

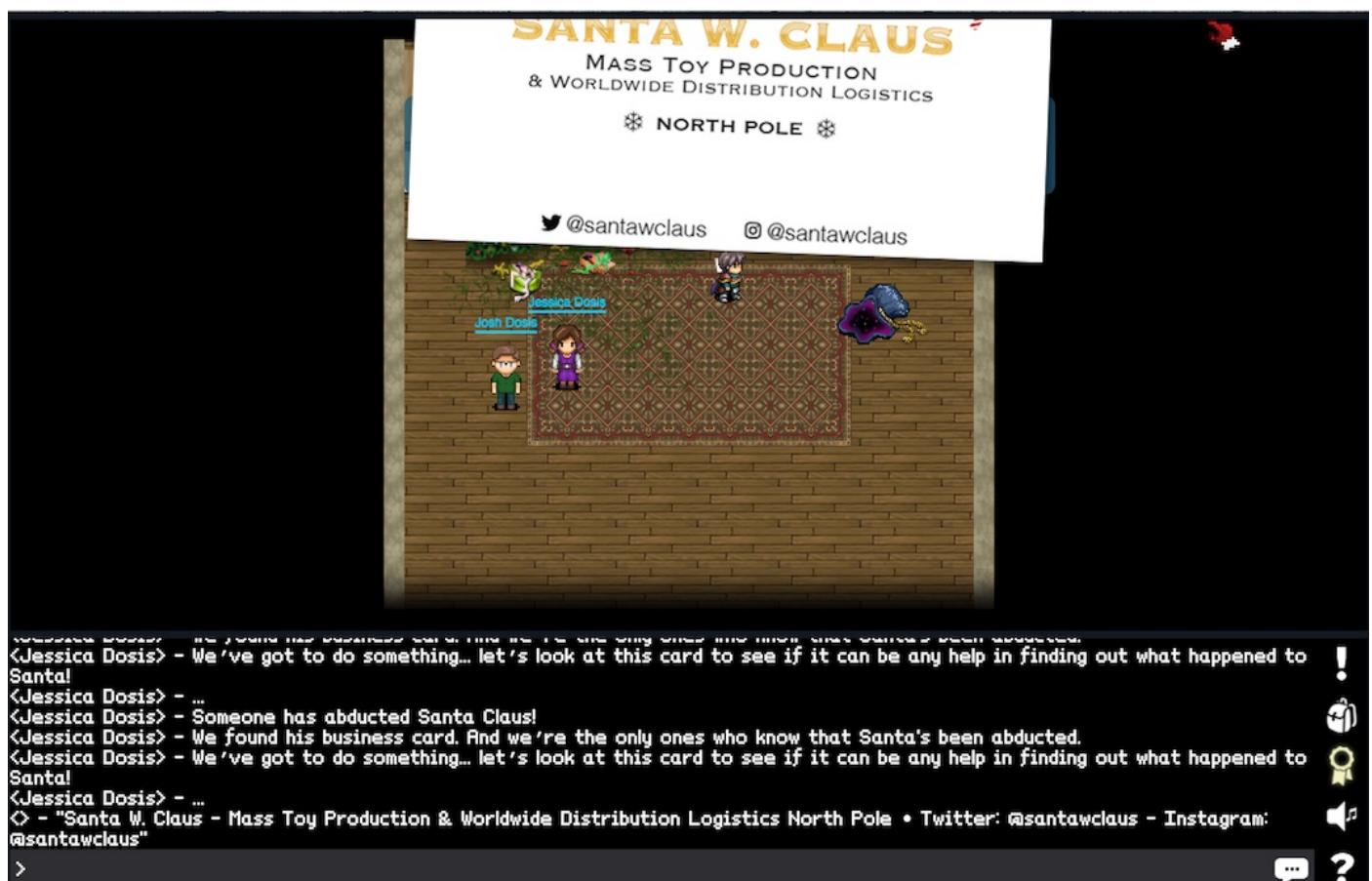
# 2016-sans-holiday-hack-challenge

## About

This is a write-up for the [2016 SANS Holiday Hack Challenge](#). What follows is a step by step guide. A summary of answers to the questions is given at the end of the document.

## Step by step guide

You start off in a room. Talk to Jessica and Josh to get some info and the first two quests. Browse the room for Santa's business card (it is lying in front of the fireplace).



This gives us two pieces of information to have a look at:

- Santa's Twitter account @santawclaus
- Santa's Instagram account @santawclaus

We will check out the Twitter account first.



Santa's tweets look a bit odd. Since the first question directly asks for a secret message in them, we decided to pull them all down via the Twitter API.

Turns out that there is a Python package for talking to Twitter called [tweepy](#). They do offer a solid [documentation](#). The most challenging part was to actually create the necessary Twitter API credentials [here](#). With that out of the way, a small python script like the following will pull all 350 tweets from @santawclaus .

```
import tweepy
```

```
consumer_key='<YOUR CONSUMER KEY>'  
consumer_secret='<YOUR CONSUMER SECRET>'  
access_token='<YOUR ACCESS TOKEN>'  
access_token_secret='<YOUR ACCESS TOKEN SECRET>'  
  
auth = tweepy.OAuthHandler(consumer_key, consumer_secret)  
auth.set_access_token(access_token, access_token_secret)  
  
all_tweets = api.user_timeline('santawclaus', count=200)  
  
max_id = all_tweets[-1].id - 1  
  
all_tweets.extend(api.user_timeline('santawclaus', count=200, max_  
  
for tweet in all_tweets:  
    print tweet.text
```

The code is a bit messy. Since the maximum count that you can specify is 200, and Santa has done 350 tweets, we have to call the API twice. The `max_id` parameter ensures that we get only older tweets in the second call compared to the first one. At first, I overlooked this issue - getting an incomplete secret message.

