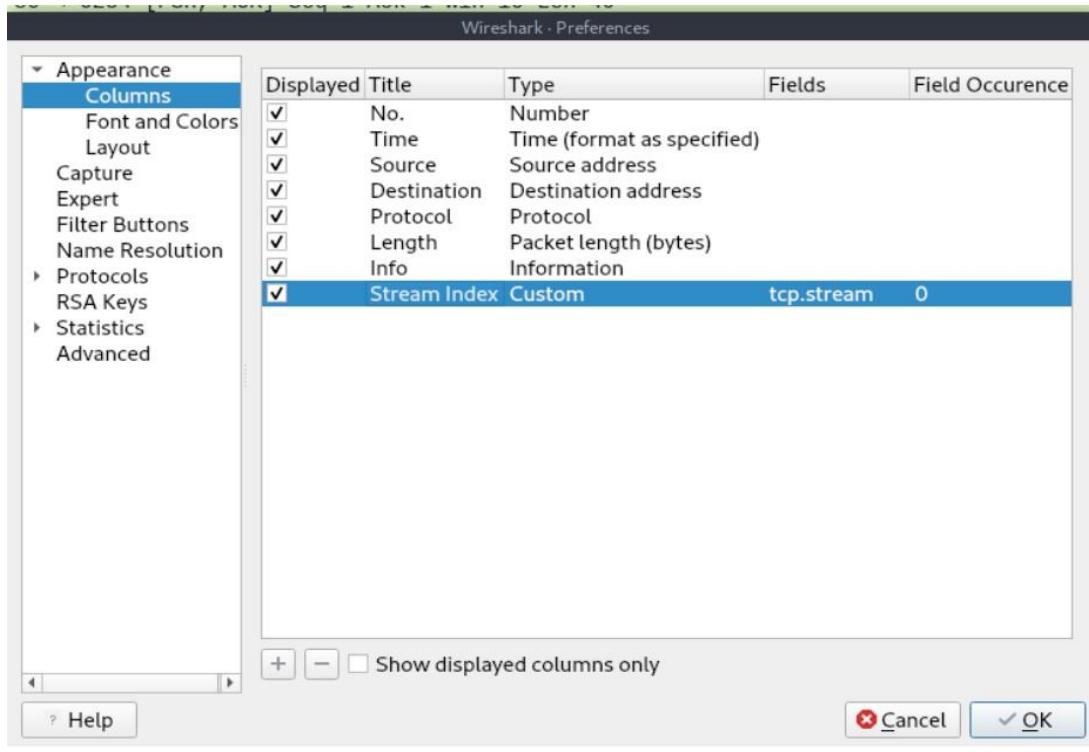
3. In what kind of “bar” is the client interested?

Answer: tiki bar

4779 197.790470	204.79.197.200	192.168.1.71	TCP	69	80 → 6287 [PSH, ACK] Seq=297466 A
4780 197.790470	204.79.197.200	192.168.1.71	HTTP	60	HTTP/1.1 200 OK (text/html)
4781 197.790550	192.168.1.71	204.79.197.200	TCP	54	6287 → 80 [ACK] Seq=46159 Ack=297
→ 4782 197.820815	192.168.1.71	204.79.197.200	HTTP	1089 Mozilla/...	GET /AS/Suggestions?pt=Page.SERP&
4783 197.855305	204.79.197.200	192.168.1.71	TCP	60	80 → 6287 [ACK] Seq=297486 Ack=47
4784 197.859983	204.79.197.200	192.168.1.71	TCP	1365	80 → 6288 [PSH, ACK] Seq=87769 Ac
4785 197.860777	204.79.197.200	192.168.1.71	TCP	69	80 → 6288 [PSH, ACK] Seq=89080 Ac
4786 197.860778	204.79.197.200	192.168.1.71	HTTP	60	HTTP/1.1 200 OK (text/html)
4787 197.860843	192.168.1.71	204.79.197.200	TCP	54	6288 → 80 [ACK] Seq=19326 Ack=891
4788 197.952338	204.79.197.200	192.168.1.71	TCP	1368	80 → 6287 [PSH, ACK] Seq=297486 A

4. Which TCP stream experienced the most Retransmissions?

Answer: 129



Time	Source	Destination	Protocol	Length	Info	Stream Index
080 235.261054	65.294.231.349	192.168.1.71	TCP	1514	[TCP Fast Retransmission] 80 - 6451 [ACK] Seq=16051 Ack=408 Win=4708 Len=1408 [Last segment of a reassembled PDU]	183
081 235.261054	65.294.231.349	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6450 [ACK] Seq=16050 Ack=408 Win=4708 Len=1408 [Last segment of a reassembled PDU]	183
087 237.229443	66.216.216.123	192.168.1.71	TCP	68	[TCP Retransmission] 80 - 6443 [SYN, ACK] Seq=9 Ack=1 Win=5040 Len=8 MSS=1468 SACK_PERM=1 WS=128	173
087 234.479879	69.89.25.173	192.168.1.71	TCP	68	[TCP Retransmission] 80 - 6437 [SYN, ACK] Seq=9 Ack=1 Win=14680 Len=8 MSS=1468 SACK_PERM=1 WS=128	173
076 307.339923	192.168.1.71	68.151.190.199	TCP	84	[TCP Retransmission] 8418 - 6437 [FIN, ACK] Seq=10 Ack=1 Win=61248 Len=8 MSS=1468 SACK_PERM=1 WS=128	150
080 217.084958	218.156.211.19	192.168.1.71	TCP	1514	[TCP Spurious Retransmission] 80 - 6451 [ACK] Seq=16051 Ack=408 Win=4708 Len=1408	183
080 217.084958	218.156.211.19	192.168.1.71	TCP	1514	[TCP Spurious Retransmission] 80 - 6450 [ACK] Seq=16050 Ack=408 Win=4708 Len=1408	183
084 226.989853	218.156.211.20	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6459 [ACK] Seq=81789 Ack=22148 Len=1408	129
084 226.989853	218.156.211.20	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6458 [ACK] Seq=81788 Ack=22148 Len=1408	129
084 226.979052	218.156.211.20	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6459 [ACK] Seq=81788 Ack=22148 Len=1408	129
084 226.979052	218.156.211.20	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6458 [ACK] Seq=81788 Ack=22148 Len=1408	129
085 226.979052	218.156.211.20	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6459 [ACK] Seq=81788 Ack=22148 Len=1408	129
085 226.979052	218.156.211.20	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6458 [ACK] Seq=81788 Ack=22148 Len=1408	129
085 226.979052	218.156.211.20	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6459 [ACK] Seq=81788 Ack=22148 Len=1408	129
085 226.979052	218.156.211.20	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6458 [ACK] Seq=81788 Ack=22148 Len=1408	129
089 226.971539	218.156.211.19	192.168.1.71	TCP	972	[TCP Retransmission] 80 - 6306 [PSH, ACK] Seq=78821 Ack=3482 Win=23176 Len=518	40
051.227.388992	218.156.211.19	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6307 [ACK] Seq=34254 Ack=22084 Win=19660 Len=1408	47
049 227.388992	218.156.211.19	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6308 [ACK] Seq=34255 Ack=22084 Win=19660 Len=1408	47
047.227.327245	216.156.211.19	192.168.1.71	TCP	1514	[TCP Retransmission] 80 - 6304 [ACK] Seq=33996 Ack=2204 Win=22384 Len=1408	44
084.72.067308	54.292.140.193	192.168.1.71	TCP	1106	[TCP Spurious Retransmission] 80 - 6277 [PSH, ACK] Seq=34161 Ack=3810 Win=34810 Len=1132 [reassembled error, protocol TCP: New F...	23
084.72.067308	54.292.140.193	192.168.1.71	TCP	1106	[TCP Spurious Retransmission] 80 - 6278 [PSH, ACK] Seq=34162 Ack=3810 Win=34810 Len=1132 [reassembled error, protocol TCP: New F...	23
086.72.243456	54.292.140.193	192.168.1.71	TCP	1409	[TCP Spurious Retransmission] 80 - 6274 [PSH, ACK] Seq=8455 Ack=1747 Win=26752 Len=1451 [reassembled error, protocol TCP: New F...	18
029.73.207459	54.292.140.193	192.168.1.71	TCP	642	[TCP Spurious Retransmission] 80 - 6274 [PSH, ACK] Seq=34654 Ack=408 Win=28024 Len=580 [reassembled error, protocol TCP: New F...	18
029.73.207459	54.292.140.193	192.168.1.71	TCP	642	[TCP Spurious Retransmission] 80 - 6275 [PSH, ACK] Seq=34655 Ack=408 Win=28024 Len=580 [reassembled error, protocol TCP: New F...	18
014.73.179596	54.292.140.193	192.168.1.71	TCP	859	[TCP Spurious Retransmission] 80 - 6272 [PSH, ACK] Seq=50441 Ack=428 Win=34830 Len=785 [reassembled error, protocol TCP: New F...	16
078.71.472843	54.292.140.193	192.168.1.71	TCP	239	[TCP Spurious Retransmission] 80 - 6271 [PSH, ACK] Seq=209689 Ack=888 Win=24801 Len=179 [reassembled error, protocol TCP: New F...	15
078.71.472843	54.292.140.193	192.168.1.71	TCP	3141	[TCP Spurious Retransmission] 80 - 6272 [PSH, ACK] Seq=209690 Ack=888 Win=24801 Len=179 [reassembled error, protocol TCP: New F...	15

5. Frame 8500 is a retransmission triggered by duplicate ACKs. Why isn't it marked as a Fast Retransmission?

Answer: We can see that there are two duplicate ACK packets before frame 8500. If there are two duplicate ACKs in the reverse direction and if the packet occurs within 20ms of the last duplicate ACK then it will be considered as fast retransmission. Using a

timestamp of 8500 it was more than 20 ms longer than the previous frame. So, it isn't a fast retransmission.

