

https://docs.google.com/document/d/17vU134ZfKiiE-DgiynrO0MySo4_VCGCpw2YJV_Kp3Pk/edit

	Protocol	Length	Info
4192...	DNS	155	Standard query 0xaafe A 43616e64792043616e652053657269616c204e756d6265722038343931.holidaythief.com
4192...	DNS	155	Standard query 0x3b9a AAAA 43616e64792043616e652053657269616c204e756d6265722038343931.holidaythief.com
	DNS	135	Standard query 0x3b9a AAAA 43616e64792043616e652053657269616c204e756d6265722038343931.holidaythief.com
	DNS	135	Standard query 0xaafe A 43616e64792043616e652053657269616c204e756d6265722038343931.holidaythief.com
4192...	DNS	229	Standard query response 0x3b9a No such name AAAA 43616e64792043616e652053657269616c204e756d6265722038343931.hol
4192...	DNS	229	Standard query response 0xaafe No such name A 43616e64792043616e652053657269616c204e756d6265722038343931.holida
4192...	DNS	90	Standard query 0x52e3 A google.com
	DNS	70	Standard query 0xa630 A google.com
	DNS	209	Standard query response 0xaafe No such name A 43616e64792043616e652053657269616c204e756d6265722038343931.holida
	DNS	209	Standard query response 0x3b9a No such name AAAA 43616e64792043616e652053657269616c204e756d6265722038343931.hol
4192...	DNS	106	Standard query response 0x52e3 A google.com A 172.217.11.14
	DNS	86	Standard query response 0xa630 A google.com A 172.217.12.142
4192...	DNS	97	Standard query 0xad3e A sb-ssl.google.com
4192...	DNS	97	Standard query 0x3ab0 AAAA sb-ssl.google.com
4192...	DNS	97	Standard query 0xb5be A wpad.nycap.rr.com

1. What data was exfiltrated via DNS?

- Download the capture file and open in Wireshark
- Filter the packets by searching for DNS
- Examining the DNS queries, they have a long string, appended with .holidaythief.com
- Taking that hex string and converting it to a text string:

Hex to String (Hex to Text) ☆

Enter the hexadecimal text to decode

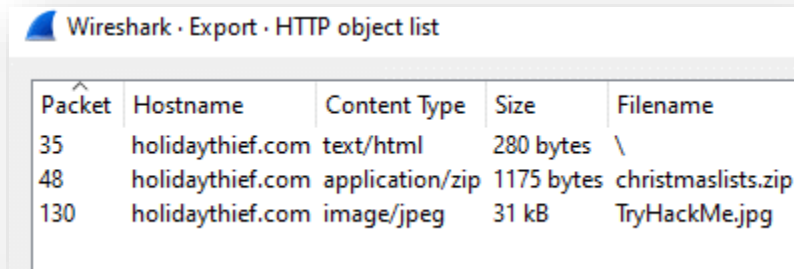
43616e64792043616e652053657269616c204e756d6265722038343931|

The decoded string:

Candy Cane Serial Number 8491

- Candy Cane Serial Number 8491

2. What did Little Timmy want to be for Christmas?



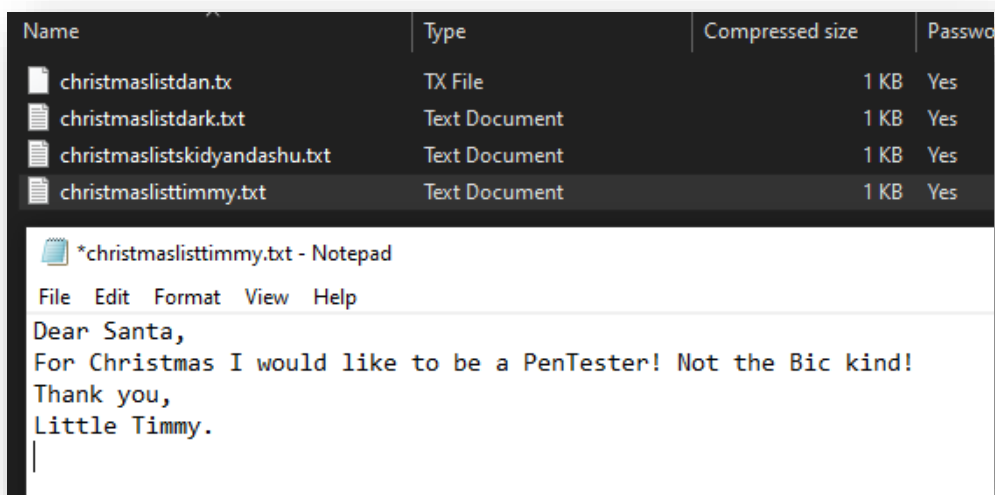
Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
35	holidaythief.com	text/html	280 bytes	\
48	holidaythief.com	application/zip	1175 bytes	christmaslists.zip
130	holidaythief.com	image/jpeg	31 kB	TryHackMe.jpg