The correct result looks as follows on the terminal:

```
SANTAELFHOHOHOCHRISTMASSANTACHRISTMASPEACEONEARTHCHRISTMASELFANTA  
GOODWILLTOWARDSMENSANTAPEACEONEARTHHOHOHOJOYSANTAGOODWILLTOWARDSME  
GOODWILLTOWARDSMENGOODWILLTOWARDSMENJOYHOHOHOJOYELFELFPEACEONEARTH  
GOODWILLTOWARDSMENSANTACHRISTMASCHRISTMASPEACEONEARTHNORTHPOLEHOHO  
JOYNORTHPOLECHRISTMASPEACEONEARTHNORTHPOLEJOYGOODWILLTOWARDSMENELF  
CHRISTMASGOODWILLTOWARDSMENELFHOHOHOCHRISTMASPEACEONEARTHPEACEONEA  
HOHOHOGOODWILLTOWARDSMENNORTHPOLEGOODWILLTOWARDSMENSANTAPEACEONEAR  
GOODWILLTOWARDSMENP?????????????????????????????????4CHRISTMASJOYELF  
NORTHPOLEHOHOHOELFF.....]PEACEONEARTHHOH
```

SANTASANTAJOYELFQQf ..... ]PEACEONEARTHCHR  
CHRISTMASSELFELFJOYf ..... ]HOHOHOSANTAHOHO  
SANTASANTAJOYJOYQQf ..... ]GOODWILLTOWARDS  
NORTHPOLEELFELFF ..... ]PEACEONEARTHHOH  
NORTHPOLECHRISTMASf ..... ]PEACEONEARTHCHR  
PEACEONEARTHSANTAQf ..... ]PEACEONEARTHNR  
JOYCHRISTMASSANTAQf ..... ]CHRISTMASHOHOHO  
NORTHPOLEHOHOHOJOYf ..... ]PEACEONEARTHPEA  
SANTAELFELFJOYJOYQf ..... aaaaaa/\_aaaaaa.....]PEACEONEARTHNR  
GOODWILLTOWARDSMENf ..... QQWQWQf ..... ]ELFWQ.....]HOHOHOHOHOHOCHR  
NORTHPOLESANTAJOYQf ..... HOHOHOF.....]JOYQQ.....]CHRISTMASCHRIST  
NORTHPOLEELFJOYJOYf ..... SANTAQf.....]JOYQQ.....]NORTHPOLEPEACEO  
SANTAPEACEONEARTHQf ..... HOHOHOF.....]SANTA.....]PEACEONEARTHCHR  
ELFSANTASANTAJOYQQf ..... HOHOHOF.....]JOYQW.....]CHRISTMASPEACEO  
JOYHOHOHONORTHPOLEf ..... SANTAQ[.....)ELFQE.....]PEACEONEARTHPEA  
HOHOHOCHRISTMASJOYf ..... \$WJOYQ(.....\$WQQ(.....]GOODWILLTOWARDS  
JOYPEACEONEARTHELFF ..... )JOYQ@.....??'.....]SANTAPEACEONEAR  
JOYJOYPEACEONEARTH ..... ?\$QV' ..... ]CHRISTMASJOYNOR  
SANTAJOYCHRISTMASQk ..... jGOODWILLTOWARDS  
GOODWILLTOWARDSMENW ..... jJOYNORTHPOLEJOY  
HOHOHOSANTAJOYELFQQ ..... GOODWILLTOWARDSM  
CHRISTMASSANTASANTA; ..... ; ..... =JOYNORTHPOLEPEAC  
GOODWILLTOWARDSMENQL ..... )L ..... jHOHOHOHOHOHOCHR  
CHRISTMASHOHOHOELFQQ ..... dQ, ..... &lt;GOODWILLTOWARD  
GOODWILLTOWARDSMENQQL ..... &lt;QQm, ..... \_HOHOHOHOHOHOCHR  
SANTACHRISTMASELFELFQc ..... \_mJOYQc ..... aPEACEONEARTHCHRISTM  
CHRISTMASPEACEONEARTHQw ..... \_mSANTAwmaawGOODWILLTOWARDSMENSAN  
PEACEONEARTHELFSAELFQw, , . \_yHOHOHOELFQWQQWGOODWILLTOWARDSMENHO  
ELFHOHOHONORTHPOLEELFJOYWGOODWILLTOWARDSMENCHRISTMASSANTACHRISTMAS  
ELFELFHOHOHOHOHOHOHOHOHOHNORTHPOLEJOYHOHOHOGOODWILLTOWARDSMENELFELF  
ELFHOHOHOJOYPEACEONEARTHPEACEONEARTHJOYGOODWILLTOWARDSMENJOYELFPEA  
GOODWILLTOWARDSMENJOYGOODWILLTOWARDSMENGOODWILLTOWARDSMENSANTAELFJ  
ELFSANTAPEACEONEARTHJOYJOYQQDT?????????????????????4NORTHPOLEPEACEO  
NORTHPOLENORTHPOLESANTAQWT^ ..... ]NORTHPOLEELFHOH  
HOHOHOHOHOHOCHRISTMASQQP` ..... ]JOYGOODWILLTOWA  
ELFPEACEONEARTHSANTAQQ( ..... ]HOHOHOSANTACHRI  
JOYJOYCHRISTMASELFJOY( ..... ]GOODWILLTOWARDS  
CHRISTMASELFELFELFQQf ..... ]HOHOHONORTHPOLE  
SANTACHRISTMASJOYQQD ..... ]HOHOHOHOHOHOSAN