No.	Time	Source	Destination	Protocol	Length	User-Agent	Info
8452	226.899178	192.168.1.71	216.156.211.19	TCP	54		6308 + 80 [ACK] Seq=3482 Ack=71521 Win=65536 Len=0
8453	226.899919	216.156.211.19	192.168.1.71	TCP	1514		80 + 6308 [ACK] Seq=71521 Ack=3482 Win=23176 Len=1460 [TCP segment of a reassembled PDU]
8454	226.899920	216.156.211.19	192.168.1.71	TCP	1514		80 + 6308 [ACK] Seq=72981 Ack=3482 Win=23176 Len=1460 [TCP segment of a reassembled PDU]
8455	226.899974	192.168.1.71	216.156.211.19	TCP	54		6308 + 80 [ACK] Seq=3482 Ack=74441 Win=65536 Len=0
8456	226.908719	216.156.211.19	192.168.1.71	TCP	1514		[TCP Previous segment not captured] 80 + 6308 [ACK] Seq=77361 Ack=3482 Win=23176 Len=1460 [TCP segment of a reassembled PDU]
8457	226.908720	216.156.211.19	192.168.1.71	TCP	572		80 + 6308 [PSH, ACK] Seq=78821 Ack=3482 Win=518 [TCP segment of a reassembled PDU]
8458	226.908720	216.156.211.19	192.168.1.71	TCP	1514		80 + 6415 [ACK] Seq=34611 Ack=1705 Win=18888 Len=1460 [TCP segment of a reassembled PDU]
8459	226.908721	216.156.211.20	192.168.1.71	TCP	60		80 + 6398 [ACK] Seq=85741 Ack=3899 Win=24248 Len=0
8460	226.908757	192.168.1.71	216.156.211.19	TCP	66		[TCP Dup ACK [455#]] 6308 + 80 [ACK] Seq=3482 Ack=74441 Win=65536 Len=0 SRE=77361
8461	226.908774	192.168.1.71	216.156.211.19	TCP	66		[TCP Dup ACK [455#]] 6308 + 80 [ACK] Seq=3482 Ack=74441 Win=65536 Len=0 SRE=77361 SRE=79339
8462	226.908813	192.168.1.71	216.156.211.19	TCP	54		6415 + 80 [ACK] Seq=1705 Ack=36071 Win=65536 Len=0
8463	226.901559	216.156.211.19	192.168.1.71	TCP	1514		80 + 6307 [ACK] Seq=25508 Ack=2204 Win=19960 Len=1460 [TCP segment of a reassembled PDU]
8464	226.901560	216.156.211.19	192.168.1.71	TCP	1514		80 + 6307 [ACK] Seq=26964 Ack=2204 Win=19960 Len=1460 [TCP segment of a reassembled PDU]
8465	226.901620	192.168.1.71	216.156.211.19	TCP	54		6307 + 80 [ACK] Seq=2204 Ack=28426 Win=65536 Len=0
8466	226.902369	216.156.211.19	192.168.1.71	TCP	1502		80 + 6307 [PSH, ACK] Seq=28426 Ack=2204 Win=19960 Len=1448 [TCP segment of a reassembled PDU]
8467	226.902371	216.156.211.26	192.168.1.71	TCP	60		80 + 6400 [ACK] Seq=90328 Ack=3835 Win=24248 Len=0
▼ Transmission Control Protocol, Src Port: 6308, Dst Port: 80, Seq: 3482, Ack: 74441, Len: 66							
Source Port: 6308 Destination Port: 80 [Stream index: 48] [Conversation completeness: Incomplete, DATA {15}] [TCP Segment Len: 0] Sequence Number: 3482 (relative sequence number) Sequence Number (raw): 2872908394 [Next Sequence Number: 3482 (relative sequence number)] Acknowledgment Number: 74441 (relative ack number) Acknowledgment number (raw): 1545819339 1000 ... = Header length: 32 bytes (8) Flags: 0x010 (ACK) Window: 256 [Calculated window size: 65536] [Window size scaling factor: 256] [hex dump, offset 0x0]							
0000: ac 5d 10 11 e2 b9 d4 3d 7e a6 43 6f 08 00 45 00 ·]-----=~Co-E- 0010: 00 34 2f 4a 40 00 80 06 00 00 c0 a8 01 47 db 9c -A/0-----G-- 0020: d3 13 18 a4 00 50 ab 3d 1a 68 5c 23 54 cb 80 18 -----P=0#@T--- 0030: 01 00 6d c6 00 00 01 01 05 04 5c 23 60 33 5c 23 --B-----\#3#\# 0040: 65 e7 e-							

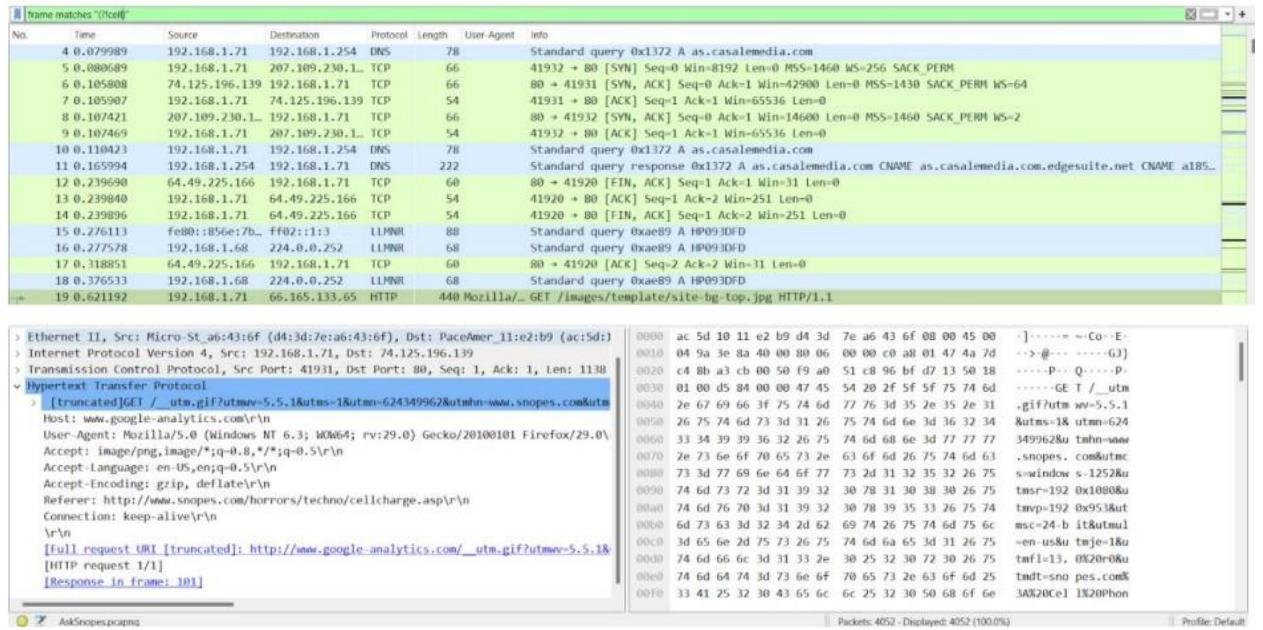
## OUCH! Trace File: AskSnopes.pcapng

- What web server software is used by www.snopes.com? Answer: Microsoft-IIS/5.0

- ▼ Hypertext Transfer Protocol
  - » GET /images/template/site-bg-top.jpg HTTP/1.1\r\n
 Host: www.snopes.com\r\n
 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0\r\n
 Accept: image/png,image/\*;q=0.8,\*/\*;q=0.5\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Referer: http://www.snopes.com/style.css\r\n
  - » Cookie: ASPSESSIONIDQQDDSBBA=OJMBNHECFANCNKIJJGBBMLDO\r\n
 Connection: keep-alive\r\n
 \r\n
 [Full request URI: http://www.snopes.com/images/template/site-bg-top.jpg]  
 [HTTP request 1/1]  
 [Response in frame: 52]

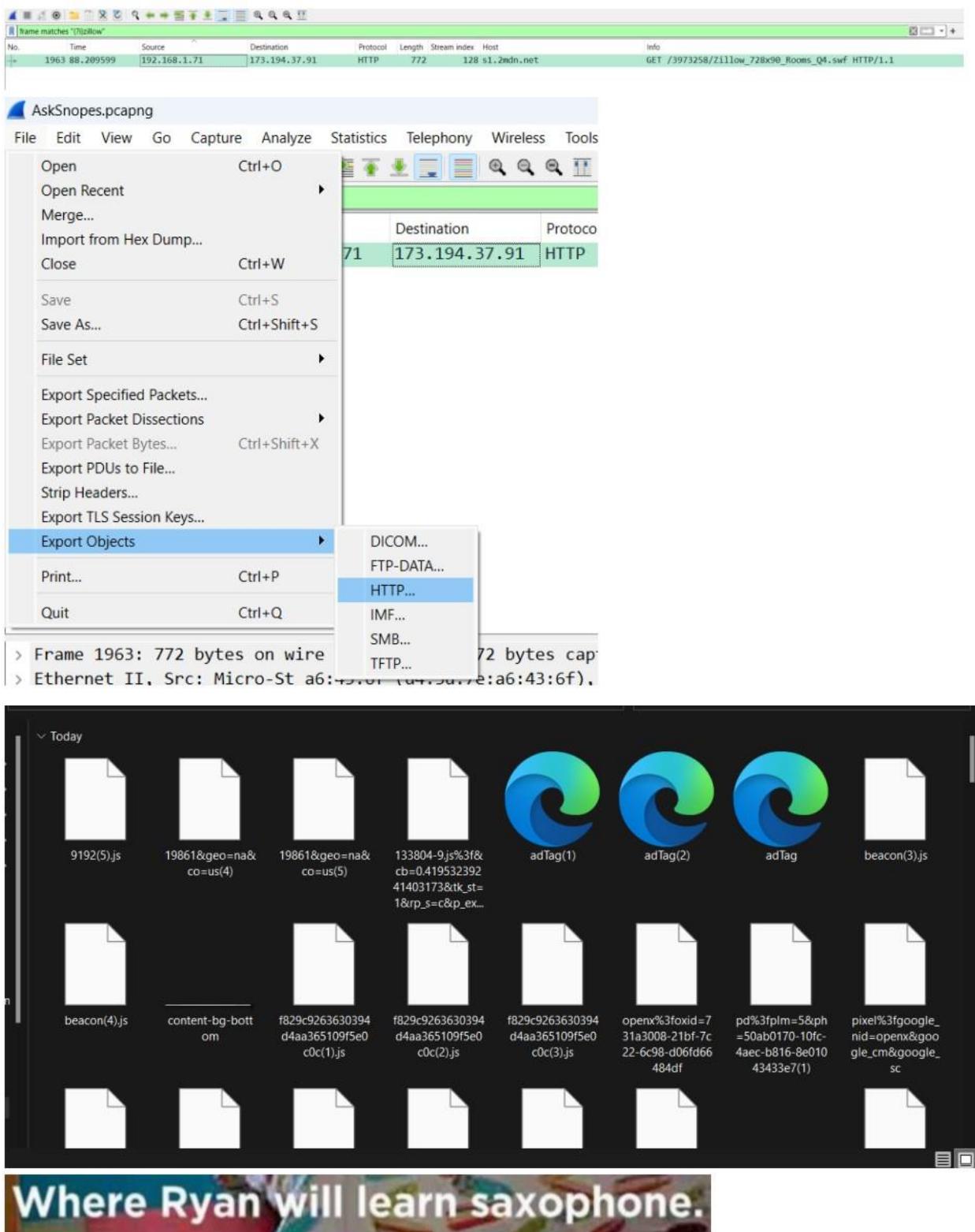
2. What cell phone problem is the client concerned?

Answer: Checking for cell phone references when we see the complete URL for No 94 we can see “Cell Phone Recharging Electrocution”.



### 3. According to Zillow, what instrument will Ryan learn to play?

Answer: Saxophone



4. How many web servers are running Apache?  
Answer: 21

http server matches "Apache"													
No.	Time	Source	Destination	Protocol	Length	User-Agent	Info						
112	3.567554	107.20.177.71	192.168.1.71	HTTP	955		HTTP/1.1 200 OK (application/x-javascript)						
1295	58.983848	107.20.177.71	192.168.1.71	HTTP	515		HTTP/1.1 200 OK (application/x-javascript)						
2443	104.056185	107.20.177.71	192.168.1.71	HTTP	836		HTTP/1.1 200 OK (application/x-javascript)						
3134	134.789555	107.20.177.71	192.168.1.71	HTTP	837		HTTP/1.1 200 OK (application/x-javascript)						
481	21.836459	162.248.16.28	192.168.1.71	HTTP	913		HTTP/1.1 200 OK (GIF89a)						
654	25.766962	162.248.16.24	192.168.1.71	HTTP	779		HTTP/1.1 200 OK (GIF89a)						
3554	164.813142	162.248.16.37	192.168.1.71	HTTP	74		HTTP/1.1 200 OK (text/html)						
366	16.184982	162.248.19.136	192.168.1.71	HTTP	721		HTTP/1.1 200 OK (text/html)						
372	16.229421	162.248.19.136	192.168.1.71	HTTP	721		HTTP/1.1 200 OK (text/html)						
417	20.900624	162.248.19.136	192.168.1.71	HTTP	921		HTTP/1.1 200 OK (GIF89a)						
2624	107.161753	199.189.107.4	192.168.1.71	HTTP	1368		HTTP/1.1 200 OK (JPEG JFIF image)						
2653	107.218339	199.189.107.4	192.168.1.71	HTTP	461		HTTP/1.1 200 OK (JPEG JFIF image)						
2664	107.287630	199.189.107.4	192.168.1.71	HTTP	960		HTTP/1.1 200 OK (JPEG JFIF image)						
2692	107.404002	199.189.107.4	192.168.1.71	HTTP	1161		HTTP/1.1 200 OK (JPEG JFIF image)						
743	31.501042	207.109.230.L	192.168.1.71	HTTP	1054		HTTP/1.1 200 OK (text/html)						
2043	91.652121	207.109.230.L	192.168.1.71	HTTP	1054		HTTP/1.1 200 OK (text/html)						

Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets A → A	Bytes A → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.71	23.23.197.19	2	1.151 KiB	13	15.38%	0	0 bytes	2	1.151 KiB	14.871442	9.0852	0 bytes	1.014 KiB
192.168.1.71	23.210.219.985	6	6.316 KiB	56	10.71%	0	0 bytes	6	6.316 KiB	7.762760	161.9039	0 bytes	319 bytes
192.168.1.71	23.210.231.153	12	6.019 KiB	314	3.82%	0	0 bytes	12	6.019 KiB	10.694794	184.0216	0 bytes	267 bytes
192.168.1.71	50.19.115.152	13	4.291 KiB	50	26.00%	0	0 bytes	13	4.291 KiB	2.871487	177.3290	0 bytes	198 bytes
192.168.1.71	50.97.236.98	2	1.712 KiB	36	5.56%	0	0 bytes	2	1.712 KiB	42.700396	67.8534	0 bytes	206 bytes
192.168.1.71	50.116.194.421	1	1.021 KiB	11	9.09%	0	0 bytes	1	1.021 KiB	76.690824	5.3140	0 bytes	1.536 KiB
192.168.1.71	50.116.194.28	1	527 bytes	11	9.09%	0	0 bytes	1	527 bytes	79.809615	5.3124	0 bytes	793 bytes
192.168.1.71	54.243.109.84	1	609 bytes	11	9.09%	0	0 bytes	1	609 bytes	106.497568	59.9250	0 bytes	81 bytes
192.168.1.71	63.135.172.251	2	837 bytes	14	14.29%	0	0 bytes	2	837 bytes	106.780786	6.3934	0 bytes	1.022 KiB
192.168.1.71	69.25.24.24	13	14.672 KiB	143	9.09%	0	0 bytes	13	14.672 KiB	24.755133	149.4709	0 bytes	804 bytes
192.168.1.71	69.25.24.26	3	3.015 KiB	30	10.00%	0	0 bytes	3	3.015 KiB	42.755805	97.9370	0 bytes	252 bytes
192.168.1.71	107.20.177.71	4	3.069 KiB	29	13.79%	0	0 bytes	4	3.069 KiB	2.911223	191.8342	0 bytes	131 bytes
192.168.1.71	162.248.16.24	2	1.652 KiB	24	8.33%	0	0 bytes	2	1.652 KiB	21.300858	4.4916	0 bytes	2.942 KiB
192.168.1.71	162.248.16.37	1	74 bytes	32	3.13%	0	0 bytes	1	74 bytes	153.981593	10.8567	0 bytes	54 bytes
192.168.1.71	162.248.19.136	3	2.308 KiB	42	7.14%	0	0 bytes	3	2.308 KiB	14.992486	8.9642	0 bytes	2.059 KiB
192.168.1.71	207.109.230.154	3	3.088 KiB	44	6.82%	0	0 bytes	3	3.088 KiB	31.446135	115.1637	0 bytes	219 bytes
192.168.1.71	207.109.230.161	2	1.146 KiB	30	6.67%	0	0 bytes	2	1.146 KiB	0.080689	171.0507	0 bytes	54 bytes
192.168.1.71	207.109.230.187	3	2.965 KiB	42	7.14%	0	0 bytes	3	2.965 KiB	130.470514	64.2095	0 bytes	378 bytes
192.168.1.71	216.39.54.212	1	225 bytes	12	8.33%	0	0 bytes	1	225 bytes	14.893408	1.0217	0 bytes	1.720 KiB
199.189.107.4	192.168.1.71	4	3.857 KiB	209	1.91%	4	3.857 KiB	0	0 bytes	3.194677	109.2084	289 bytes	0 bytes

## 5. What hosts (IP addresses) think that jokes are more entertaining when they are explained?

Answer: 173.241.244.7, 173.241.244.99, 173.241.244.153

No.	Time	Source	Destination	Protocol	Length	User-Agent	Info						
1704	79.610211	173.241.244.7	192.168.1.71	HTTP	509		HTTP/1.1 302 Moved Temporarily						
1712	79.68924	173.241.244.7	192.168.1.71	TCP	362		80 → 42039 [PSH, ACK] Seq=1 Ack=776 Win=8190 Len=308 [TCP segment of a reassembled PDU]						
1720	79.82471	173.241.244.7	192.168.1.71	TCP	362		80 → 42038 [PSH, ACK] Seq=1 Ack=797 Win=8190 Len=308 [TCP segment of a reassembled PDU]						
1725	79.916204	173.241.244.7	192.168.1.71	TCP	362		80 → 42040 [PSH, ACK] Seq=1 Ack=776 Win=8190 Len=308 [TCP segment of a reassembled PDU]						
3851	185.6666031	173.241.244.7	192.168.1.71	TCP	362		80 → 42179 [PSH, ACK] Seq=1 Ack=1033 Win=8190 Len=308 [TCP segment of a reassembled PDU]						
3857	185.741891	173.241.244.7	192.168.1.71	TCP	362		80 → 42181 [PSH, ACK] Seq=1 Ack=1040 Win=8190 Len=308 [TCP segment of a reassembled PDU]						
3867	185.821000	173.241.244.7	192.168.1.71	TCP	362		80 → 42183 [PSH, ACK] Seq=1 Ack=1038 Win=8190 Len=308 [TCP segment of a reassembled PDU]						
3871	185.886139	173.241.244.7	192.168.1.71	TCP	362		80 → 42188 [PSH, ACK] Seq=1 Ack=1033 Win=8190 Len=308 [TCP segment of a reassembled PDU]						
3875	185.966567	173.241.244.7	192.168.1.71	TCP	362		80 → 42182 [PSH, ACK] Seq=1 Ack=1033 Win=8190 Len=308 [TCP segment of a reassembled PDU]						
1923	71.671370	173.241.244.99	192.168.1.71	TCP	1514		80 → 42026 [ACK] Seq=1 Ack=395 Win=8190 Len=1460 [TCP segment of a reassembled PDU]						
1563	72.870190	173.241.244.99	192.168.1.71	TCP	1514		80 → 42028 [ACK] Seq=1 Ack=876 Win=8190 Len=1460 [TCP segment of a reassembled PDU]						
1590	74.327106	173.241.244.99	192.168.1.71	HTTP	424		HTTP/1.1 200 OK (GIF89a)						
3647	174.461200	173.241.244.99	192.168.1.71	TCP	1514		80 → 42169 [ACK] Seq=1 Ack=639 Win=8190 Len=1460 [TCP segment of a reassembled PDU]						
3705	176.346391	173.241.244.99	192.168.1.71	TCP	1514		[TCP Fast Retransmission] 80 → 42170 [ACK] Seq=1 Ack=1120 Win=8190 Len=1460 [TCP segment of a reassembled PDU]						
3735	178.076445	173.241.244.99	192.168.1.71	HTTP	424		HTTP/1.1 200 OK (GIF89a)						
636	25.600785	66.165.133.65	192.168.1.71	TCP	1514		80 → 41971 [ACK] Seq=16061 Ack=854 Win=16667 Len=1460 [TCP segment of a reassembled PDU]						

## Wireshark Challenge 2

Examine the wireshark window and find answers to the following questions:

- This packet capture file contains two TCP handshakes. Find the first handshake and write down the packet numbers of those packets (the column labeled "No."). Ans: Packets: 1, 2 and 3

No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
1	0.000000	10.100.1.24	74.125.19.113	TCP	66 ✓		51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 ✓		80 + 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
5	0.044744	74.125.19.113	10.100.1.24	TCP	54 ✓		80 + 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6	0.081566	74.125.19.113	10.100.1.24	HTTP	401 ✓		HTTP/1.1 200 OK (text/javascript)
7	0.281518	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=495 Ack=348 Win=16384 Len=0

2. In this session, a client machine initiated a connection to a server and then downloaded a file. What is the client's IP address?

Ans: 10.100.1.24

No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
1	0.000000	10.100.1.24	74.125.19.113	TCP	66 ✓		51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 ✓		80 + 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
5	0.044744	74.125.19.113	10.100.1.24	TCP	54 ✓		80 + 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6	0.081566	74.125.19.113	10.100.1.24	HTTP	401 ✓		HTTP/1.1 200 OK (text/javascript)

3. How many HTTP GET request packets are there? Ans: 3

No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
13	0.590925	10.100.1.24	147.144.1.212	HTTP	484 ✓		GET /Graphics/ccsfseal.gif HTTP/1.1
28	1.594435	10.100.1.24	147.144.1.212	HTTP	387 ✓		GET /favicon.ico HTTP/1.1

4. Find the first HTTP GET request packet. What was the server's IP address? (The server is the Destination).

Ans: 74.125.19.113

No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
1	0.000000	10.100.1.24	74.125.19.113	TCP	66 ✓		51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 ✓		80 + 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
5	0.044744	74.125.19.113	10.100.1.24	TCP	54 ✓		80 + 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6	0.081566	74.125.19.113	10.100.1.24	HTTP	401 ✓		HTTP/1.1 200 OK (text/javascript)

5. Examine the first packet. Look at the center pane in Wireshark. How many bytes were sent on the wire to form this packet?

Ans: 66 bytes

No.	Time	Source	Destination	Protocol	Length	Frame	Info
1	0.000000	10.100.1.24	74.125.19.113	TCP	66 ✓		51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 ✓		80 + 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
5	0.044744	74.125.19.113	10.100.1.24	TCP	54 ✓		80 + 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6	0.081566	74.125.19.113	10.100.1.24	HTTP	401 ✓		HTTP/1.1 200 OK (text/javascript)

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
Encapsulation type: Ethernet (1)  
Arrival Time: Sep 3, 2009 22:11:38.447250000 India Standard Time

## Wireshark Challenge 3 WHAT

### THE HECK?

TRACE FILE: challengescan.pcapng

**BACKGROUND:** This captured file was taken from a very large and well-established network that had been considered very stable and unchanging. The network administrator has given you this file that contains what he considers “suspicious” behavior and has asked you to evaluate it.

## QUESTIONS:

1. What is the IP address of the scanning host?

Answer: 192.168.1.141

Analysis – ICMP echo request is coming through 192.168.1.141.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.141	192.168.1.123	ICMP	98	Echo (ping) request id=0xdb2b, seq=0/0, ttl=64 (reply in 2)
2	0.000034	192.168.1.123	192.168.1.141	ICMP	98	Echo (ping) reply id=0xdb2b, seq=0/0, ttl=32 (request in 1)
3	0.007962	192.168.1.141	192.168.1.123	ICMP	98	Echo (ping) request id=0xdb2b, seq=1/256, ttl=64 (reply in 4)
4	0.007982	192.168.1.123	192.168.1.141	ICMP	98	Echo (ping) reply id=0xdb2b, seq=1/256, ttl=32 (request in 3)
5	0.058086	192.168.1.141	192.168.1.123	ICMP	60	Timestamp request id=0xdb2b, seq=0/0, ttl=64

2. What is the IP address of the target host?

Answer: 192.168.1.123

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.141	192.168.1.123	ICMP	98	Echo (ping) request id=0xdb2b, seq=0/0, ttl=64 (reply in 2)
2	0.000034	192.168.1.123	192.168.1.141	ICMP	98	Echo (ping) reply id=0xdb2b, seq=0/0, ttl=32 (request in 1)
3	0.007962	192.168.1.141	192.168.1.123	ICMP	98	Echo (ping) request id=0xdb2b, seq=1/256, ttl=64 (reply in 4)
4	0.007982	192.168.1.123	192.168.1.141	ICMP	98	Echo (ping) reply id=0xdb2b, seq=1/256, ttl=32 (request in 3)
5	0.058086	192.168.1.141	192.168.1.123	ICMP	60	Timestamp request id=0xdb2b, seq=0/0, ttl=64

3. Which TCP port opens on the target?

Answer: Port 68

Analysis: Find SYN,ACK Packet and its source host

No.	Time	Source	Destination	Protocol	Length	Info
145	3678.513...	192.168.1.141	192.168.1.123	TCP	74	53187 → 66 [SYN] Seq=0 Win=5840 MSS=1460 SACK_PERM=1 TSval=4233011 TSecr=0 WS=4
146	3678.513...	192.168.1.123	192.168.1.141	TCP	54	66 → 53187 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
147	3678.513...	192.168.1.141	192.168.1.123	TCP	74	47660 → 67 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=4233012 TSecr=0 WS=4
148	3678.513...	192.168.1.123	192.168.1.141	TCP	54	67 → 47660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	3678.513...	192.168.1.141	192.168.1.123	TCP	74	42993 → 68 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=4233012 TSecr=0 WS=4
150	3678.513...	192.168.1.123	192.168.1.141	TCP	74	68 + 42993 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4097742 TS...

