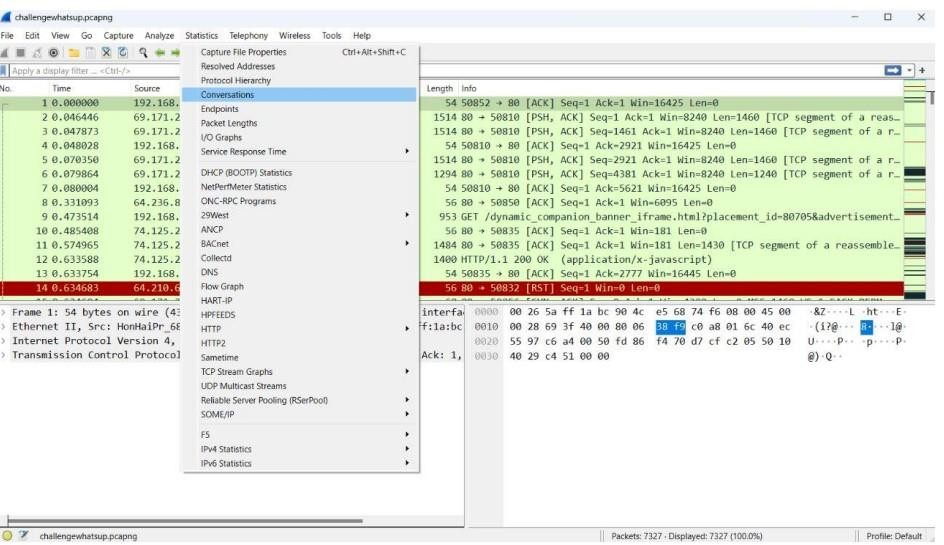
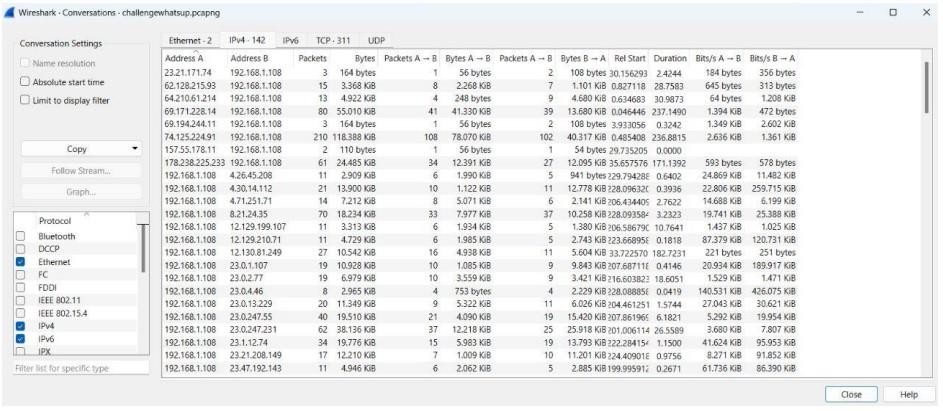
# Cursed

1. 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

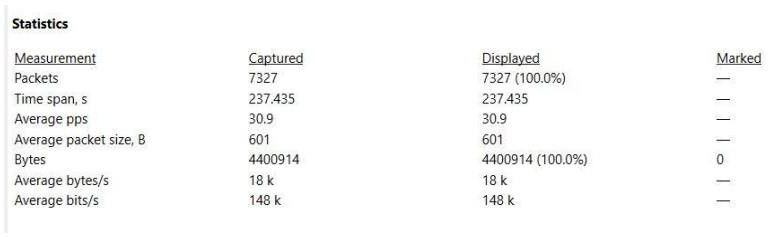


Then we can select the Ipv4 tab and see the count is 142 which means that there are 142 Ips communicating with Scott’s machine.