HOHOHOELFSANTAELFQQ( ..... ] GOODWILLTOWARDS  
GOODWILLTOWARDSMENW ..... ] NORTHPOLEHOHOHO  
CHRISTMASHOHOHOJOYF ..... ] GOODWILLTOWARDS  
CHRISTMASCHRISTMAS[ ..... \_aaaaaaaaaaaaaaaaaaaj PEACEONEARTHELF  
SANTANORTHPOLEELFQ( ..... j JOYQWQWWQWWQWWWWWWWWGOODWILLTOWARDSME  
ELFPEACEONEARTHELF; ..... j WWSANTAGOODWILLTOWARDSMENSANTAGOODWILLT  
ELFJOYNORTHPOLEJOY` ..... QWGOODWILLTOWARDSMENGODWILLTOWARDSMENCH  
PEACEONEARTHJOYELF ..... ] WPEACEONEARTHCHRISTMASNORTHPOLEPEACEONEA  
CHRISTMASJOYHOHOHO ..... ] HOHOHOELFGOODWILLTOWARDSMENPEACEONEARTH  
JOYCHRISTMASJOYELF ..... ] PEACEONEARTHCHRISTMASGOODWILLTOWARDSMENE  
JOYPEACEONEARTHJOY ..... ) WGOODWILLTOWARDSMENSANTANORTHPOLEJOYPEAC  
CHRISTMASHOHOHOELF ..... \$WPEACEONEARTHNORTHPOLESANTAPEACEONEARTH  
JOYHOHOHOELFELFJOY; ..... -QWCHRISTMASGOODWILLTOWARDSMENPEACEONEAR  
HOHOHOCHRISTMASJOY( ..... -?QWJOYCHRISTMASSANTACHRISTMASCHRISTMA  
ELFJOYELFCHRISTMASf ..... ] PEACEONEARTHNOR  
ELFHOHOHOSANTAELFQh ..... ] GOODWILLTOWARDS  
SANTACHRISTMASELFQQ, ..... ] PEACEONEARTHPEA  
GOODWILLTOWARDSMENQL ..... ] HOHOHOELFCHRIST  
GOODWILLTOWARDSMENQQ, ..... ] PEACEONEARTHELF  
NORTHPOLESANTAHOOHOHm ..... ] HOHOHOGOODWILLT  
PEACEONEARTHCHRISTMASg ..... ] ELFHOHOHOSANTAN  
NORTHPOLECHRISTMASJOYQm, ..... ] NORTHPOLECHRIST  
SANTASANTACHRISTMASSANTAw, ..... ] GOODWILLTOWARDS  
GOODWILLTOWARDSMENHOHOHOWQga,, ..... ] PEACEONEARTHPEA  
PEACEONEARTHJOYCHRISTMASELFWCHRISTMASGOODWILLTOWARDSMENJOYPEACEONE  
PEACEONEARTHPEACEONEARTHCHRISTMASJOYSANTAPEACEONEARTHCHRISTMAELFH  
GOODWILLTOWARDSMENNORTHPOLECHRISTMASPEACEONEARTHHOHOHOELFJOYNORTH  
JOYGOODWILLTOWARDSMENSANTACHRISTMASJOYPEACEONEARTHHOHOHOELFCHRISTM  
HOHOHOCHRISTMASHOHOHOSANTANORTHPOLEPEACEONEARTHJOYPEACEONEARTHJOYJ  
JOYELFGOODWILLTOWARDSMENSANTAQBTT??TT\$SANTASANTAPEACEONEARTHNORTH  
SANTACHRISTMASCHRISTMASJOYWP" ` ..... -"9NORTHPOLEPEACEONEARTHCHR  
SANTAELFELFELFSANTAJOYQQWP` ..... -4JOYSANTANORTHPOLEJOYSA  
ELFELFELFHOHOHOHOHOQQ@' ..... \$"CHRISTMASELFANTSANTANOR  
ELFCHRISTMASSANTAELFQQP` ..... -\$WELFWPEACEONEARTHSA  
SANTANORTHPOLEJOYELFQE ..... -\$SANTAELFWGOODWILLT  
NORTHPOLEELFELFELFQQ@` ..... -QWPEACEONEARTHPEAC  
PEACEONEARTHJOYJOYQQ( ..... ] CHRISTMASHOHOHOEL  
HOHOHOCHRISTMASELFQP ..... \$NORTHPOLEJOYQWJO  
SANTACHRISTMASJOYQQ( ..... ] WSANTAWPEACEONEA