> Internet Protocol Version 4, Src: 192.168.1.123, Dst: 192.168.1.141  
  Transmission Control Protocol, Src Port: 68, Dst Port: 42993, Seq: 0, Ack: 1, Len: 0  
    Source Port **68**

4. Which ICMP packets contain non-standard Type/Code numbers?

Answer: Code 123

Analysis: After checking all ICMP packets, the selected 4 packets had code 123. Others had 0 and 3

No.	Time	Source	Destination	Protocol	Length	Info
16.	3751.790...	192.168.1.123	192.168.1.141	ICMP	296	Echo (ping) reply id=0x0001, seq=1/256, ttl=32 (request in 1651)
16.	3751.796...	192.168.1.123	192.168.1.141	ICMP	296	Echo (ping) reply id=0x0001, seq=1/256, ttl=32 (request in 1653)
16..	3752.805...	192.168.1.123	192.168.1.141	ICMP	43	Echo (ping) reply id=0x0001, seq=1/256, ttl=32 (request in 1655)
10..	3716.112...	192.168.1.141	192.168.1.123	ICMP	60	Echo (ping) reply id=0x029c, seq=1/256, ttl=64
16..	3751.234...	192.168.1.123	192.168.1.141	ICMP	46	Echo (ping) reply id=0x02a6, seq=1/256, ttl=32 (request in 1631)
+ 833	3697.715...	192.168.1.123	192.168.1.141	ICMP	12	Echo (ping) reply id=0x70d0, seq=28880/53360, ttl=32 (request in 832)
2 0.000034	192.168.1.123	192.168.1.141	ICMP	98	Echo (ping) reply id=0xdb2b, seq=0/0, ttl=32 (request in 1)	
4 0.007982	192.168.1.123	192.168.1.141	ICMP	98	Echo (ping) reply id=0xdb2b, seq=1/256, ttl=32 (request in 3)	
13	3678.493...	192.168.1.141	192.168.1.123	ICMP	60	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 14)
16..	3751.767...	192.168.1.141	192.168.1.123	ICMP	60	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1644)
16..	3751.772...	192.168.1.141	192.168.1.123	ICMP	296	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1646)
16..	3751.779...	192.168.1.141	192.168.1.123	ICMP	296	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1648)
16..	3751.784...	192.168.1.141	192.168.1.123	ICMP	296	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1650)
16..	3751.790...	192.168.1.141	192.168.1.123	ICMP	296	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1652)
16..	3751.796...	192.168.1.141	192.168.1.123	ICMP	296	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1654)
16..	3752.805...	192.168.1.141	192.168.1.123	ICMP	60	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1656)
16..	3751.234...	192.168.1.141	192.168.1.123	ICMP	60	Echo (ping) request id=0x02a6, seq=1/256, ttl=255 (reply in 1632)
+ 832	3697.715...	192.168.1.141	192.168.1.123	ICMP	60	Echo (ping) request id=0x70d0, seq=28880/53360, ttl=64 (reply in 833)
1 0.000000	192.168.1.141	192.168.1.123	ICMP	98	Echo (ping) request id=0xdb2b, seq=0/0, ttl=64 (reply in 2)	
3 0.007962	192.168.1.141	192.168.1.123	ICMP	98	Echo (ping) request id=0xdb2b, seq=1/256, ttl=64 (reply in 4)	
865	3700.790...	192.168.1.141	192.168.1.123	ICMP	60	Information request id=0x5c36, seq=1/256, ttl=255
871	3701.868...	192.168.1.141	192.168.1.123	ICMP	60	Information request id=0x5c36, seq=1/256, ttl=255
874	3703.003...	192.168.1.141	192.168.1.123	ICMP	60	Information request id=0x5c36, seq=1/256, ttl=255
8 0.105926	192.168.1.141	192.168.1.123	ICMP	60	Information request id=0xdb2b, seq=0/0, ttl=64	
v Internet Control Message Protocol						
Type:	A (Echo (ping) reply)					
Code:	123					
Checksum:	0x1de4 [correct]					

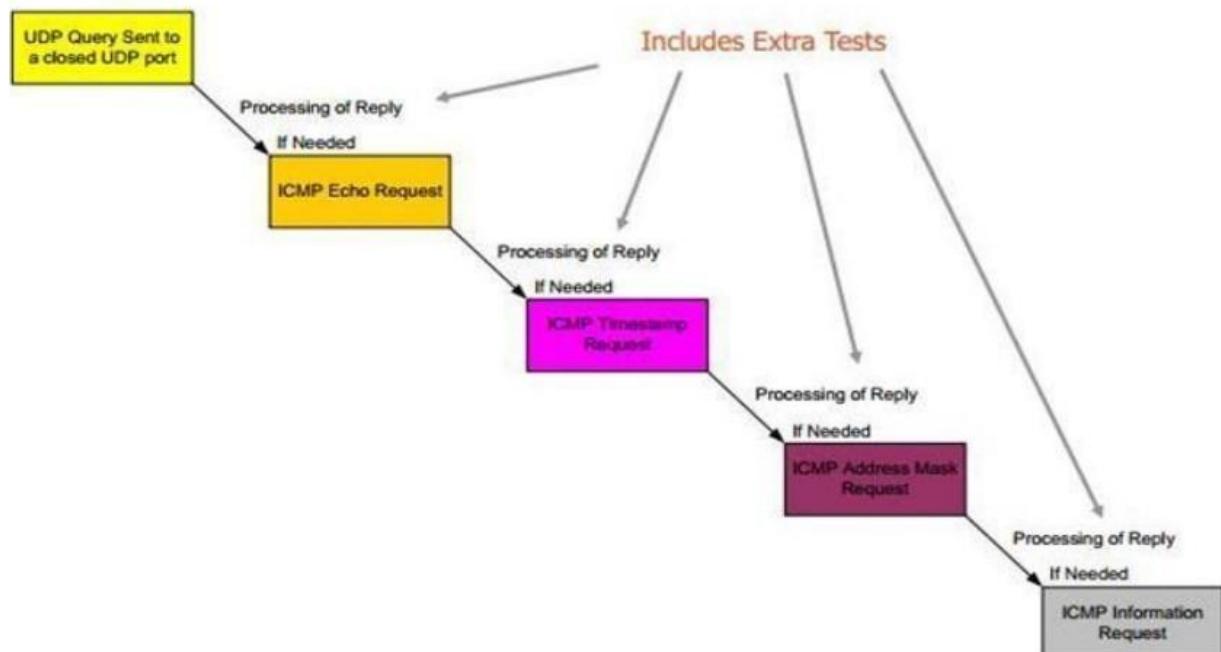
5. What software is used to scan the target?

Answer: Xprobe

Analysis:

## Xprobe - The Signature Based Approach

### The Logic Of Initiation of Queries



As can be seen in the above diagram, it is an ICMP based scan and the first request is an ICMP echo request; after that it sends the ICMP timestamp request, then it sends the

ICMP address mask request, and at last it sends the ICMP information request. The same pattern is also available in the trace file where we applied the filter for ICMP packets.

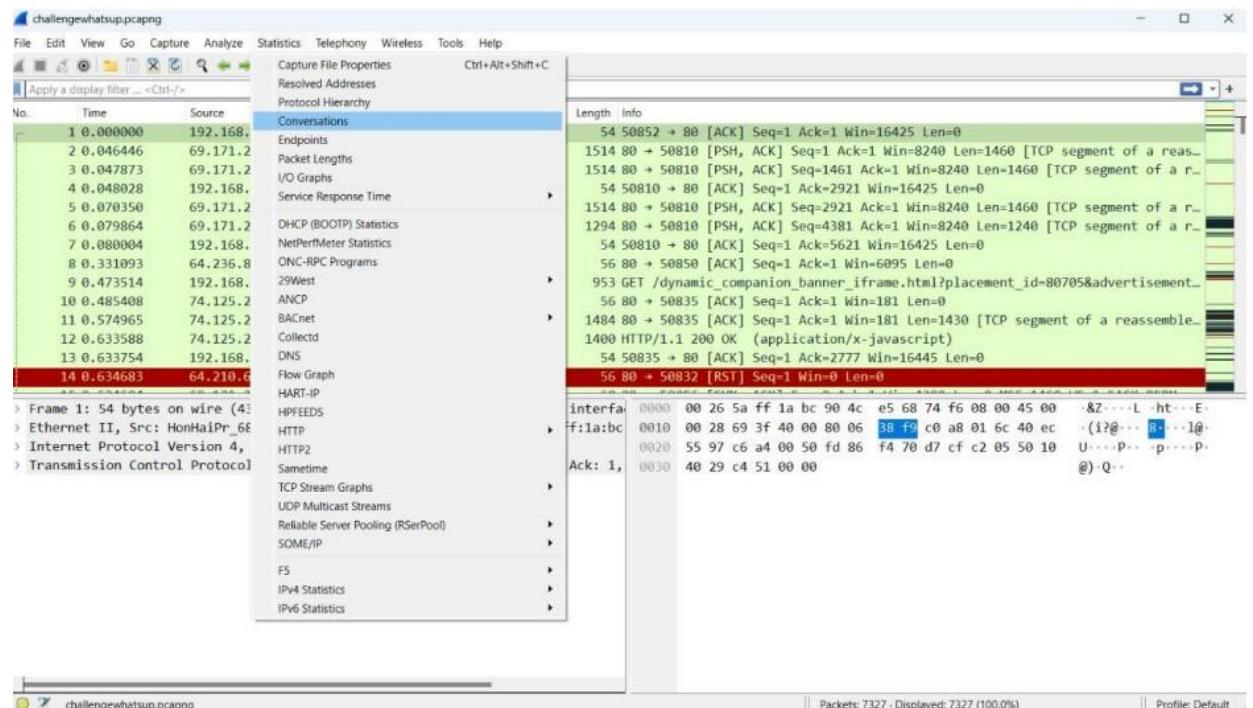
Expression... Clear Apply Save					
Time	Source	Destination	Protocol	Length	Info
1 0.000000000	192.168.1.141	192.168.1.123	ICMP	98	Echo (ping) request
2 0.000034000	192.168.1.123	192.168.1.141	ICMP	98	Echo (ping) reply
3 0.007962000	192.168.1.141	192.168.1.123	ICMP	98	Echo (ping) request
4 0.007982000	192.168.1.123	192.168.1.141	ICMP	98	Echo (ping) reply
5 0.058086000	192.168.1.141	192.168.1.123	ICMP	60	Timestamp request
6 0.058104000	192.168.1.123	192.168.1.141	ICMP	54	Timestamp reply
7 0.080966000	192.168.1.141	192.168.1.123	ICMP	60	Address mask request
8 0.105926000	192.168.1.141	192.168.1.123	ICMP	60	Information request
10 0.305756000	192.168.1.123	192.168.1.141	ICMP	146	Destination unreachable (Port unreachable)
13 3678.4937840	192.168.1.141	192.168.1.123	ICMP	60	Echo (ping) request
14 3678.4938130	192.168.1.123	192.168.1.141	ICMP	42	Echo (ping) reply
518 3680.6034700	192.168.1.123	192.168.1.141	ICMP	72	Destination unreachable (Port unreachable)
530 3680.6640110	192.168.1.123	192.168.1.141	ICMP	126	Destination unreachable (Port unreachable)
532 3680.6645770	192.168.1.123	192.168.1.141	ICMP	126	Destination unreachable (Port unreachable)
539 3680.6799280	192.168.1.123	192.168.1.141	ICMP	90	Destination unreachable (Port unreachable)
563 3680.7443950	192.168.1.123	192.168.1.141	ICMP	110	Destination unreachable (Port unreachable)
565 3680.7509100	192.168.1.123	192.168.1.141	ICMP	118	Destination unreachable (Port unreachable)
610 3681.6501260	192.168.1.123	192.168.1.141	ICMP	111	Destination unreachable (Port unreachable)
634 3682.6499840	192.168.1.123	192.168.1.141	ICMP	110	Destination unreachable (Port unreachable)

## Cursed

- How many different IP hosts is Scott's machine communicating with?