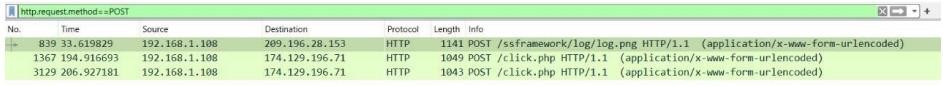
1. What is the average packets per second rate seen in this trace file? Answer: 30.9

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



1. 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

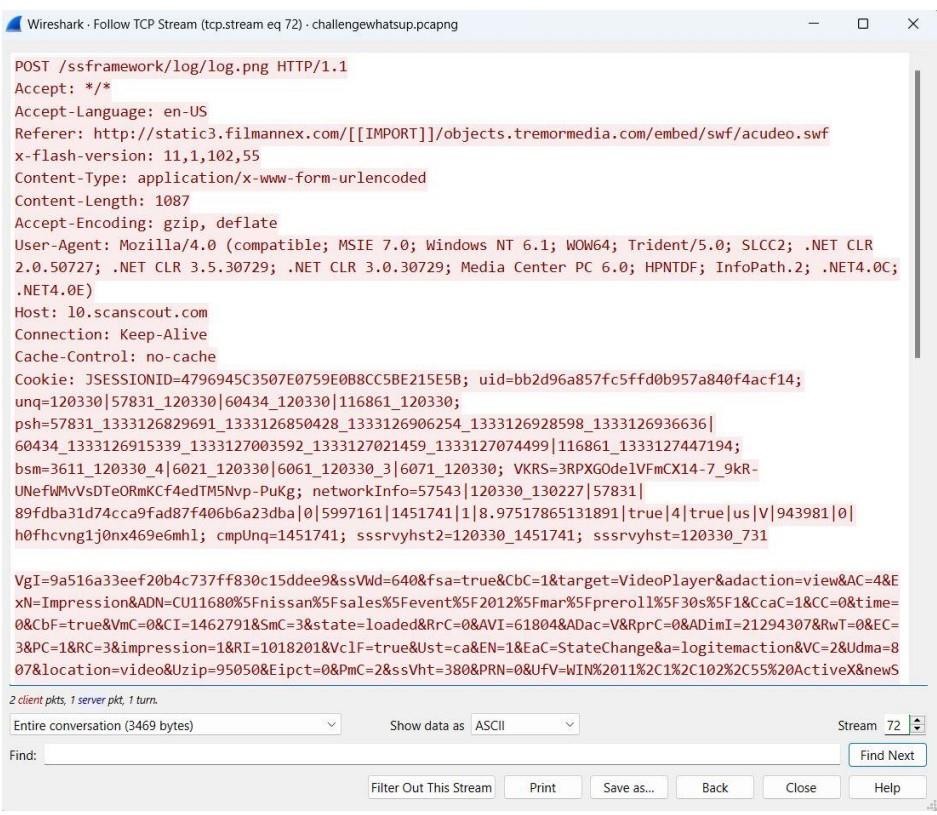


1. What location information is contained in the POST toscanscout.com? Answer: San Francisco – Oakland – San Jose

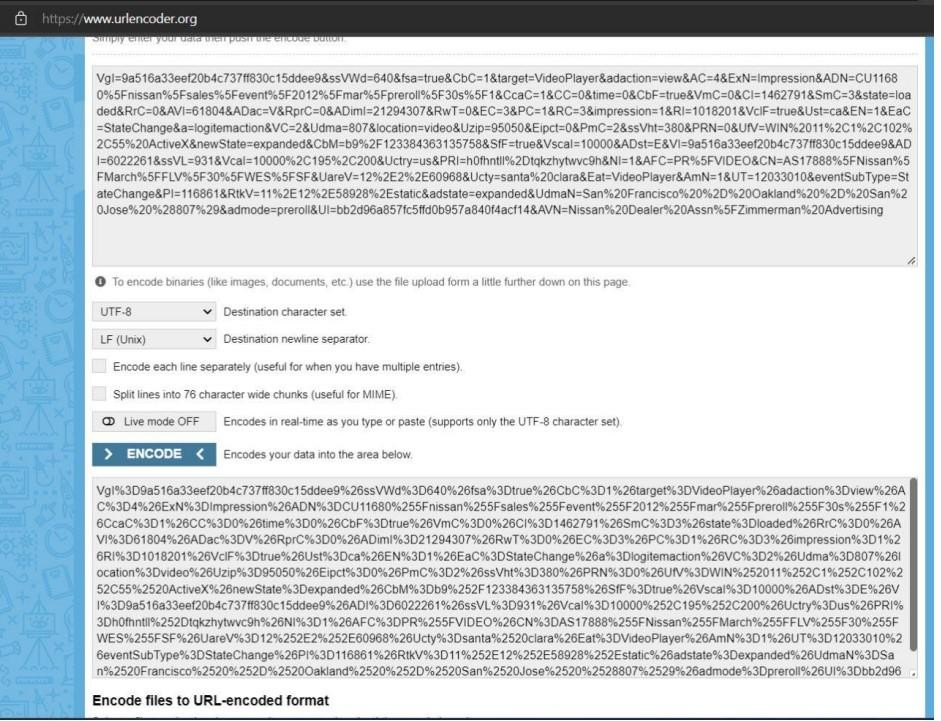
First find the POST request, and there are only three of them, and next we have to find which request header contains the