HOHOHOSANTAJOYELFQW.....\_aaaas,.....QWCHRISTMASQWHOH  
SANTAPEACEONEARTHQf.....\_wELFWWWWWQW,.....3ELFHOHOJOYJOY  
CHRISTMASSANTAELFQ[.....&lt;HOHOHOELFELFQc.....]CHRISTMASPEA  
CHRISTMASCHRISTMAS(.....\_PEACEONEARTHJOY/.....)NORTHPOLESANTE  
PEACEONEARTHSANTAQ`.....dNORTHPOLEHOHOHOM.....:NORTHPOLEWCHRIS  
PEACEONEARTHELFELF.....SANTANORTHPOLEJOY;.....SANTASANTAJOYQW  
PEACEONEARTHSANTAQ.....]ELFSANTAJOYJOYELF[.....GOODWILLTOWARDS  
GOODWILLTOWARDSMEN.....]ELFNORTHPOLEJOYQQF.....ELFSANTAJOYHOHO  
GOODWILLTOWARDSMEN.....]ELF.....]JOYELF[.....PEACEONEARTHPEA  
HOHOHOJOYNORTHPOLE.....]JOY.....]SANTAQ'.....SANTASANTAQQWNO  
CHRISTMASNORTHPOLE:.....)WQQ.....]SANTAD.....NORTHPOLESANTE  
ELFCHRISTMASSANTAQ;.....-JOY.....]ELFQW'.....:PEACEONEARTHCHR  
CHRISTMASSANTAELFQ[.....WQQ.....]ELFD'.....=HOHOHOGOODWILLT  
ELFELFSANTAJOYELFQL.....]QQ.....]ELF.....]PEACEONEARTHQWC  
NORTHPOLESANTAELFQm.....+QQ.....]ELF;.....jWNORTHPOLENORTH  
JOYELFHOHOHOSANTAQQ.....]JOY[.....mCHRISTMASCHRIST  
NORTHPOLENORTHPOLEQ[.....]JOYL.....\_PEACEONEARTHSANT  
SANTANORTHPOLEJOYQQm.....]ELFk.....dHOHOHOPEACEONEAR  
PEACEONEARTHHOHOHQOC.....]JOYm.....]PEACEONEARTHHOHOH  
CHRISTMASHOHOHOJOYQQm.....]ELFQ.....\_GOODWILLTOWARDSMEN  
JOYELFNORTHPOLEJOYELFL.....]JOYQ;....&lt;SANTAHOOHONORTH  
PEACEONEARTHELFHOHOHOQ,.....]JOYQ[...wPEACEONEARTHELFSANTA  
CHRISTMASELFELFELFJOYQ6.....]ELFQL\_wPEACEONEARTHHOHOHOCHRI  
HOHOHOJOYNORTHPOLEQWELFaaaaaaaaaaaaajPEACEONEARTHGOODWILLTOWARDSME  
CHRISTMASELFPEACEONEARTHWWWWQWWQWWWWELFELFSANTANORTHPOLESANTAELFQQW  
CHRISTMASNORTHPOLEHOHOHOHOHOCHRISTMASGOODWILLTOWARDSMENNORTHPOLE  
GOODWILLTOWARDSMENNORTHPOLENORTHPOLESANTANORTHPOLEJOYSANTAELFELFWC  
GOODWILLTOWARDSMENHOHOHOHOHOHONORTHPOLEELFSANTAELFNORTHPOLEPEACEON  
PEACEONEARTHELFELFQWPEACEONEARTHPEACEONEARTHHOHOHOPEACEONEARTHWNOR  
ELFPEACEONEARTHCHRISTMASELFPEACEONEARTHJOYNORTHPOLEGODWILLTOWARDS  
SANTASANTASANTAJOYELFJOYWGOODWILLTOWARDSMENPEACEONEARTHSANTAWPEACE  
PEACEONEARTHSANTAJOYGOODWILLTOWARDSMENSANTACHRISTMASELFCHRISTMASEL  
CHRISTMASCHRISTMASELFELFHOHOHOWJOYWNORTHPOLESANTACHRISTMASWSANTAJO  
ELFJOYSANTAJOYJOYQQWJOYWPEACEONEARTHNORTHPOLEHOHOHOHOHONORTHPOLE  
ELFNORTHPOLEJOYSANTANORTHPOLECHRISTMASQQWPEACEONEARTHJOYQWHOOHOJO  
NORTHPOLECHRISTMASHOHOHOSANTAWPEACEONEARTHGOODWILLTOWARDSMENCHRIST  
GOODWILLTOWARDSMENSANTACHRISTMASSANTAQQWELFHOHOHOSANTAQQWJOYSANTAQ  
JOYNORTHPOLEJOYPEACEONEARTHWELFELFQQWNORTHPOLEQWHOHOHONORTHPOLEELF  
CHRISTMASSANTASANTAWJOYWCHRISTMASHOHOHONORTHPOLEJOYQQWHOOHOHOSANTAW

PEACEONEARTHSANTASANTAPEACEONEARTHNORTHPOLEJOYJOYJOYELFCHRISTMASHO  
SANTASANTACHRISTMASJOYJOYJOYELFJOYQWHOHOHOJOYQWPEACEONEARTHelfQQWC  
GOODWILLTOWARDSMENelfPEACEONEARTHHOHOHOCHRISTMASelfFQWHOHOHOWCHRIST  
CHRISTMASelfelfPEACEONEARTHelfQQWHOHOHQWCHRISTMASelfJOYNORTHPOL  
SANTAPEACEONEARTHQQWJOYWCHRISTMASHOHOHOPEACEONEARTHGOODWILLTOWARDS  
JOYJOYHOHOHOELFELF?????????????????????????????????4SANTAQQWPEACEON  
NORTHPOLENORTHPOLEf.....]PEACEONEARTHQQW  
CHRISTMASJOYHOHOHOF.....]ELFGOODWILLTOWA  
NORTHPOLEelfelfelff.....]PEACEONEARTHHOH  
NORTHPOLEHOHOHOELFF.....]CHRISTMASJOYQWS  
SANTAJOYNORTHPOLEQf.....]SANTAHOOHOHOWJOY  
GOODWILLTOWARDSMENf.....]PEACEONEARTHHOH  
ELFPEACEONEARTHelff.....]GOODWILLTOWARDS  
JOYCHRISTMASelfelff.....]GOODWILLTOWARDS  
GOODWILLTOWARDSMENf.....]NORTHPOLEPEACEO  
ELFSANTAHOOHOELFQf.....aaaaaa/.....\_aaaaa.....]GOODWILLTOWARDS  
NORTHPOLEHOHOHOELFF.....QWWWWQf.....]QQWWQ.....]HOHOHOHOHOHQW  
SANTANORTHPOLEJOYQf.....HOHOHOF.....]JOYQQ.....]HOHOHOHOHOHONOR  
NORTHPOLEJOYJOYELF.....JOYELFf.....]SANTA.....]NORTHPOLEHOHOHO  
SANTASANTASANTAELFF.....JOYELFf.....]SANTA.....]NORTHPOLENORTH  
GOODWILLTOWARDSMENf.....JOYJOYf.....]JOYQW.....]PEACEONEARTHHOH  
GOODWILLTOWARDSMENf.....HOHOHO[.....)JOYQE.....]HOHOHOELFHOHOHO  
JOYNORTHPOLEelfelff.....\$WELFQ(.....\$WQQ(.....]PEACEONEARTHNO  
NORTHPOLEJOYELFJOYf.....)ELFQ@.....??'.....]CHRISTMASPEACEO  
SANTAPEACEONEARTHQL.....?\$QV'.....]HOHOHOGOODWILLT  
JOYELFPEACEONEARTHk.....]jJOYSANTACHRISTM  
SANTAPEACEONEARTHQW.....]jSANTAGOODWILLTO  
CHRISTMASSANTAELFQQ.....]HOHOHOPEACEONEAR  
ELFCHRISTMASelfelfQ;.....;.....]=NORTHPOLENORTHPO  
NORTHPOLEJOYSANTAQQ[.....)L.....]jPEACEONEARTHJOYH  
CHRISTMASHOHOHOJOYQm.....dQ,.....&lt;GOODWILLTOWARD  
SANTACHRISTMASSANTAQL.....&lt;QQm,.....\_JOYELFGOODWILLT  
HOHOHOSANTASANTAJOYQQc.....\_mELFQc.....aGOODWILLTOWARDSMENS  
CHRISTMASHOHOHOJOYJOYQw.....\_mELFQQWmwaawGOODWILLTOWARDSMENNOR  
NORTHPOLEelfPEACEONEARTHw,..\_yELFJOYJOYQWQWQWGOODWILLTOWARDSMENC  
JOYNORTHPOLEelfNORTHPOLEGOODWILLTOWARDSMENNORTHPOLEJOYJOYJOYSANTA  
JOYSANTAEFLFOHOHOQQWNORTHPOLENORTHPOLEGOODWILLTOWARDSMENSANTASANTA  
ELFHOHOHOCHRISTMASCHRISTMASelfPEACEONEARTHHOHOHOELFCHRISTMASHOHOHO  
JOYPEACEONEARTHJOYNORTHPOLEGOODWILLTOWARDSMENHOHOHONORTHPOLEHOHOHO

