

# KringleCon 4: Calling Birds!

---

## 11) Customer Complaint Analysis

1. Click **Map** (Destinations) icon and then click FrostFest **Talks Lobby**
2. Click to talk to **Pat Tronizer**

Hrmph. Oh hey, I'm Pat Tronizer.

I'm SO glad to have all these first-rate talks here.

We issued a Call for Talks, but only one person responded... We put him in track 1.

But Jack came up with an ingenious way to borrow additional talks for FrostFest! You can hardly tell where we got these great speakers!

Anyway, I cannot believe an actual human connected to the Tower network. It's supposed to be the domain of us trolls and of course Jack Frost himself.

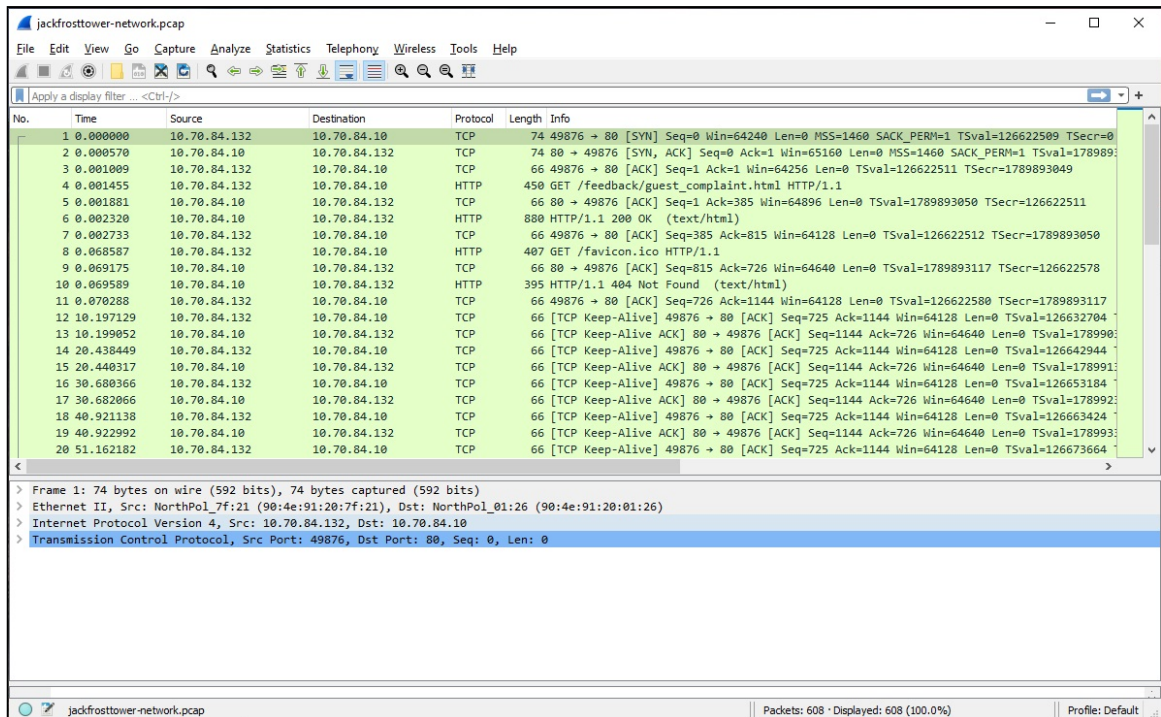
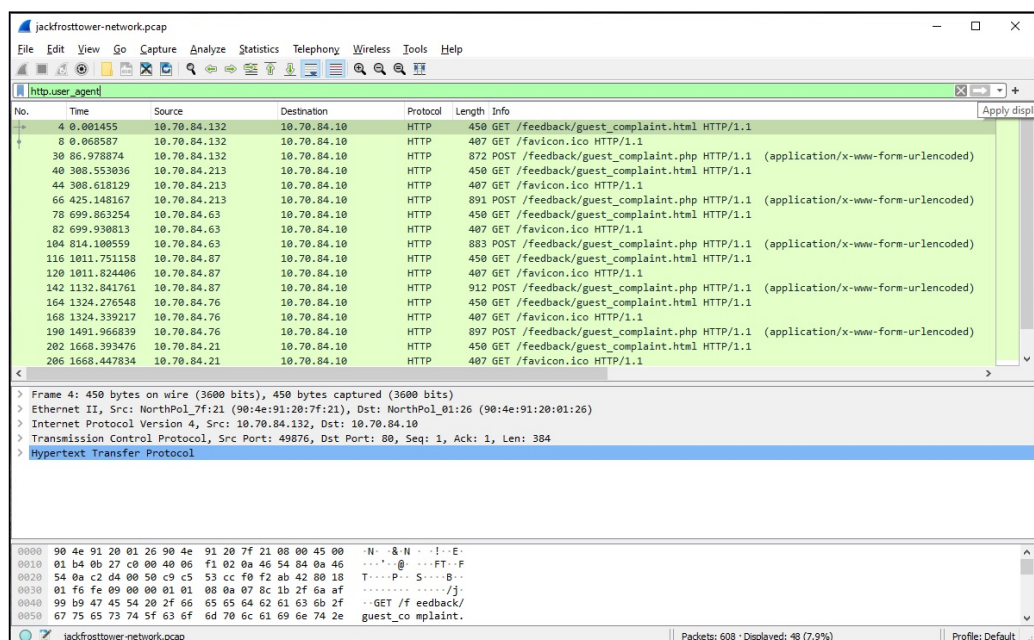
Mr. Frost has a strict policy: all devices must be RFC3514 compliant. It fits in with our nefarious plans.