scanscout.com. We checked out all three requests and found one of the request headers is for scanscout.com.



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



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.



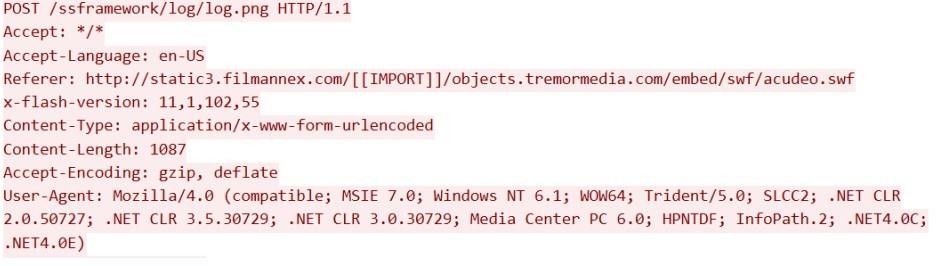
Now we can see in the below figure that the parameter Udam has its value San Francisco

– Oakland – San Jose.

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

Answer: Internet Explorer 9

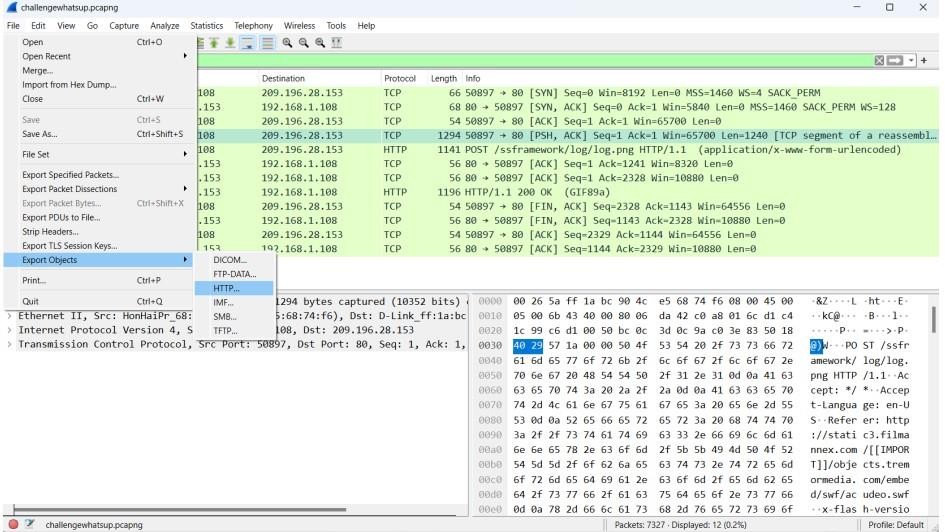
It can be done by analyzing the User-Agent string of any GET/POST request