HOHOHOPEACEONEARTHelfjoyjoyqv?"~....-"?christmaselfwpeaceonearth  
christmaschristmasjoyelfww?`.....-?christmasohohoqwelfwsa  
santapeaceonearthqqwelfqp`.....-4hoohowchristmasnorth  
christmasnorthpolejoyqw(.....)wgoodwilltowardsmenn  
goodwilltowardsmenjoyw'.....)wsantajoyqqwnorthpo  
joynorthpolehoohojoy(.....)peaceonearthsantae  
goodwilltowardsmenqfq.....4peaceonearthelfqw  
northpolehoohoelfqw`.....-hoohowchristmasc  
goodwilltowardsmenqf.....]joyjoysantaelfwc  
hoohonorthpolejoyq`.....-hoohoelfqwchris  
elfelfelfjoyhoohoe.....\_wwqwwqmg,.....\$goodwilltowards  
northpolechristmasf.....\_yjoywsantaqqg,.....]peaceonearthpea  
santanorthpolejoyq[.....\_elfelfsantaelfq,.....]christmassantas  
christmaschristmas;.....dpeaceonearthjoyk.....=joyjoyhoohoqwj  
elfnorthpoleelfelf.....\_hoohochristmasqq,.....northpoleqwsant  
peaceonearthjoyjoy.....]peaceonearthjoyqq[.....goodwilltowards  
hoohoelfnorthpole.....]peaceonearthsantaf.....northpolehooho  
elfsantaelfhoohoq.....]northpolehoohoqq[.....goodwilltowards  
christmaschristmas.....)peaceonearthjoyqq(.....hoohoohohosan  
santasantaelfjoyqq.....hoohochristmasqq@.....:northpoleelfqws  
christmaschristmas;.....]peaceonearthelf[.....<hoohosantan  
hoohopeaceonearth[.....4hoohojoyelfqf.....]peaceonearthhhoh  
christmaschristmasl....."hwjoysantad^.....jnorthpolenorthp  
goodwilltowardsmenm....."!???"`.....northpolehoohow  
christmasjoyelfelfq/.....]wnorthpolechrist  
santajoychristmasqqk.....dpeaceonearthelfe  
santapeaceonearthjoy/.....<northpolechris  
elfsantasantasantaqqm.....mjoyelfsantapeaceo  
christmaschristmaselfk.....jgoodwilltowardsmen  
elfjoychristmasjoyjoyql.....jnorthpolenorthpolej  
elfelfjoyantsantajoyelfelfg,.....\_ygoodwilltowardsmenqq  
peaceonearthjoyelfqwsantac.....aqwchristmasohohosanta  
santajoyjoypeaceonearthelfqa,.....\_wqwwhoohosantaJoyelfqqwj  
hoohoelfjoypeaceonearthqqwjoymwaaaaawyjoywchristmasohohopeaceone  
elfchristmassantasantasantaJoyqqwwwwqwgoodwilltowardsmenjoyelfqwch  
elfchristmassantasantasantaJoyqqwwwwqwgoodwilltowardsmenjoyelfqwch  
santaohohoelfpeaceonearthgoodwilltowardsmenjoypeaceonearthsantasa  
hoohojoyelfjoyelfqwgoodwilltowardsmenpeaceonearthgoodwilltowardsm  
northpolejoyjoyelfhoohowpeaceonearthnorthpolechristmasohohoqwelef