Answer: 142

First we have to check the communication which can be seen by opening Statistics > Conversations



Then we can select the Ipv4 tab and see the count is 142 which means that there are 142 Ips communicating with Scott's machine.

Conversation Settings													
Ethernet - 2	IPv4 - 142	IPv6	TCP - 311	UDP									
<input type="checkbox"/> Name resolution	Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets A → B	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
<input type="checkbox"/> Absolute start time	23.21.171.74	192.168.1.108	3	164 bytes	1	56 bytes	2	108 bytes	30.156293	2.4244	184 bytes	356 bytes	
<input type="checkbox"/> Limit to display filter	62.128.215.93	192.168.1.108	15	3.368 kB	8	2.268 kB	7	1.101 kB	0.827118	28.7583	645 bytes	313 bytes	
	64.210.61.214	192.168.1.108	13	4.922 kB	4	248 bytes	9	4.680 kB	0.634683	30.9873	64 bytes	1.208 kB	
	69.171.228.14	192.168.1.108	80	55.010 kB	41	41.330 kB	39	13.680 kB	0.046444	237.1490	1.394 kB	472 bytes	
	69.194.244.11	192.168.1.108	3	164 bytes	1	56 bytes	2	108 bytes	3.933056	0.3242	1.349 kB	2.602 kB	
	74.125.224.91	192.168.1.108	210	118.388 kB	108	78.070 kB	102	40.317 kB	0.485400	236.8815	2.636 kB	1.361 kB	
	157.55.178.11	192.168.1.108	2	110 bytes	1	56 bytes	1	54 bytes	29.735205	0.0000			
	178.238.225.233	192.168.1.108	61	24.485 kB	34	12.391 kB	27	12.095 kB	35.657576	171.1392	593 bytes	578 bytes	
	192.168.1.108		4.26.45.200	11	2.909 kB	6	1.990 kB	5	941 bytes	29.79428E	0.6402	24.869 kB	11.482 kB
	192.168.1.108		4.30.14.112	21	13.900 kB	10	1.122 kB	11	12.778 kB	28.09632C	0.3936	22.806 kB	259.715 kB
	192.168.1.108		4.71.251.71	14	7.212 kB	8	5.071 kB	6	2.141 kB	206.434405	2.7622	14.688 kB	6.199 kB
	192.168.1.108		8.21.24.35	70	18.234 kB	33	7.977 kB	37	10.258 kB	28.09358A	3.2323	19.741 kB	25.388 kB
	192.168.1.108		12.129.199.107	11	3.313 kB	6	1.934 kB	5	1.380 kB	206.58679C	10.7641	1.437 kB	1.025 kB
	192.168.1.108		12.129.210.71	11	4.729 kB	6	1.985 kB	5	2.743 kB	223.66895F	0.1818	87.379 kB	120.731 kB
	192.168.1.108		12.130.81.249	27	10.542 kB	16	4.938 kB	11	5.604 kB	33.722570	182.7233	221 bytes	251 bytes
	192.168.1.108		23.0.1.107	19	10.928 kB	10	1.085 kB	9	9.843 kB	207.68711F	0.4146	20.934 kB	189.917 kB
	192.168.1.108		23.0.2.77	19	6.979 kB	10	3.559 kB	9	3.421 kB	216.60382Z	18.6051	1.529 kB	1.471 kB
	192.168.1.108		23.0.4.46	8	2.965 kB	4	753 bytes	4	2.229 kB	228.09885F	0.0419	140.531 kB	426.075 kB
	192.168.1.108		23.0.13.229	20	11.349 kB	9	5.322 kB	11	6.026 kB	204.461251	1.5744	27.043 kB	30.621 kB
	192.168.1.108		23.0.247.755	40	19.510 kB	21	4.090 kB	19	15.240 kB	207.86196C	6.1821	5.292 kB	19.954 kB
	192.168.1.108		23.0.247.231	62	38.136 kB	37	12.218 kB	25	25.918 kB	201.006114	26.5589	3.680 kB	7.807 kB
	192.168.1.108		23.1.12.74	34	19.776 kB	15	5.983 kB	19	13.793 kB	222.28415F	1.1500	41.624 kB	95.953 kB
	192.168.1.108		23.21.208.149	17	12.210 kB	7	1.009 kB	10	11.201 kB	224.40901E	0.9756	8.271 kB	91.852 kB
	192.168.1.108		23.47.192.143	11	4.946 kB	6	2.062 kB	5	2.885 kB	199.99591Z	0.2671	61.736 kB	86.390 kB

## 2. What is the average packets per second rate seen in this trace file?

Answer: 30.9

We can check out the packets rate per second from the summary options. Select > Statistics > Capture File Properties And as shown below, we can see the average packets rate per second

### Statistics

Measurement	Captured	Displayed	Marked
Packets	7327	7327 (100.0%)	—
Time span, s	237.435	237.435	—
Average pps	30.9	30.9	—
Average packet size, B	601	601	—
Bytes	4400914	4400914 (100.0%)	0
Average bytes/s	18 k	18 k	—
Average bits/s	148 k	148 k	—

## 3. How many HTTP POST requests did Scott's machine send?

Answer: 3

We applied a filter i.e. http.request.method == POST to filter only POST requests

http.request.method==POST						
No.	Time	Source	Destination	Protocol	Length	Info
839	33.619829	192.168.1.108	209.196.28.153	HTTP	1141	POST /ssframework/log/log.png HTTP/1.1 (application/x-www-form-urlencoded)
1367	194.916693	192.168.1.108	174.129.196.71	HTTP	1049	POST /click.php HTTP/1.1 (application/x-www-form-urlencoded)
3129	206.927181	192.168.1.108	174.129.196.71	HTTP	1043	POST /click.php HTTP/1.1 (application/x-www-form-urlencoded)

## 4. What location information is contained in the POST to scanscout.com?

Answer: San Francisco – Oakland – San Jose

First find the POST request, and there are only three of them, and next we have to find which request header contains the scanscout.com. We checked out all three requests and found one of the request headers is for scanscout.com.

```
Content-Type: application/x-www-form-urlencoded\r\n> Content-Length: 1087\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Tri\r\nHost: 10.scanscout.com\r\nConnection: Keep-Alive\r\nCache-Control: no-cache\r\n> [truncated]Cookie: JSESSIONID=4796945C3507E0759E0B8CC5BE215E5B; uid=bb2d\r\n\r\n[Full request URI: http://10.scanscout.com/ssframework/log/log.png]\r\n[HTTP request 1/1]\r\n[Response in frame: 889]\r\nFile Data: 1087 bytes\r\n> HTML Form URL Encoded: application/x-www-form-urlencoded
```

After that we need to find the location. So to find it click on the POST request and select follows TCP stream.

POST /ssframework/log/log.png HTTP/1.1

Accept: \*/\*

Accept-Language: en-US

Referer: http://static3.filmannex.com/[[IMPORT]]/objects.tremormedia.com/embed/swf/acudeo.swf

x-flash-version: 11,1,102,55

Content-Type: application/x-www-form-urlencoded

Content-Length: 1087

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; HPNTDF; InfoPath.2; .NET4.0C; .NET4.0E)

Host: 10.scanscout.com

Connection: Keep-Alive

Cache-Control: no-cache

Cookie: JSESSIONID=4796945C3507E0759E0B8CC5BE215E5B; uid=bb2d96a857fc5ffd0b957a840f4acf14; unq=120330|57831\_120330|60434\_120330|116861\_120330; psh=57831\_1333126829691\_1333126850428\_1333126906254\_1333126928598\_1333126936636|60434\_1333126915339\_1333127003592\_1333127021459\_1333127074499|116861\_1333127447194; bsm=3611\_120330\_4|6021\_120330|6061\_120330\_3|6071\_120330; VKRS=3RPXG0de1VFmCX14-7\_9kR-UNefWMvVsDTeORmKCF4edTM5Nvp-PuKg; networkInfo=57543|120330\_130227|57831|89fdbba31d74cca9fad87f406b6a23dba|0|5997161|1451741|1|8.97517865131891|true|4|true|us|V|943981|0|h0fhcvng1j0nx469e6mh1; cmpUnq=1451741; sssrvyhst2=120330\_1451741; sssrvyhst=120330\_731

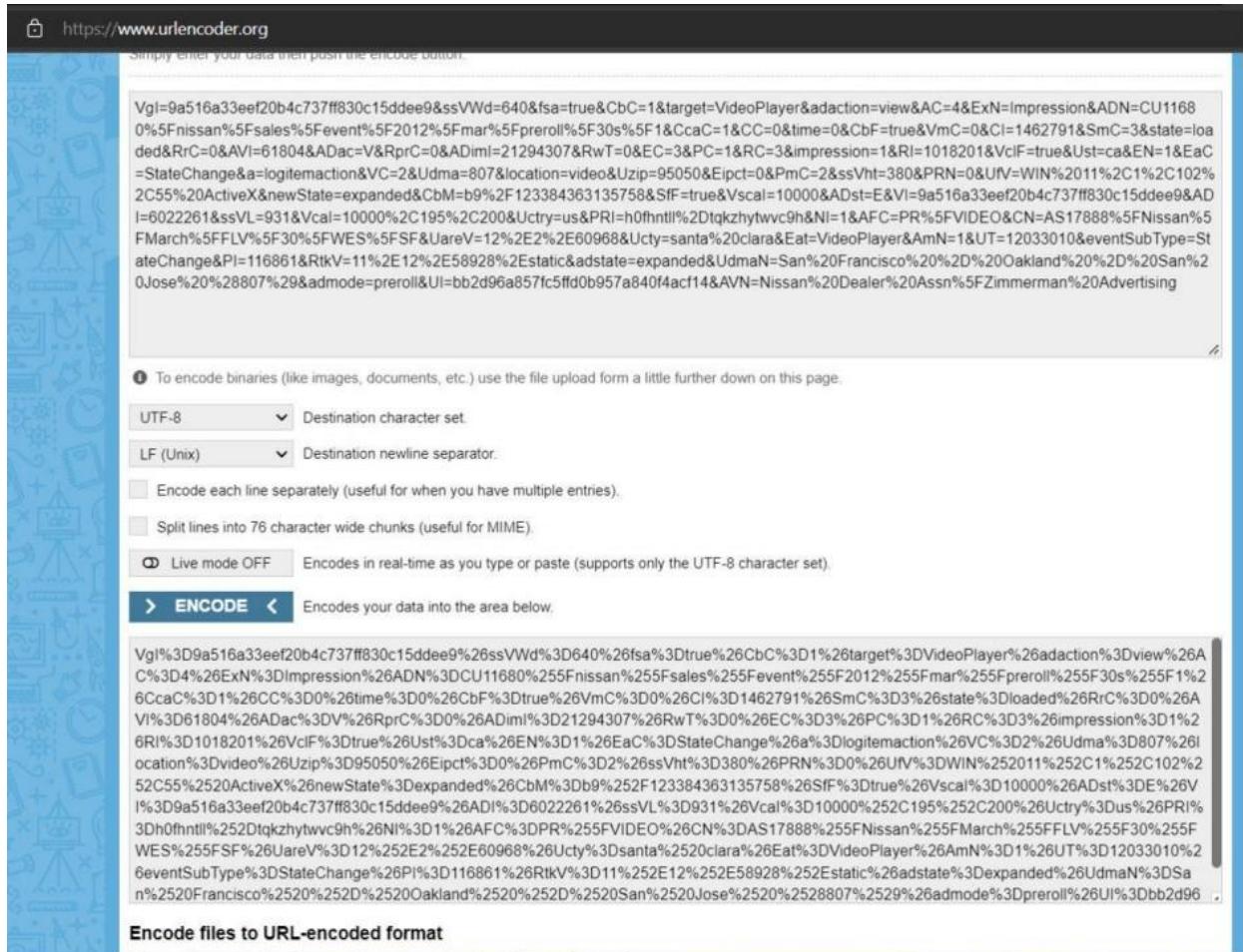
VgI=9a516a33eeef20b4c737ff830c15ddee9&ssVWd=640&fsa=true&CbC=1&target=VideoPlayer&adaction=view&AC=4&ExN=Impression&ADN=CU11680%5Fnissan%5Fsales%5Fevent%5F2012%5Fmar%5Fpreroll%5F30s%5F1&CcaC=1&CC=0&time=0&CbF=true&VmC=0&CI=1462791&SmC=3&state=loaded&RrC=0&AVI=61804&ADac=V&RprC=0&AdimI=21294307&RwT=0&EC=3&PC=1&RC=3&impression=1&RI=1018201&VclF=true&Ust=ca&EN=1&EaC=StateChange&a=logitemaction&VC=2&Udma=807&location=video&Uzip=95050&Eipct=0&PmC=2&ssVht=380&PRN=0&UFV=WIN%2011%2C1%2C102%2C55%20ActiveX&newS