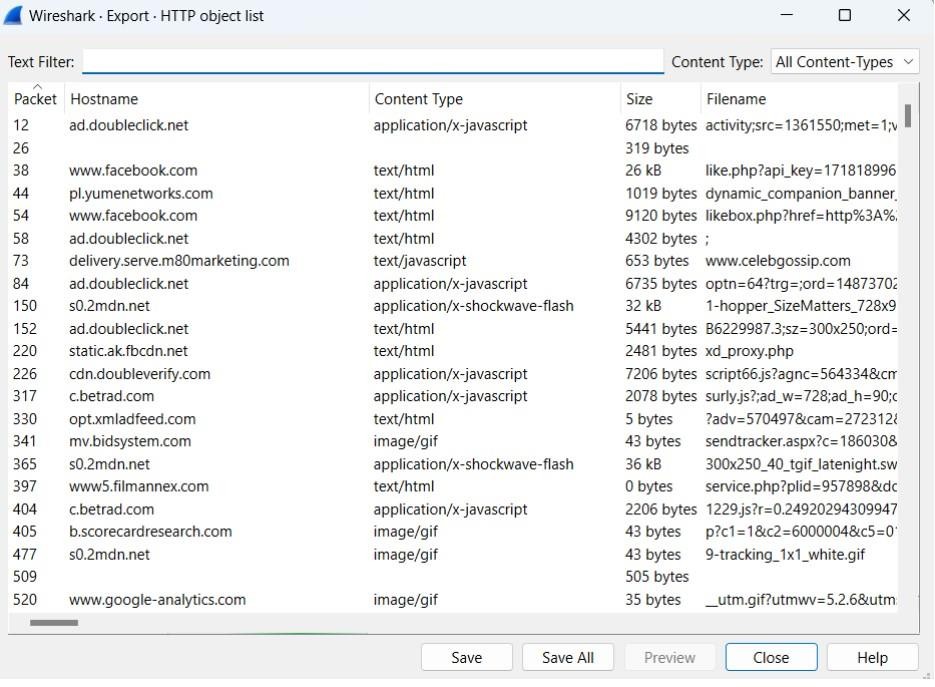


## Find,export and reassemble load\_small.png. what shape is in the image?

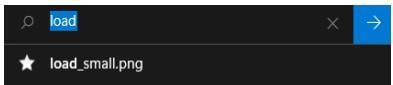
Answer: Star

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





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.

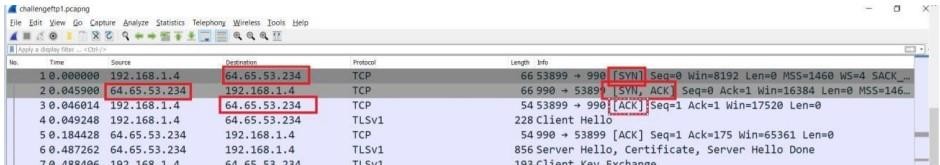


**FTPS ANALYSIS TRACE FILES: challengeftp1.pcapng challengeftp2.pcapng BACKGROUND:** A customer needed a secure file transfer application put in place.

These two trace files illustrate the separate options they have tested – implicit FTPS and explicit FTPS.