GOODWILLTOWARDSMENSANTAJOYNORTHPOLENORTHPOLEHOHOHOHOHOGOODWILLTO  
CHRISTMASJOYSANTANORTHPOLEV?"-.....]GOODWILLTOWARDS  
GOODWILLTOWARDSMENSANTAW?`.....]GOODWILLTOWARDS  
HOHOHOELFJOYJOYELFQWQQD'.....]HOHOHONORTHPOLE  
PEACEONEARTHHOHOHOJOYP`.....]SANTAJOYELFWHOH  
PEACEONEARTHHOHOHQWD`.....]JOYPEACEONEARTH  
PEACEONEARTHHOHOHQW'.....]CHRISTMASJOYELF  
ELFPEACEONEARTHELFQf.....]PEACEONEARTHELF  
SANTACHRISTMASJOYQQ`.....]NORTHPOLEQQWNOR  
CHRISTMASHOHOHOELFE.....]SANTAGOODWILLTO  
GOODWILLTOWARDSMENf.....]GOODWILLTOWARDS  
ELFCHRISTMASELFFJOY[.....amWNORTHPOLEGODWILLTOWARDSMENJOYJOYJO  
PEACEONEARTHJOYJOY(.....\_QQWHOHOHOWJOYWPEACEONEARTHPEACEONEARTH  
NORTHPOLEELFELFJOY`.....mSANTAQQWCHRISTMASQQWGOODWILLTOWARDSMENQ  
JOYSANTANORTHPOLEQ`.....=CHRISTMASPEACEONEARTHSANTANORTHPOLENORTH  
NORTHPOLESANTAJOYQ.....]NORTHPOLEPEACEONEARTHELFHOHOHOGOODWILLTO  
ELFNORTHPOLESANTAQ.....]GOODWILLTOWARDSMENQWELFJOYYPEACEONEARTHCH  
HOHOHONORTHPOLEJOY.....]GOODWILLTOWARDSMENJOYJOYQWPEACEONEARTHJO  
PEACEONEARTHJOYELF.....-QWSANTAELFWSANTAWHOHOHOPEACEONEARTHCHRIS  
CHRISTMASSANTAJOYQ.....]SANTASANTASANTAGOODWILLTOWARDSMENPEACEO  
ELFHOHOHOCHRISTMAS;.....?ELFJOYYPEACEONEARTHELFQWGOODWILLTOWARDS  
GOODWILLTOWARDSMEN[.....-"??????????????????????4ELFCHRISTMASHOH  
SANTASANTAJOYSANTAL.....]HOHOHOQWJOYELFQ  
NORTHPOLECHRISTMASQ.....]NORTHPOLEELFQWJ  
SANTANORTHPOLEELFQwC.....]GOODWILLTOWARDS  
JOYSANTACHRISTMASQQm.....]ELFNORTHPOLECHR  
CHRISTMASSANTASANTAQL.....]PEACEONEARTHWJO  
ELFNORTHPOLEHOHOHOJOYc.....]SANTACHRISTMASJ  
SANTAELFHOHOHOJOYJOYQQc.....]PEACEONEARTHSAN  
GOODWILLTOWARDSMENSANTAw,.....]NORTHPOLEHOHOHO  
NORTHPOLENORTHPOLEQWSANTAA,.....]PEACEONEARTHWSA  
SANTACHRISTMASHOHOHOELFELFQQgwaaaaaaaaaaaaaaajCHRISTMASJOYPEA  
SANTAHOOHOHOPEACEONEARTHSANTAQWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW  
NORTHPOLESANTASANTANORTHPOLESANTAPEACEONEARTHCHRISTMASSELFWHOHOHOELF  
JOYELFJOYNORTHPOLEPEACEONEARTHJOYGOODWILLTOWARDSMENPEACEONEARTHELF  
SANTAJOYCHRISTMASQQWELFWGOODWILLTOWARDSMENSANTANORTHPOLENORTHPOLEJ  
JOYPEACEONEARTHSANTAGOODWILLTOWARDSMENJOYYPEACEONEARTHJOYELFJOYCHRI  
PEACEONEARTHJOYHOHOHOJOYHOHOHONORTHPOLEHOHOHOGOODWILLTOWARDSMENPEA  
SANTASANTAELFJOYQQP?????????????????????????????4PEACEONEARTHJOY