2 client pkts, 1 server pkt, 1 turn.

Entire conversation (3469 bytes) Show data as ASCII Stream 72

Find: Find Next Filter Out This Stream Print Save as... Back Close Help

As can be seen below we can now see the whole POST data of that request. It contains a lot of parameters and its value and its URL are encoded, so we are not able to read them clearly. We copied the whole data and used a url decoder.



Now we can see in the below figure that the parameter Udam has its value San Francisco – Oakland – San Jose.

5. What application appears to be generating these GET/POST requests?

Answer: Internet Explorer 9

It can be done by analyzing the User-Agent string of any GET/POST request

POST /ssframework/log/log.png HTTP/1.1

Accept: \*/\*

Accept-Language: en-US

Referer: http://static3.filmannex.com/

x-flash-version: 11.1.103.55

X-Flash-Version: 11,1,102,33

Content-Type: application/x-tar

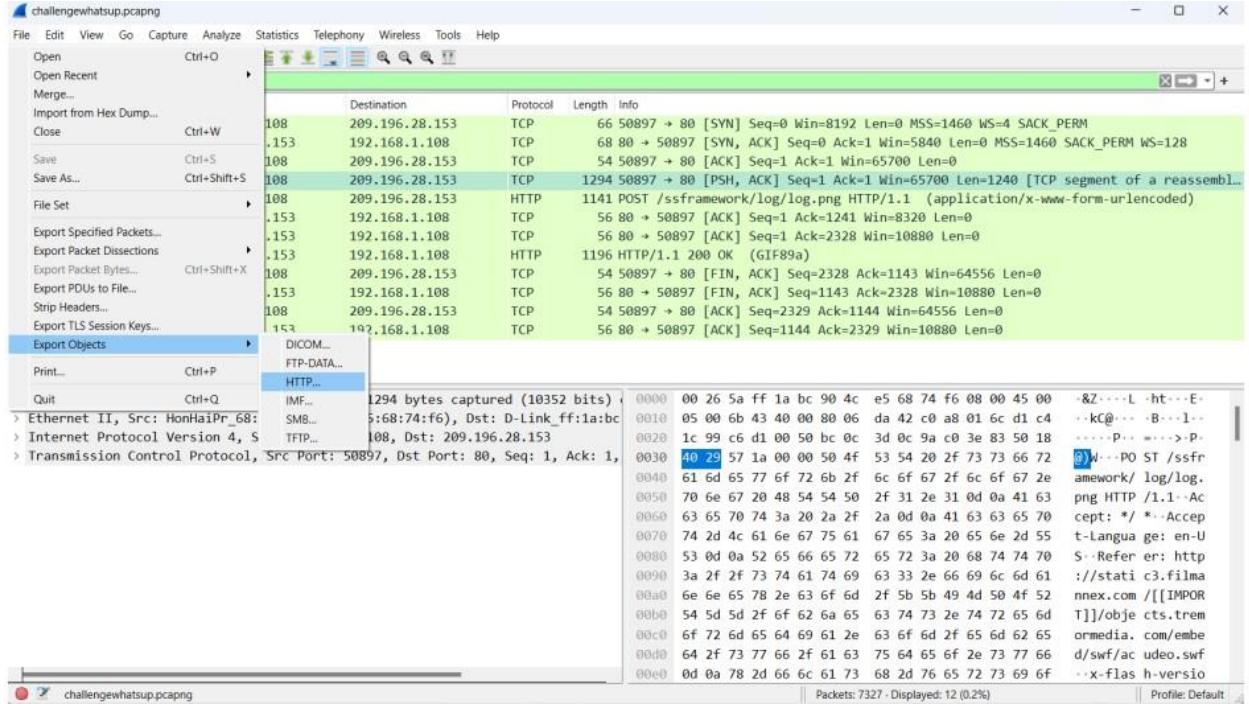
Content-Length: 1087  
Accept-Encoding: gzip, deflate

Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; HPNTDF; InfoPath.2; .NET4.0C;.NET4.0E)

6. Find, export and reassemble load small.png. what shape is in the image?

Answer: Star

We have to find a .png image in this. All packets can't check every request manually and look for this image, so we will extract all the HTTP objects from this trace file. Go to File and select Export Objects > HTTP



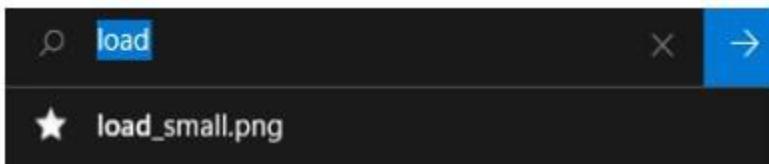
Wireshark - Export - HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
12	ad.doubleclick.net	application/x-javascript	6718 bytes	activity;src=1361550;met=1;v319 bytes
26			26 kB	like.php?api_key=171818996
38	www.facebook.com	text/html	1019 bytes	dynamic_companion_banner
44	pl.yumenetworks.com	text/html	9120 bytes	likebox.php?href=http%3A%
54	www.facebook.com	text/html	4302 bytes	;
58	ad.doubleclick.net	text/html	653 bytes	www.celebgossip.com
73	delivery.serve.m80marketing.com	text/javascript	6735 bytes	optn=64?trg=;ord=14873702
84	ad.doubleclick.net	application/x-javascript	32 kB	1-hopper_SizeMatters_728x9
150	s02mdn.net	application/x-shockwave-flash	5441 bytes	B6229987.3;sz=300x250;ord=
152	ad.doubleclick.net	text/html	2481 bytes	xd_proxy.php
220	static.ak.fbcdn.net	text/html	7206 bytes	script66.js?agnc=564334&cr
226	cdn.doubleverify.com	application/x-javascript	2078 bytes	surly.js?;ad_w=728;ad_h=90;c
317	c.betrad.com	application/x-javascript	5 bytes	?adv=570497&cam=272312
330	opt.xmladfeed.com	text/html	43 bytes	sendtracker.aspx?c=1860308
341	mv.bidsystem.com	image/gif	36 kB	300x250_40_tgif_latenight.sw
365	s02mdn.net	application/x-shockwave-flash	0 bytes	service.php?plid=957898&dc
397	www5.filmannex.com	text/html	2206 bytes	1229.js?r=0.24920294309947
404	c.betrad.com	application/x-javascript	43 bytes	p?c1=1&c2=6000004&c5=0
405	b.scorecardresearch.com	image/gif	43 bytes	9-tracking_1x1_white.gif
477	s02mdn.net	image/gif	505 bytes	
509			35 bytes	_utm.gif?utmwv=5.2.6&utm
520	www.google-analytics.com	image/gif		

Save Save All Preview Close Help

we don't know where this load\_small.png file is located in which hostname, so that's why we will save all. We saved all files in a directory and searched for the load\_small.png file and we found that file load\_small.png. It is a star shape.



## FTPS ANALYSIS TRACE FILES: challengeftp1.pcapng challengeftp2.pcapng

**BACKGROUND:** A customer needed a secure file transfer application put in place. These two trace files illustrate the separate options they have tested – implicit FTPS and explicit FTPS.

### QUESTIONS:

- What is the IP address of the server?

Answer: 64.65.53.234

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.4	64.65.53.234	TCP	66	53899 → 990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK... 66 990 → 53899 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=146...
2	0.045900	64.65.53.234	192.168.1.4	TCP	54	53899 → 990 [ACK] Seq=1 Ack=1 Win=17520 Len=0
3	0.046014	192.168.1.4	64.65.53.234	TCP	54	990 → 53899 [ACK] Seq=1 Ack=175 Win=65361 Len=0
4	0.049248	192.168.1.4	64.65.53.234	TLSV1	856	Server Hello, Certificate, Server Hello Done
5	0.184428	64.65.53.234	192.168.1.4	TCP	228	Client Hello
6	0.487262	64.65.53.234	192.168.1.4	TLSV1	54	990 → 53899 [ACK] Seq=1 Ack=175 Win=65361 Len=0
7	0.487262	192.168.1.4	64.65.53.234	TLSV1	102	Client Hello

## 2. Which trace illustrates implicit FTPS?

Answer: challengeftp1.pcapng, implicit FTPS is a secure connection and it runs on port 990

Filter: tcp.stream eq 0							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
18	0.648445000	192.168.1.4	64.65.53.234	TCP	1	/1 53899→				
19	0.694269000	64.65.53.234	192.168.1.4	TCP	107	990→53				
20	0.694785000	192.168.1.4	64.65.53.234	TCP	91	53899→				
21	0.742101000	64.65.53.234	192.168.1.4	TCP	123	990→53				
22	0.747670000	192.168.1.4	64.65.53.234	TCP	251	53899→				
23	0.792366000	64.65.53.234	192.168.1.4	TCP	123	990→53				
24	0.991444000	192.168.1.4	64.65.53.234	TCP	54	53899→				
25	14.493834000	192.168.1.4	64.65.53.234	TCP	139	53899→				
26	14.539410000	64.65.53.234	192.168.1.4	TCP	139	990→53				
27	14.539695000	192.168.1.4	64.65.53.234	TCP	139	53899→				
28	14.584811000	64.65.53.234	192.168.1.4	TCP	123	990→53				
29	14.585185000	192.168.1.4	64.65.53.234	TCP	91	53899→				
30	14.636684000	64.65.53.234	192.168.1.4	TCP	107	990→53				
31	14.636965000	192.168.1.4	64.65.53.234	TCP	219	53899→				
32	14.686012000	64.65.53.234	192.168.1.4	TCP	139	990→53				
33	14.686772000	192.168.1.4	64.65.53.234	TCP	235	53899→				
38	14.782527000	64.65.53.234	192.168.1.4	TCP	107	990→53				
43	14.977911000	192.168.1.4	64.65.53.234	TCP	54	53899→				
48	14.996603000	64.65.53.234	192.168.1.4	TCP	107	990→53				
52	15.197908000	192.168.1.4	64.65.53.234	TCP	54	53899→				