## QUESTIONS:

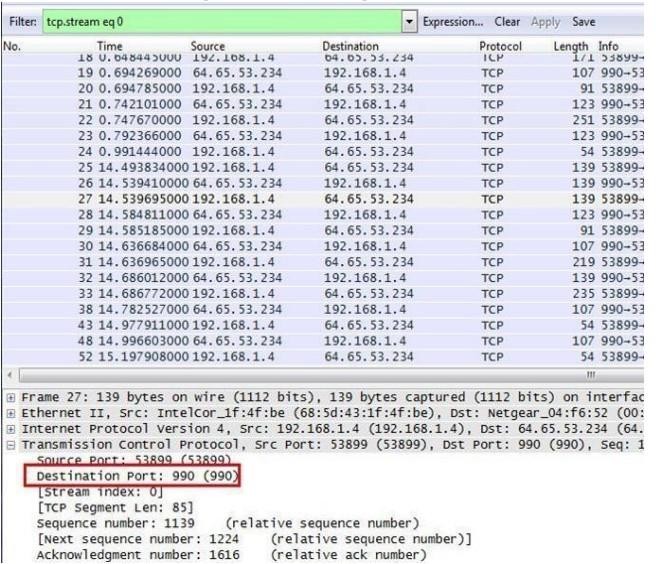
1. What is the IP address of the server? Answer: 64.65.53.234



1. Which trace illustrates implicit FTPS?

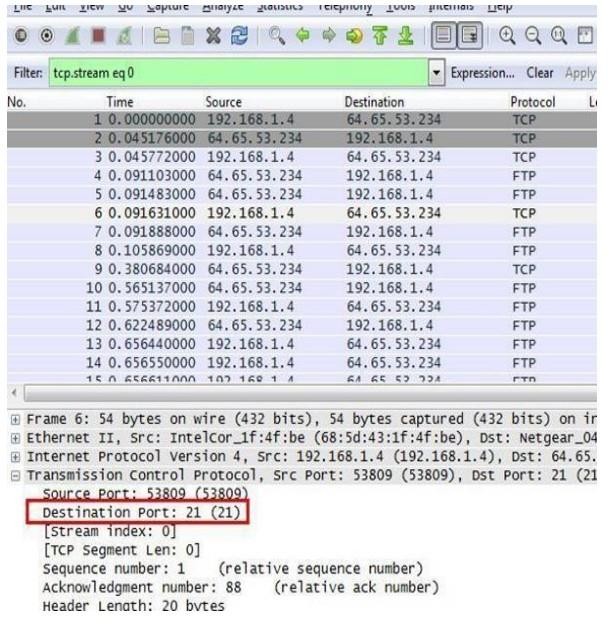
Answer: challengeftp1.pcapng, implicit FTPS is a secure connection and it runs on port

990



1. Which trace illustrates explicit FTPS?

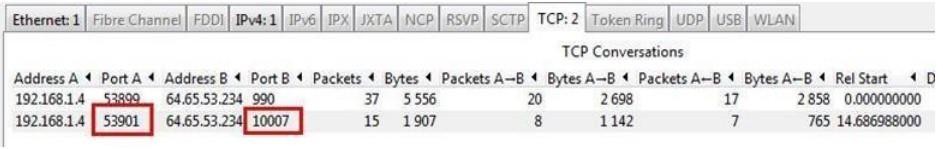
Answer: challengeftp2.pcapng (explicit FTPS runs on port 21)



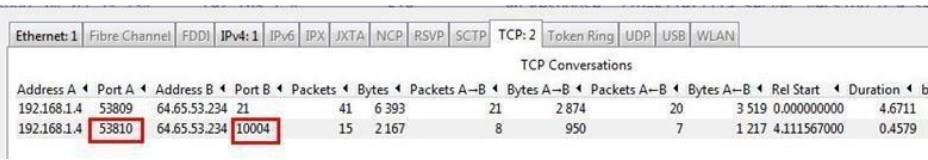
1. What IP address initiated the data connections in the trace file? Answer: 192.168.1.4