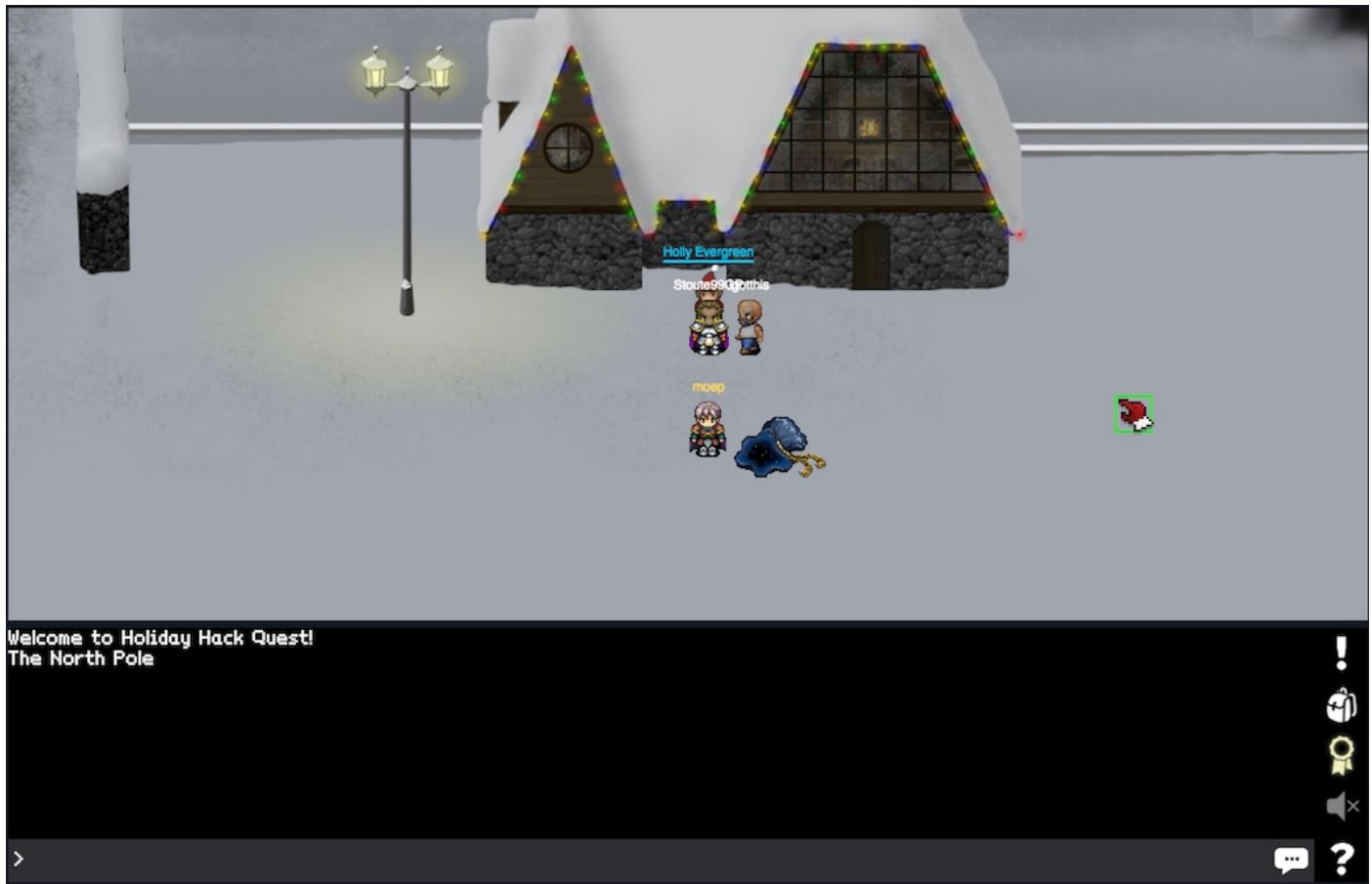
ELFELFHOHOHOHOHOHOF ..... ] GOODWILLTOWARDS  
SANTAJOYELFELFELFQf ..... ] CHRISTMASNORTHP  
SANTAHOHOHOELFJOYQf ..... ] GOODWILLTOWARDS  
GOODWILLTOWARDSMENf ..... ] CHRISTMASCHRIST  
JOYSANTAELFJOYELFQf ..... ] PEACEONEARTHSAN  
CHRISTMASCHRISTMASf ..... ] GOODWILLTOWARDS  
PEACEONEARTHSAFTAQf ..... ] HOHOHOHOHOHOJOY  
JOYELFHOHOHOJOYELFF ..... ] GOODWILLTOWARDS  
SANTANORTHPOLEJOYQf ..... ] PEACEONEARTHNR  
HOHOHOGOODWILLTOWARDSMENSANTAWJOYQ@' ..... sPEACEONEARTHELF  
GOODWILLTOWARDSMENHOHOHOCHRISTMASf ..... \_yWWPEACEONEARTH  
SANTAGOODWILLTOWARDSMENQQWELFQQ@' ..... sQWGOODWILLTOWARDSME  
NORTHPOLECHRISTMASNORTHPOLEQQWF ..... \_yQWELFELFELFSANTASANT  
NORTHPOLECHRISTMASSELFQQWELFQ@' ..... aWCHRISTMASSELFPEACEONEA  
SANTAHOHOHOHOHOJOYWSANTAQ? ..... \_yQWPEACEONEARTHCHRISTMAS  
CHRISTMASSANTACHRISTMASQQ@' ..... aJOYNORTHPOLESANTAELFOHOOH  
SANTACHRISTMASNORTHPOLEW? ..... \_yCHRISTMASCHRISTMASCHRISTMA  
PEACEONEARTHHOHOHQWQWD' ..... aHOHOHOHOHOHONORTHPOLEHOHOHOE  
HOHOHOCHRISTMASSELFELF! ..... \_mGOODWILLTOWARDSMENCHRISTMASSA  
JOYPEACEONEARTHelfQD' ..... aCHRISTMASPEACEONEARTHSAHTAHOOH  
NORTHPOLEJOYHOHOHOF ..... "?????????????????4PEACEONEARTHQQW  
HOHOHOELFSANTAEFLQf ..... ] SANTAQWJOYWNORT  
HOHOHOPEACEONEARTHf ..... ] PEACEONEARTHPEA  
JOYPEACEONEARTHelfF ..... ] HOHOHOSANTASANT  
GOODWILLTOWARDSMENf ..... ] PEACEONEARTHNR  
NORTHPOLEHOHOHOELFF ..... ] HOHOHOCHRISTMAS  
ELFSANTACHRISTMASQf ..... ] SANTAJOYJOYQWSA  
HOHOHNORTHPOLEJOYf ..... ] PEACEONEARTHSD  
GOODWILLTOWARDSMENf ..... ] CHRISTMASCHRIST  
PEACEONEARTHelfJOYf ..... ] PEACEONEARTHJOY  
JOYSANTAPEACEONEARTHSAFTAQQWQQWGOODWILLTOWARDSMENCHRISTMASJOYSANT  
ELFNORTHPOLESANTAELFOHOOHOJOYGOODWILLTOWARDSMENNORTHPOLECHRISTMASQ  
HOHOHOCHRISTMASSANTAJOYCHRISTMASHOHOHOSANTAELFQQWJOYHOHOHOJOYJOYEL  
CHRISTMASJOYJOYHOHOHOHOJOYPEACEONEARTHSAFTAELFGOODWILLTOWARDSM  
HOHOHOELFOHOOHOJOYNORTHPOLEHOHOHOCHRISTMASQ?????4GOODWILLTOWARDS  
NORTHPOLECHRISTMASQQWELFWELFWPEACEONEARTHQQ ..... ] HOHOHOCHRISTMAS  
JOYJOYGOODWILLTOWARDSMENSANTAELFQWNORTHPOLE ..... ] PEACEONEARTHCHR  
JOYELFCHRISTMASSELFHOHOHOPEACEONEARTHJOYJOYQ ..... ] GOODWILLTOWARDS  
NORTHPOLESANTAELFQQWGOODWILLTOWARDSMENELFQQ ..... ] CHRISTMASCHRIST

