# Objective 11 Customer Complaint Analysis

At last, a Wireshark challenge! It is always good to dissect some network traffic.

|  |  |
| --- | --- |
| Graphical user interface  Description automatically generated with medium confidence | <https://downloads.holidayhackchallenge.com/2021/jackfrosttower-network.zip> |

Of course, we need to visit Tinsel Upatree in the kitchen to help with her terminal.

|  |  |
| --- | --- |
| Graphical user interface, application  Description automatically generated | Text  Description automatically generated |

## Terminal Strace Ltrace Retrace

This terminal demonstrates the command line tool ltrace and how it can be used. In this case we need to defeat the simple registration method in Tinsel’s make\_the\_candy app.

Text

Description automatically generated

Text

Description automatically generated

### Step 1 question Try ltrace

Run the app though ltrace.

### Step 1 answer

It wants a file.  
A screenshot of a computer

Description automatically generated with medium confidence

### Step 2 question: Give it a file

It tried to open the file registration.json, so create one. The command touch is good for that.

### Step 2 answer

It says “Unregistered. Maybe it wants “Registered” to be in the file.  
Text

Description automatically generated

### Step 3 question: Make it registered

You can use echo > to put Registered in the file.

### Step 3 answer

Now it wants Registered (new line) Registration”  
Text

Description automatically generated

### Step 4 question: Ok, add Registration to the end

We can append to the file, instead of overwrite, with >>

### Step 4 answer

Now it wants to see Registered (new line) Registration followed by “:”  
Text

Description automatically generated

### Step 5 question: Ok, add a colon

Stuck using nano or vim now.

### Step 5 answer

Now it wants to see “True”.  
Text

Description automatically generated

### Step 6 question: Will True make you happy?

Add True using nano or vim.

### Step 6 answer

Now it is happy.  
Text

Description automatically generated

## Hints from Terminal Ltrace Strace Retrace

Tom Liston has a talk for us about RFC 3514 Compliant Testing.  
Graphical user interface

Description automatically generated with low confidence

<http://www.youtube.com/watch?v=ermEx0UvcqY>

Tinsel mentions RFC 3514, so maybe it would be wise to attend the talk as well.  
<https://datatracker.ietf.org/doc/html/rfc3514>

|  |  |
| --- | --- |
| Graphical user interface  Description automatically generated with medium confidence  <https://datatracker.ietf.org/doc/html/rfc3514>  Text  Description automatically generated with medium confidence  <https://wiki.wireshark.org/DisplayFilters> | Text  Description automatically generated |

## Objective 11 Customer Complaint Analysis

### Step 1 Question: RFC 3514?

What is all this talk of RFC 3514 about? See if you can figure that out from the talk and the RFC.

### Step 1 Answer

Every April Fools’ Day, April 1, people submit RFCs as jokes. There have been some especially good ones, IP on Avian Carriers (RFC 1149, 2549) and this one about the evil bit. The reserved bit in the IP flags is designated as the evil bit and set to one for evil traffic. If the bad guys would follow the RFC, we wouldn’t need NextGen Firewalls; everything with the evil bit set could be blocked.

### Step 2 Question: Who is non-compliant?

The trolls in Jack Frost Tower are proud that they are evil, so they set the evil bit on all their traffic. Humans have attached to the Tower network with a non-compliant host that does not set the evil bit. Find their traffic in this file, <https://downloads.holidayhackchallenge.com/2021/jackfrosttower-network.zip>

### Step 2 Answer

The hints have given us the flag to search for, ip.flags.rb (reserved bit—Wireshark needs to update that to evil bit) so this one is easy.

A screenshot of a computer

Description automatically generated

Find the POST in the traffic and select Follow HTTP Stream.  
Graphical user interface, application

Description automatically generated

Here is the human complaint.  
Graphical user interface, text, application

Description automatically generated

Now you can select key words from the human complaint and search the troll comments (ip.flags.rb == 1) for the key words.

### Step 3 question: Who complained?

Search the troll traffic and see if you can find three troll complaints that have the same keyword. One way is to set your display filter for the reserved bit, HTTP POST, and contains “keyword”

### Step 3 answer

This is a good display filter, with the keyword “insult”.  
ip.flags.rb == 1 && http.request.method == POST && http contains "insult"

It returns three complaints, which were submitted by Yaqh, Flud, and Hagg. Submit that to your badge as Flud Yaqh Hagg.  
Graphical user interface, table

Description automatically generated with medium confidence

If you want to read all the complaints use this tshark command from the terminal.  
tshark -r jackfrosttower-network.pcap -Y 'ip.flags.rb == 1 && http.request.method==POST' -T fields -e 'http.file\_data'

The complaints are funny, so it is worth your time.