1. What port numbers are used for the data connection in each trace file? Answer: 53901-10007



Answer: 53810 – 10004



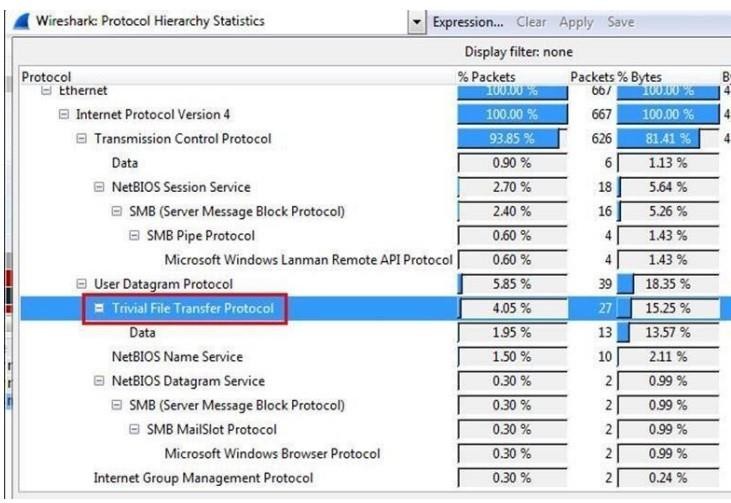
## OUCH! TRACE FILE: challengeattack.pcapng

**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.

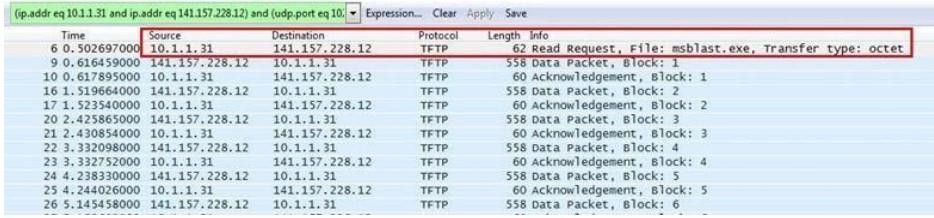
## QUESTIONS:

1. What file transfer application is seen in this trace file? Ans: Trivial File Transfer Protocol

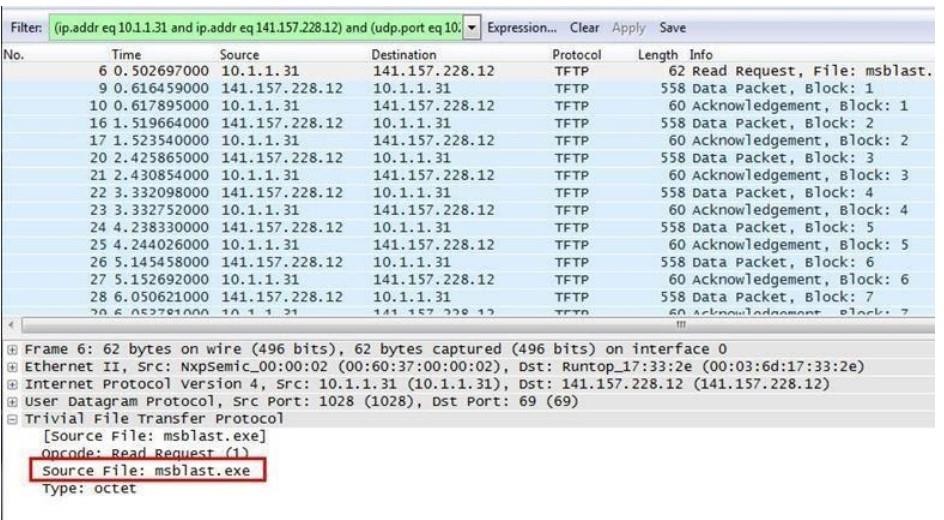
Go to Statistics and then select Protocol Hierarchy which will show all protocols used in this trace file.