Frame 27: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface  
 Ethernet II, Src: IntelCor\_1f:4f:be (68:5d:43:1f:4f:be), Dst: Netgear\_04:f6:52 (00:  
 Internet Protocol Version 4, Src: 192.168.1.4 (192.168.1.4), Dst: 64.65.53.234 (64.  
 Transmission Control Protocol, Src Port: 53899 (53899), Dst Port: 990 (990), Seq: 1  
 Source Port: 53899 (53899)  
 Destination Port: 990 (990)  
 [Stream index: 0]  
 [TCP Segment Len: 85]  
 Sequence number: 1139 (relative sequence number)  
 [Next sequence number: 1224 (relative sequence number)]  
 Acknowledgment number: 1616 (relative ack number)

## 3. Which trace illustrates explicit FTPS?

Answer: challengeftp2.pcapng (explicit FTPS runs on port 21)

Filter: `tcp.stream eq 0`

No.	Time	Source	Destination	Protocol	Length
1	0.0000000000	192.168.1.4	64.65.53.234	TCP	40
2	0.045176000	64.65.53.234	192.168.1.4	TCP	40
3	0.045772000	192.168.1.4	64.65.53.234	TCP	40
4	0.091103000	64.65.53.234	192.168.1.4	FTP	1460
5	0.091483000	64.65.53.234	192.168.1.4	FTP	1460
6	0.091631000	192.168.1.4	64.65.53.234	TCP	40
7	0.091888000	64.65.53.234	192.168.1.4	FTP	1460
8	0.105869000	192.168.1.4	64.65.53.234	FTP	1460
9	0.380684000	64.65.53.234	192.168.1.4	TCP	40
10	0.565137000	64.65.53.234	192.168.1.4	FTP	1460
11	0.575372000	192.168.1.4	64.65.53.234	FTP	1460
12	0.622489000	64.65.53.234	192.168.1.4	FTP	1460
13	0.656440000	192.168.1.4	64.65.53.234	FTP	1460
14	0.656550000	192.168.1.4	64.65.53.234	FTP	1460
15	0.656611000	102.168.1.4	64.65.53.234	FTP	1460

```

⊕ Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface
⊕ Ethernet II, Src: IntelCor_1f:4f:be (68:5d:43:1f:4f:be), Dst: Netgear_04 (08:00:27:04:00:04)
⊕ Internet Protocol Version 4, Src: 192.168.1.4 (192.168.1.4), Dst: 64.65.53.234 (64.65.53.234)
⊖ Transmission Control Protocol, Src Port: 53809 (53809), Dst Port: 21 (21)
    Source Port: 53809 (53809)
    Destination Port: 21 (21)
        [Stream index: 0]
        [TCP Segment Len: 0]
        Sequence number: 1      (relative sequence number)
        Acknowledgment number: 88   (relative ack number)
        Header Lenath: 20 bytes

```

4.What IP address initiated the data connections in the trace file? Answer: 192.168.1.4

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.4	64.65.53.234	TCP	40	66 53899 → 990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK...
2	0.045900	64.65.53.234	192.168.1.4	TCP	40	66 990 → 53899 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=146...
3	0.046014	192.168.1.4	64.65.53.234	TCP	1460	54 53899 → 990 [ACK1 Seq=1 Ack=1 Win=17520 Len=0]

5.What port numbers are used for the data connection in each trace file?

Answer: 53901-10007

Ethernet: 1	Fibre Channel	FDDI	<b>IPv4: 1</b>	IPv6	IPX	JXTA	NCP	RSVP	SCTP	TCP: 2	Token Ring	UDP	USB	WLAN
TCP Conversations														
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A→B	Bytes A→B	Rel Start	Duration			
192.168.1.4	53809	64.65.53.234	990	37	5 556	20	2 698	17	2 858	0.000000000				
192.168.1.4	53901	64.65.53.234	10007	15	1 907	8	1 142	7	765	14.686988000				

Answer: 53810 – 10004

Ethernet: 1	Fibre Channel	FDDI	<b>IPv4: 1</b>	IPv6	IPX	JXTA	NCP	RSVP	SCTP	TCP: 2	Token Ring	UDP	USB	WLAN
TCP Conversations														
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A→B	Bytes A→B	Rel Start	Duration	b		
192.168.1.4	53809	64.65.53.234	21	41	6 393	21	2 874	20	3 519	0.000000000	4.6711			
192.168.1.4	53810	64.65.53.234	10004	15	2 167	8	950	7	1 217	4.111567000	0.4579			

## OUCH! TRACE FILE: challengeattack.pcapng

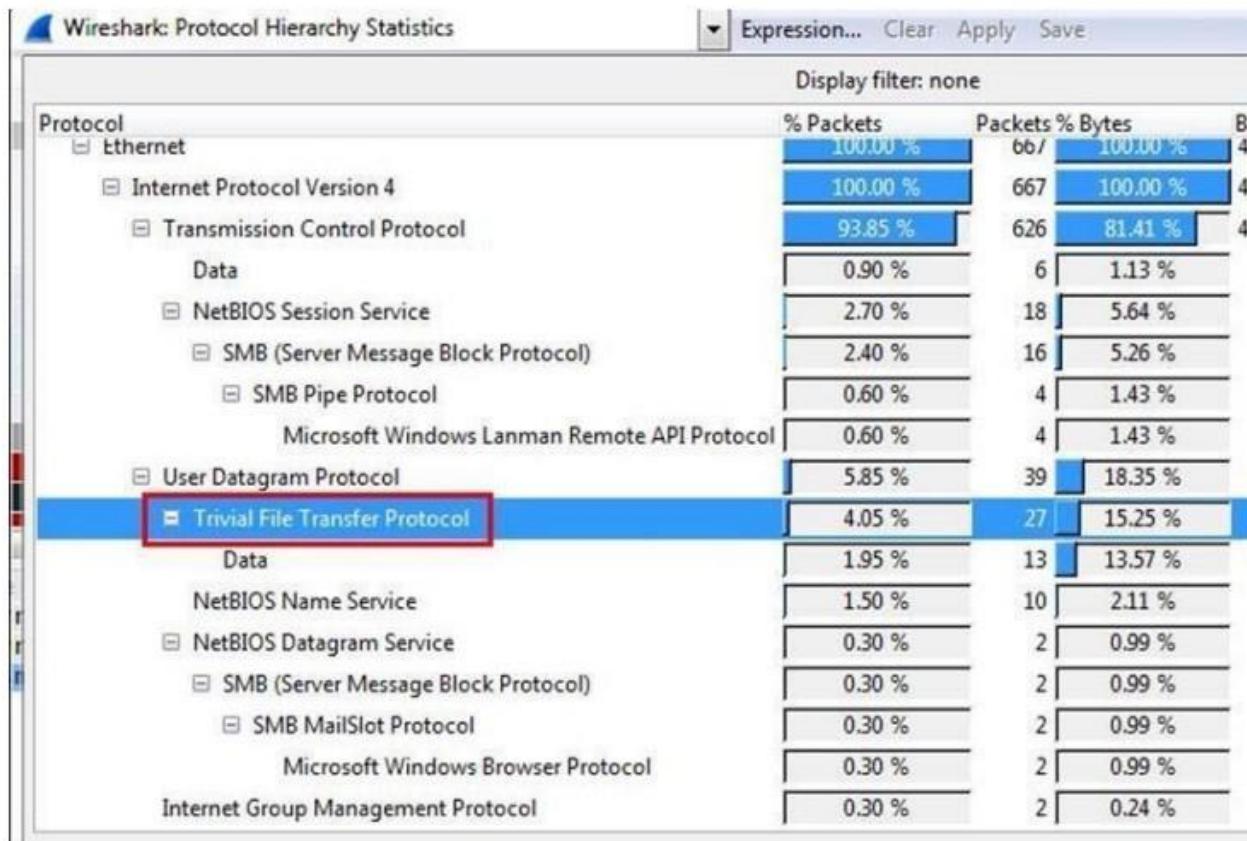
**BACKGROUND:** These capture files were taken from a network that was experiencing a “zero-day” attack and was completely overwhelmed. It is also reported that some of the nodes within the network appear to be unable to update their antivirus/security software. The Network Administrator has given you this file that contains what he considers “suspicious” behavior and has asked you to help. The Administrator can tell you that 141.157.228.12 is a server and that 10.1.1.31 is a client machine.

### QUESTIONS:

- What file transfer application is seen in this trace file?

Ans: Trivial File Transfer Protocol

Go to Statistics and then select Protocol Hierarchy which will show all protocols used in this trace file.



2. What is the IP address of the host that is receiving the file?

Answer: 10.1.1.31

(ip.addr eq 10.1.1.31 and ip.addr eq 141.157.228.12) and (udp.port eq 10)

Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
6 0.502697000	10.1.1.31	141.157.228.12	TFTP	62	Read Request, File: msblast.exe, Transfer type: octet
9 0.616459000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 1
10 0.617895000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 1
16 1.519664000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 2
17 1.523540000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 2
20 2.425865000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 3
21 2.430854000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 3
22 3.332098000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 4
23 3.332752000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 4
24 4.238330000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 5
25 4.244026000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 5
26 5.145458000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 6

3. What is the name of the file that is being transferred?

Answer: mblast.exe

Filter: (ip.addr eq 10.1.1.31 and ip.addr eq 141.157.228.12) and (udp.port eq 10... Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6	0.502697000	10.1.1.31	141.157.228.12	TFTP	62	Read Request, File: msblast.
9	0.616459000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 1
10	0.617895000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 1
16	1.519664000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 2
17	1.523540000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 2
20	2.425865000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 3
21	2.430854000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 3
22	3.332098000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 4
23	3.332752000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 4
24	4.238330000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 5
25	4.244026000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 5
26	5.145458000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 6
27	5.152692000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 6
28	6.050621000	141.157.228.12	10.1.1.31	TFTP	558	Data Packet, Block: 7
29	6.053781000	10.1.1.31	141.157.228.12	TFTP	60	Acknowledgement, Block: 7

```

Frame 6: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: NxpSemic_00:00:02 (00:60:37:00:00:02), Dst: Runtap_17:33:2e (00:03:6d:17:33:2e)
Internet Protocol Version 4, Src: 10.1.1.31 (10.1.1.31), Dst: 141.157.228.12 (141.157.228.12)
User Datagram Protocol, Src Port: 1028 (1028), Dst Port: 69 (69)
Trivial File Transfer Protocol
[Source File: msblast.exe]
Opcode: Read Request (1)
Source File: msblast.exe
Type: octet

```

## DNS TROUBLE TRACE FILE: challengednstrouble.pcapng

**BACKGROUND:** After a maintenance window on the day before, when several servers had been upgraded to a newer operating system, a lot of trouble tickets have come in. Users complain that connecting to web sites and other services takes a long time now, especially when connecting for the first time. A quick check on all relevant switches, routers and servers reveals no bottlenecks in CPU, memory or disk I/O, so of course the tickets are handed over to the network guys – it must be the network, right? Finally, one of the network engineers comes to you and asks you to help him with analyzing a trace he took. He suspects that there is something wrong with the DNS name resolution, but even after filtering away most of the other stuff he can't put his finger on it. Can you take a look at his trace to find out what happened and if this is a network problem at all?

## QUESTIONS:

- What FQDN is the client attempting to resolve?