- View all the objects that were sent
- What we want is in christmaslists.zip
- Password protected, need to brute force
- Use fcrackzip program and a rockyou.txt list found from github

```
chetsboii@XPS15:~$ fcrackzip -b --method 2 -D -p /mnt/c/Users/Chet/Downloads/rockyou.txt
-v /mnt/c/Users/Chet/Downloads/christmaslists.zip
found file 'christmaslistdan.tx', (size cp/uc 91/ 79, flags 9, chk 9a34)
found file 'christmaslistdark.txt', (size cp/uc 91/ 82, flags 9, chk 9a4d)
found file 'christmaslistskidyandashu.txt', (size cp/uc 108/ 116, flags 9, chk 9a74)
)
found file 'christmaslisttimmy.txt', (size cp/uc 105/ 101, flags 9, chk 9a11)
possible pw found: december ()
```

- Possible password found is December



Name	Type	Compressed size	Password
christmaslistdan.tx	TX File	1 KB	Yes
christmaslistdark.txt	Text Document	1 KB	Yes
christmaslistskidyandashu.txt	Text Document	1 KB	Yes
christmaslisttimmy.txt	Text Document	1 KB	Yes

*christmaslisttimmy.txt - Notepad

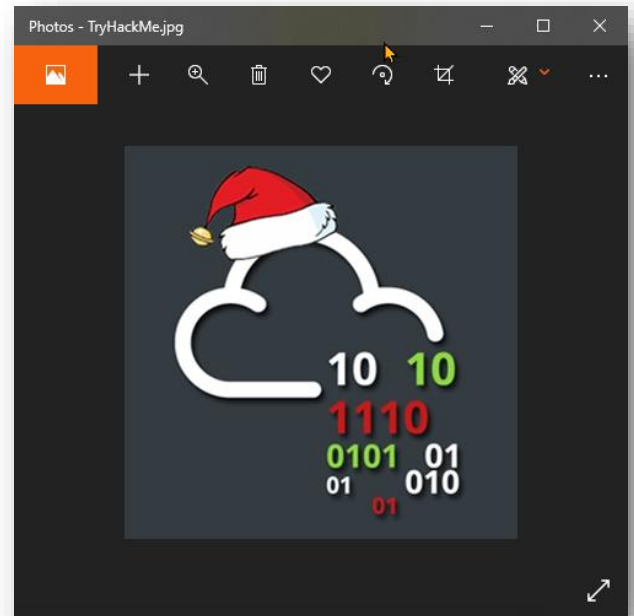
File Edit Format View Help

Dear Santa,
For Christmas I would like to be a PenTester! Not the Bic kind!
Thank you,
Little Timmy.

- After entering the password and opening the file, we can see that Timmy wants to be a **PenTester** for christmas

3. What was hidden within the file?

- The file is a .jpg picture
- To see if there is hidden information someone added to the file, we can use a Steganographical method program, Steghide. It can hide information into a picture or audio file and can retrieve that information. The files are resistant to first-order scans.
- Command is `steghide extract -sf <file>`



```
chetboii@XPS15:~$ steghide extract -sf /mnt/c/Users/Chet/Downloads/TryHackMe.jpg
Enter passphrase:
wrote extracted data to "christmasmonster.txt".
```

- Christmasmonster is **RFC527**: ARPAWOCKY
- Link to RFC527: <https://tools.ietf.org/html/rfc527>
- The contents of christmasmonster.txt:

```
chetboii@XPS15:~$ cat christmasmonster.txt
```

ARPAWOCKY

RFC527

Twas brillig, and the Protocols
Did USER-SERVER in the wabe.
All mimsey was the FTP,
And the RJE outgrabe,

Beware the ARPANET, my son;
The bits that byte, the heads that scratch;
Beware the NCP, and shun
the frumious system patch,

He took his coding pad in hand;
Long time the Echo-plex he sought.
When his HOST-to-IMP began to limp
he stood a while in thought,

And while he stood, in uffish thought,
The ARPANET, with IMPish bent,
Sent packets through conditioned lines,
And checked them as they went,

One-two, one-two, and through and through
The IMP-to-IMP went ACK and NACK,
When the RFNM came, he said "I'm game",
And sent the answer back,

Then hast thou joined the ARPANET?
Oh come to me, my bankrupt boy!
Quick, call the NIC! Send RFCs!
He chortled in his joy.

Twas brillig, and the Protocols
Did USER-SERVER in the wabe.
All mimsey was the FTP,
And the RJE outgrabe.

D.L. COVILL
May 1973