1. What is the IP address of the host that is receiving the file? Answer: 10.1.1.31



1. What is the name of the file that is being transferred? Answer: mblast.exe



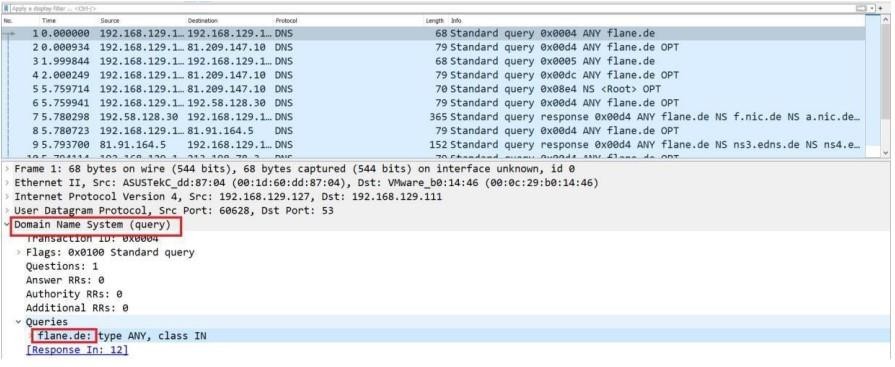
## DNS TROUBLE TRACE FILE: challengednstrouble.pcapng

**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:

1. What FQDN is the client attempting to resolve? Answer: flane.de



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



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

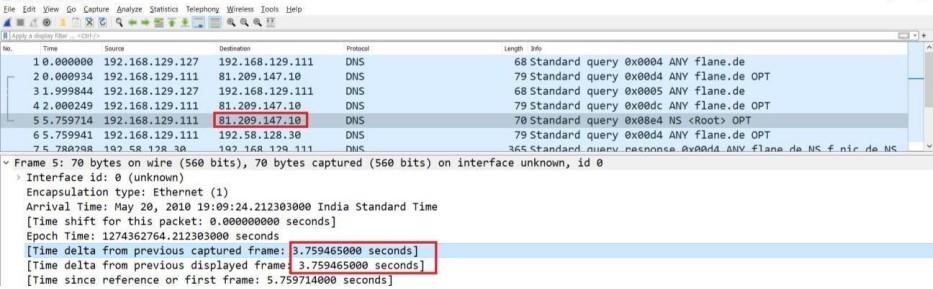


1. The trace file includes authoritative DNS servers responsible for whattop level country code domain?

Answer: .de is the country code top-level domain (ccTLD) for Federal Republic of Germany

1. What is the IP address of the host that is responsible for the longdelay in resolving the host name?

Answer: 81.209.147.10

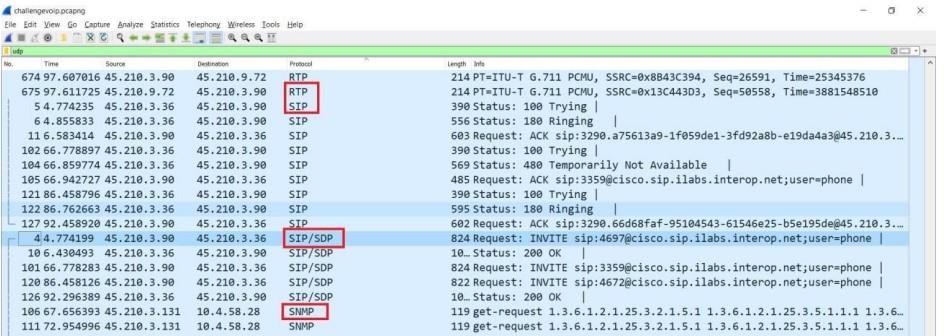


## VOIP RECONSTRUCTION TRACE FILES: challengevoip.pcapng

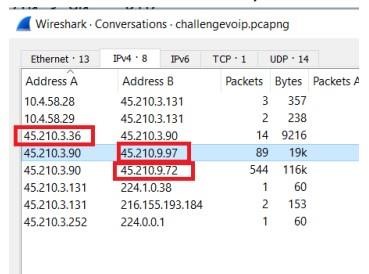
**BACKGROUND:** This captured file was collected from a recently installed VoIP network that is experiencing performance issues, and you have been asked to evaluate it and recommend corrective action.