Answer: flane.de

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.129.1	192.168.129.1	DNS	68	Standard query 0x0004 ANY flane.de
2	0.000934	192.168.129.1	81.209.147.10	DNS	79	Standard query 0x00d4 ANY flane.de OPT
3	1.999844	192.168.129.1	192.168.129.1	DNS	68	Standard query 0x0005 ANY flane.de
4	2.000249	192.168.129.1	81.209.147.10	DNS	79	Standard query 0x00dc ANY flane.de OPT
5	5.759714	192.168.129.1	81.209.147.10	DNS	70	Standard query 0x08e4 NS <Root> OPT
6	5.759941	192.168.129.1	192.58.128.30	DNS	79	Standard query 0x00d4 ANY flane.de OPT
7	5.780298	192.58.128.30	192.168.129.1	DNS	365	Standard query response 0x00d4 ANY flane.de NS f.nic.de NS a.nic.de...
8	5.780723	192.168.129.1	81.91.164.5	DNS	79	Standard query 0x00d4 ANY flane.de OPT
9	5.793700	81.91.164.5	192.168.129.1	DNS	152	Standard query response 0x00d4 ANY flane.de NS ns3.edns.de NS ns4.e...
						70 Standard query response 0x00d4 ANY flane.de OPT
> Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface unknown, id 0						
> Ethernet II, Src: ASUSTekC_dd:87:04 (00:1d:60:dd:87:04), Dst: VMWare_b0:14:46 (00:0c:29:b0:14:46)						
> Internet Protocol Version 4, Src: 192.168.129.127, Dst: 192.168.129.111						
> User Datagram Protocol, Src Port: 60628, Dst Port: 53						
Domain Name System (query)						
Transaction ID: 0x0004						
Flags: 0x0100 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 0						
Queries						
flane.de: type ANY, class IN						
[Response In: 12]						

2. To what IP address is the first recursive DNS query sent? Ans:  
192.168.129.111.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.129.127	192.168.129.111	DNS	68	Standard query 0x0004 ANY flane.de

3. To what IP address is the second recursive DNS query sent?  
Answer: 81.209.147.10

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.129.127	192.168.129.111	DNS	68	Standard query 0x0004 ANY flane.de
2	0.000934	192.168.129.111	81.209.147.10	DNS	79	Standard query 0x00d4 ANY flane.de OPT
3	1.999844	192.168.129.127	192.168.129.111	DNS	68	Standard query 0x0005 ANY flane.de

4. The trace file includes authoritative DNS servers responsible for what top level country code domain?  
Answer: .de is the country code top-level domain (ccTLD) for Federal Republic of Germany

5. What is the IP address of the host that is responsible for the longdelay in resolving the host name?  
Answer: 81.209.147.10

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	192.168.129.127	192.168.129.111	DNS	68 Standard query 0x0004 ANY flane.de
2	0.000934	192.168.129.111	81.209.147.10	DNS	79 Standard query 0x00d4 ANY flane.de OPT
3	1.999844	192.168.129.127	192.168.129.111	DNS	68 Standard query 0x0005 ANY flane.de
4	2.000249	192.168.129.111	81.209.147.10	DNS	79 Standard query 0x00dc ANY flane.de OPT
5	5.759714	192.168.129.111	81.209.147.10	DNS	70 Standard query 0x08e4 NS <Root> OPT
6	5.759941	192.168.129.111	192.58.128.30	DNS	79 Standard query 0x00d4 ANY flane.de OPT
7	5.760298	192.58.128.30	192.168.129.111	DNS	365 Standard query resonance AvAard ANY flane.de NS f nic de NS

Frame 5: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface unknown, id 0

- > Interface id: 0 (unknown)
- Encapsulation type: Ethernet (1)
- Arrival Time: May 20, 2010 19:09:24.212303000 India Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1274362764.212303000 seconds
- [Time delta from previous captured frame: 3.759465000 seconds]
- [Time delta from previous displayed frame: 3.759465000 seconds]
- [Time since reference or first frame: 5.759714000 seconds]

## VOIP RECONSTRUCTION TRACE FILES: challengevoip.pcapng

**BACKGROUND:** This captured file was collected from a recently installed VoIP network that is experiencing performance issues, and you have been asked to evaluate it and recommend corrective action.

### QUESTIONS:

1. What three UDP-based protocols are used for the VoIP call and call setup?

Answer: SIP, SDP, RTP, SNMP

No.	Time	Source	Destination	Protocol	Length Info
674	97.607016	45.210.3.90	45.210.9.72	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x8B43C394, Seq=26591, Time=25345376
675	97.611725	45.210.9.72	45.210.3.90	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x13C443D3, Seq=50558, Time=3881548510
5	4.774235	45.210.3.36	45.210.3.90	SIP	390 Status: 100 Trying
6	4.855833	45.210.3.36	45.210.3.90	SIP	556 Status: 180 Ringing
11	6.583414	45.210.3.90	45.210.3.36	SIP	603 Request: ACK sip:3290.a75613a9-1f059de1-3fd92a8b-e19da4a3@45.210.3...
102	66.778897	45.210.3.36	45.210.3.90	SIP	390 Status: 100 Trying
104	66.859774	45.210.3.36	45.210.3.90	SIP	569 Status: 480 Temporarily Not Available
105	66.942727	45.210.3.90	45.210.3.36	SIP	485 Request: ACK sip:3359@cisco.sip.ilabs.interop.net;user=phone
121	86.458796	45.210.3.36	45.210.3.90	SIP	390 Status: 100 Trying
122	86.762663	45.210.3.36	45.210.3.90	SIP	595 Status: 180 Ringing
127	92.458920	45.210.3.90	45.210.3.36	SIP	602 Request: ACK sip:3290.66d68faf-95104543-61546e25-b5e195de@45.210.3...
4	4.774199	45.210.3.90	45.210.3.36	SIP/SDP	824 Request: INVITE sip:4697@cisco.sip.ilabs.interop.net;user=phone
10	6.430493	45.210.3.36	45.210.3.90	SIP/SDP	10..Status: 200 OK
101	66.778283	45.210.3.90	45.210.3.36	SIP/SDP	824 Request: INVITE sip:3359@cisco.sip.ilabs.interop.net;user=phone
120	86.458126	45.210.3.90	45.210.3.36	SIP/SDP	822 Request: INVITE sip:4672@cisco.sip.ilabs.interop.net;user=phone
126	92.296389	45.210.3.36	45.210.3.90	SIP/SDP	10..Status: 200 OK
106	67.656393	45.210.3.131	10.4.58.28	SNMP	119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6...
111	72.954996	45.210.3.131	10.4.58.28	SNMP	119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6...

2. With what three IP addresses is 45.210.3.90 communicating?

Answer: 45.210.3.36, 45.210.3.97, 45.210.3.72

Wireshark · Conversations · challengevoip.pcapng

Ethernet · 13	IPv4 · 8	IPv6	TCP · 1	UDP · 14	
Address A	Address B		Packets	Bytes	Packets A
10.4.58.28	45.210.3.131		3	357	
10.4.58.29	45.210.3.131		2	238	
45.210.3.36	45.210.3.90		14	9216	
45.210.3.90	45.210.9.97		89	19k	
45.210.3.90	45.210.9.72		544	116k	
45.210.3.131	224.1.0.38		1	60	
45.210.3.131	216.155.193.184		2	153	
45.210.3.252	224.0.0.1		1	60	

3.What SIP error code is seen in this trace file?

Answer: Error code 480

No.	Time	Source	Destination	Protocol	Length	Info
5	4.774235	45.210.3.36	45.210.3.90	SIP	390	Status: 100 Trying
6	4.855833	45.210.3.36	45.210.3.90	SIP	556	Status: 180 Ringing
11	6.583414	45.210.3.90	45.210.3.36	SIP	603	Request: ACK sip:3290.a75613a9-1f059de1-3fd92a8b-e19da4a3@45.210.3...
102	66.778897	45.210.3.36	45.210.3.90	SIP	390	Status: 100 Trying
104	66.859774	45.210.3.36	45.210.3.90	SIP	569	Status: 480 Temporarily Not Available

4.What is the stated cause of this SIP error? Ans:

“Endpoint not registered”.

challengevoip.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
No.	Time	Source	Destination	Protocol	Length	Info
5	4.774235	45.210.3.36	45.210.3.90	SIP	390	Status: 100 Trying
6	4.855833	45.210.3.36	45.210.3.90	SIP	556	Status: 180 Ringing
11	6.583414	45.210.3.90	45.210.3.36	SIP	603	Request: ACK sip:3290.a75613a9-1f059de1-3fd92a8b-e19da4a3@45.210.3...
102	66.778897	45.210.3.36	45.210.3.90	SIP	390	Status: 100 Trying
104	66.859774	45.210.3.36	45.210.3.90	SIP	569	Status: 480 Temporarily Not Available

```

> Frame 104: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface unknown, id 0
> Ethernet II, Src: IBM_6:f:c:e9 (00:09:6b:6f:fc:e9), Dst: Cisco_c3:43:8b (00:30:94:c3:43:8b)
> Internet Protocol Version 4, Src: 45.210.3.36, Dst: 45.210.3.90
> User Datagram Protocol, Src Port: 59689, Dst Port: 5060
> Session Initiation Protocol (480)
  > Status-Line: SIP/2.0 480 Temporarily Not Available
    Status-Code: 480
      [Resent Packet: False]
  > Message Header
    > Via: SIP/2.0/UDP 45.210.3.90:5060;received=45.210.3.90;bran...
      Server: 3Com-SIPProxy/03.00.141.000
      From: "Cisco 3290" <sip:3290@cisco.sip.labns.interop.net>;tag=003094c3438b00ce58bfe683-6aea8095
      To: <sip:3359@cisco.sip.labns.interop.net;user=phone>;tag=80a3dff-75a3-d811-9f06-0003ba43cf93
      Call-ID: 003094c3-438b0084-3eb5412c-759958df@45.210.3.90
      [Generated Call-ID: 003094c3-438b0084-3eb5412c-759958df@45.210.3.90]
      CSeq: 101 INVITE
      Warning: 399 45.210.3.12 "Endpoint not registered"
      Content-Length: 0
      Contact: <sip:45.210.3.12>
  
```

**BOY SCOUT TRACE FILES: challengeboyscout.pcapng**

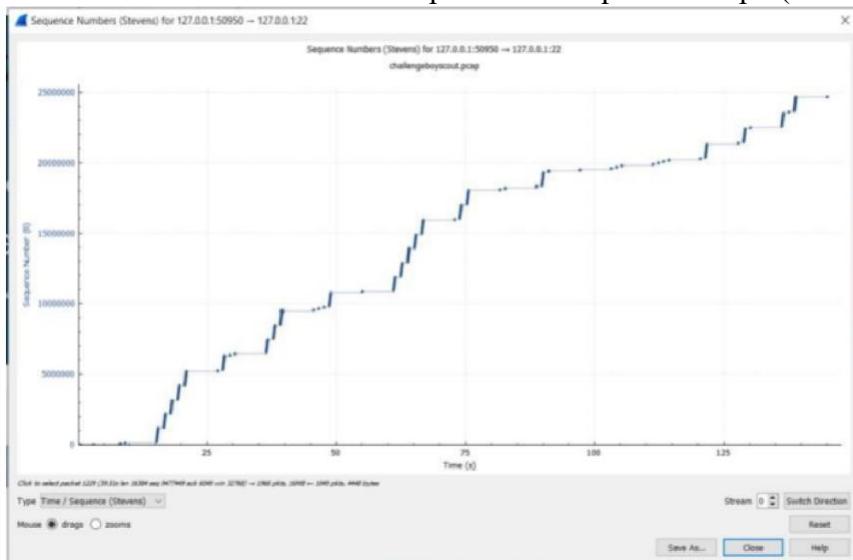
BACKGROUND: Information leaks from all sorts of place

## QUESTIONS:

1. What is the secret message? Answer:

## eei0love0wiresharke Analysis:

Select Statistics > TCP StreamGraph > TCP Sequence Graph (Stevens).



For decoding the Morse code, we used an online Morse code decoder.

## Convert morse code to text

Input data	<pre>.... -... .-.. -... - .- -.- .-.. -.-. -.- -.-</pre>
Convert	morse_code to text
Output:	eei0love0wiresharke

## **CONCLUSION:**

Thus from this experiment we used Wireshark to analyze the protocol used and frames of each protocol, applied filters to find out the information being send, downloaded files that are sent as HTTP Objects to check its content, decoded secret messages and other challenges