Some human had the nerve to use our complaint website to submit a complaint!

That website is for trolls to complain about guests, NOT the other way around.

Humans have some nerve.

3. Download the **jackfrostdtower-network.zip** file
4. Unzip the **jackfrostdtower-network.zip** file
5. Start **Wireshark**

7. Open the `jackfrosttower-network.pcap` file8. Type `http.user_agent` into the Apply a display filter text-box9. Click the **Apply display filter** button10. Expand the **Hypertext Transfer Protocol** branch in the Packet Details window

FrostyFox is the first User-Agent string in the packet capture file

11. Type `http.request.method == "POST"` and `not(http contains "FrostyFox")` into the Apply a display filter text-box
12. Click the **Apply display filter** button

```
> Frame 384: 1025 bytes on wire (8200 bits), 1025 bytes captured (8200 bits)
> Ethernet II, Src: Dell_14:9e:21 (00:12:3f:14:9e:21), Dst: NorthPol_01:26 (90:4e:91:20:01:26)
> Internet Protocol Version 4, Src: 10.70.84.251, Dst: 10.70.84.10
> Transmission Control Protocol, Src Port: 36676, Dst Port: 80, Seq: 1, Ack: 1, Len: 959
> Hypertext Transfer Protocol
  > POST /feedback/guest_complaint.php HTTP/1.1\r\n
    Host: frost-tower.local\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/18.17763\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
```

13. Scroll **Down** the Packet Details window
14. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** branch in the Packet Details window
15. Scroll **Down** the window

```
[HTTP request 1/1]
[Response in frame: 386]
File Data: 353 bytes
> HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "name" = "Muffy VonDuchess Sebastian"
  > Form item: "troll_id" = "I don't know. There were several of them."
  > Form item: "guest_info" = "Room 1024"
  > Form item: "description" = "I have never, in my life, been in a facility with such a horrible staff. They are rude and insulting. What kind of place is this? You"
  > Form item: "submit" = "Submit"
```

Guest info for Human is **Room 1024**

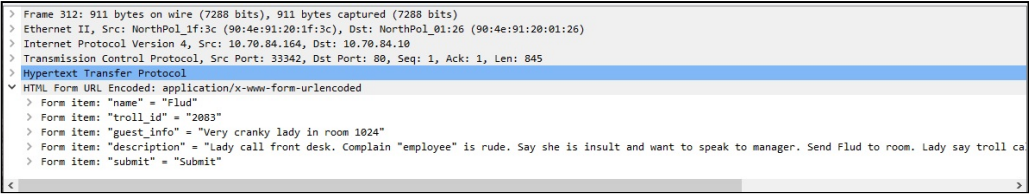
16. Type `http contains "1024"` && `http contains "FrostyFox"` into the Apply a display filter text-box
17. Click the **Apply display filter** button

18. Close the **Hypertext Transfer Protocol** branch in the Packet Details window

```
> Frame 348: 883 bytes on wire (7064 bits), 883 bytes captured (7064 bits)
> Ethernet II, Src: NorthPol_28:2d (90:4e:91:20:28:2d), Dst: NorthPol_01:26 (90:4e:91:20:01:26)
> Internet Protocol Version 4, Src: 10.70.84.106, Dst: 10.70.84.10
> Transmission Control Protocol, Src Port: 40630, Dst Port: 80, Seq: 1, Ack: 1, Len: 817
> Hypertext Transfer Protocol
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "name" = "Hagg"
    > Form item: "troll_id" = "2013"
    > Form item: "guest_info" = "Incredibly angry lady in room 1024"
    > Form item: "description" = "Lady call front desk. I am walk by so I pick up phone. She is ANGRY and shout at me. Say she has never been so insult. I say she probab"
    > Form item: "submit" = "Submit"
```

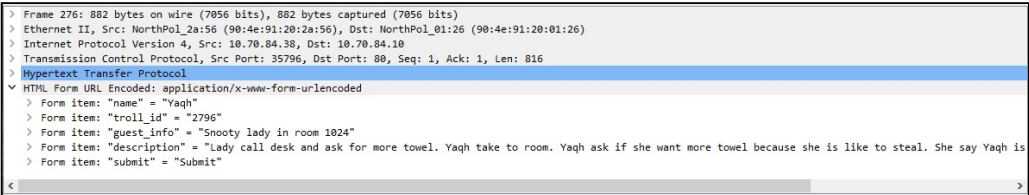
First troll **Hagg**

19. Click packet 312 in the Packet List window



Second troll **Flud**

20. Click packet 276 in the Packet List window

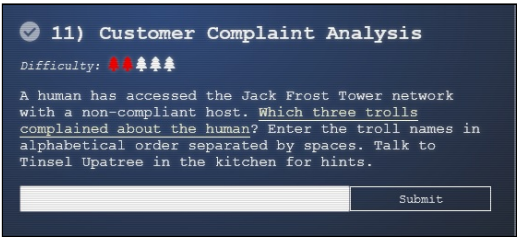


Last troll **Yaqh**

21. Close **Wireshark**

22. Click **Tick** (Objectives) icon

23. Click **11) Customer Complaint Analysis**



24. Type **Flud Hagg Yaqh**

25. Click the **Submit** button