## QUESTIONS:

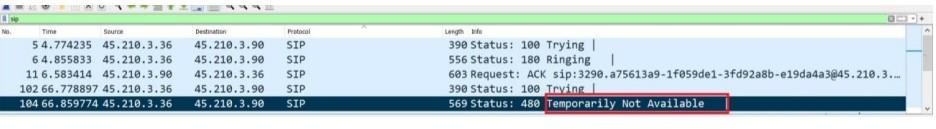
1. What three UDP-based protocols are used for the VoIP call and call setup? Answer: SIP, SDP, RTP, SNMP



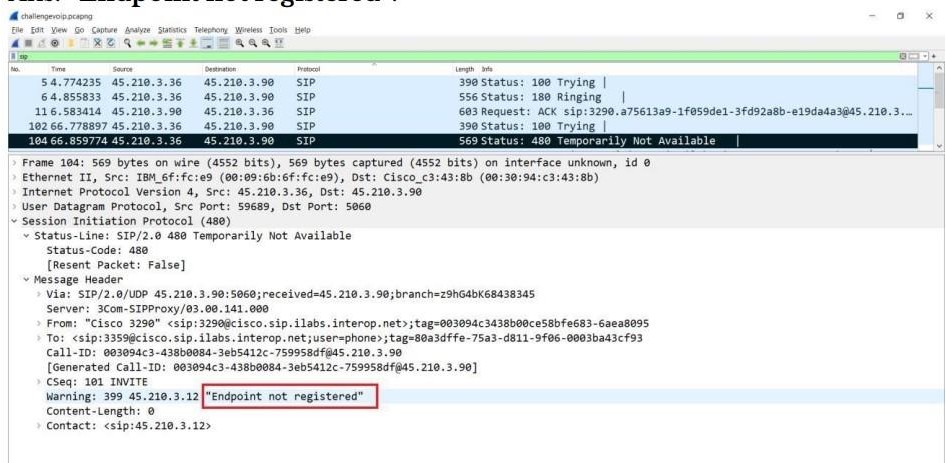
1. With what three IP addresses is 45.210.3.90 communicating? Answer: 45.210.3.36, 45.210.3.97, 45.210.3.72



1. What SIP error code is seen in this trace file? Answer: Error code 480



1. What is the stated cause of this SIP error? Ans: “Endpoint not registered”.



## BOY SCOUT TRACE FILES: challengeboyscout.pcapng

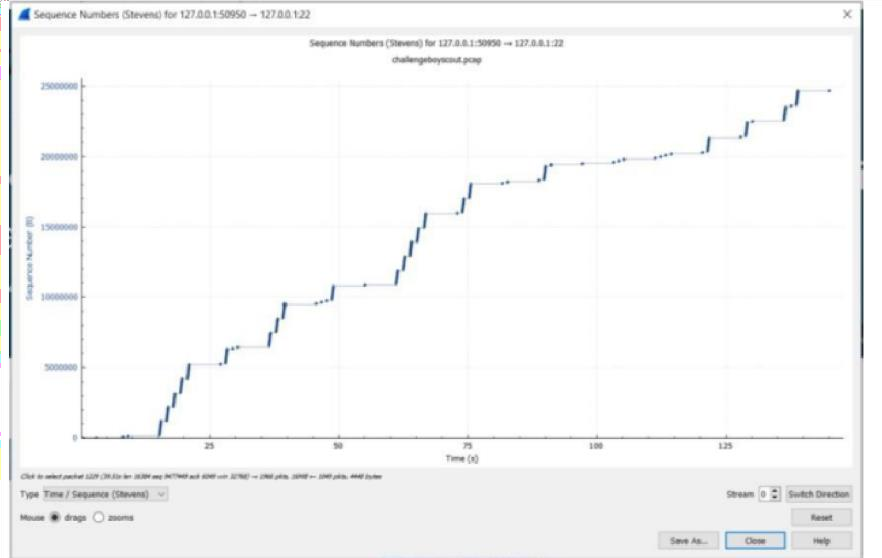
BACKGROUND: Information leaks from all sorts of place

# 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.



# 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