HOHOHOSANTAELFNORTHPOLEPEACEONEARTHelfQWelf.....]SANTAHOHOHOE LFS  
HOHOHOSANTAPEACEONEARTHelfWJOYWSANTAQWelfQQ.....]NORTHPOLENORTH P  
SANTAHOHOHOelfELFNORTHPOLENORTHPOLEWelfJOYQ.....]GOODWILLTOWARDS  
GOODWILLTOWARDSMENHOHOHOWGOODWILLTOWARDSMEN.....]SANTASANTAHOHOH  
SANTANORTHPOLESANTAWGOODWILLTOWARDSMENelfFQQ.....]CHRISTMASPEACEO  
ELFHOHOHONORTHPOLEP?????????????????????????.....]CHRISTMASSANTAQ  
PEACEONEARTH SANTAQf.....]ELFHOHOHOSANTAELF  
ELFCHRISTMASELFFELFF.....]GOODWILLTOWARDS  
PEACEONEARTHHOHOHOF.....]GOODWILLTOWARDS  
CHRISTMASNORTHPOLEF.....]HOHOHONORTHPOLE  
ELFPEACEONEARTHelfFF.....]GOODWILLTOWARDS  
JOYJOYELFSANTAELFQf.....]SANTANORTHPOLEE  
JOYHOHOHOSANTAJOYQf.....]PEACEONEARTHNO R  
SANTAELFELFHOHOHQf.....]CHRISTMASPEACEO  
HOHOHONORTHPOLEELFF.....]NORTHPOLEHOHOHO  
PEACEONEARTHelfJOY6aaaaaaaaaaaaaaaaaaaaa.....]PEACEONEARTHHOH  
CHRISTMASELFFJOYQQWWWWWWWWWWWWWWWWWWWWWWWWQQ.....]NORTHPOLENORTH P  
NORTHPOLECHRISTMASHOHOHONORTHPOLEHOHOHOJOYQ.....]PEACEONEARTHelf  
JOYPEACEONEARTHJOYCHRISTMASPEACEONEARTHelfQ.....]NORTHPOLEJOYPEA  
NORTHPOLECHRISTMASPEACEONEARTHHOHOHOSANTAQQ.....]PEACEONEARTHCHR  
HOHOHOHOHOHONORTHPOLEELFCHRISTMASHOHOHOelfQ.....]HOHOHONORTHPOLE  
NORTHPOLEJOYHOHOHQWPEACEONEARTHCHRISTMASQ.....]ELFHOHOHOE LFSAN  
ELFJOYJOYJOYNORTHPOLEJOYPEACEONEARTH SANTAQQ.....]CHRISTMASELFF  
SANTASANTACHRISTMASNORTHPOLENORTHPOLEELFJOY.....]PEACEONEARTHPEA  
ELFPEACEONEARTHJOYQWJOYJOYSANTAHOOHOJOYELF.....]GOODWILLTOWARDS  
JOYCHRISTMASJOYCHRISTMASJOYWNORTHPOLEJOYJOYaaaaaaajCHRISTMASPEACEO  
PEACEONEARTHCHRISTMASPEACEONEARTHWelfWSANTAWWWWWCHRISTMASJOYNORTH  
SANTACHRISTMASANTAELFJOYQWNORTHPOLEELFSANTAELFQQP ]NORTHPOLESANTA J  
ELFJOYCHRISTMASNORTHPOLEWPEACEONEARTHNORTHPOLEQ@^.]HOHOHOHOHOHOelf  
HOHOHOelfSANTASANTAWNORTHPOLENORTHPOLEJOYQWelfP` ..]CHRISTMASPEACEO  
CHRISTMASJOYPEACEONEARTHJOYSANTAQWCHRISTMASQ@"....]JOYGOODWILLTOWA  
GOODWILLTOWARDSMENJOYJOYWHOHOHOHOHQWelfP` ..]GOODWILLTOWARDS  
ELFSANTAHOOHOGOODWILLTOWARDSMENCHRISTMASW".....]PEACEONEARTHelf  
GOODWILLTOWARDSMENNORTHPOLEPEACEONEARTHQP` ..]GOODWILLTOWARDS  
CHRISTMASHOHOHOelfQWJOYWSANTAJOYWelfQQW".....]GOODWILLTOWARDS  
JOYHOHOHOGOODWILLTOWARDSMENHOHOHOelfQP` ..]NORTHPOLENORTH P  
PEACEONEARTHGOODWILLTOWARDSMENWJOYQW".....]HOHOHOHOHOHONOR  
ELFPEACEONEARTHJOYCHRISTMASHOHOHQP` ..]PEACEONEARTHSAN  
NORTHPOLEHOHOHOJOYELFSANTAQQWJOYW!.....]yPEACEONEARTHCHR

CHRISTMASELFJOYP?????????` ..... sPEACEONEARTHJOYJO  
JOYHOHOHOELFHOHOHOF ..... \_mWQWNORTHPOLECHRIST  
GOODWILLTOWARDSMENf ..... jCHRISTMASNORTHPOLESA  
NORTHPOLEHOHOHOELFF ..... \_JOYPEACEONEARTHELFJOYJ  
GOODWILLTOWARDSMENf ..... \_yGOODWILLTOWARDSMENCHRIS  
NORTHPOLENORTHPOLEf ..... :GOODWILLTOWARDSMENSANTASA  
ELFNORTHPOLEJOYJOYf ..... -9NORTHPOLEPEACEONEARTHCH  
NORTHPOLEELFSANTAQf ..... ?WGOODWILLTOWARDSMENHOH  
GOODWILLTOWARDSMENf ..... .4WJOYPEACEONEARTHHOHO  
PEACEONEARTHSANTAQf ..... -\$SANTACHRISTMASHOHO  
HOHOHOELFJOYJOYJOY6aaaaaaaaaaaa, ..... ?WWPEACEONEARTHPEA  
JOYELFHOHOHOJOYSANTAWWWWWWWWWWWQc ..... -4NORTHPOLEHOHOHO  
NORTHPOLEGOODWILLTOWARDSMENSANTAWWg, ..... ]GOODWILLTOWARDS  
NORTHPOLEHOHOHOELFHOHOHOCHRISTMASelfc ..... ]HOHOHOELFSANTAW  
PEACEONEARTHJOYJOYNORTHPOLESANTAJOYWwg, ..... ]GOODWILLTOWARDS  
ELFHOHOHOELFHOHOHOCHRISTMASCHRISTMASJOYc ..... ]HOHOHOJOYELFWQC  
PEACEONEARTHSANTAJOYWCHRISTMASJOYSANTAWWw, ..... ]PEACEONEARTHHOH  
CHRISTMASJOYPEACEONEARTHSANTAPEACEONEARTHQC ..... ]PEACEONEARTHSAN  
NORTHPOLEPEACEONEARTHJOYNORTHPOLEJOYELFQQWWw ..... ]PEACEONEARTHWHO  
GOODWILLTOWARDSMENQWHOOHOQWNORTHPOLEELFELFQQ/ ..... ]PEACEONEARTHNR  
ELFGOODWILLTOWARDSMENCHRISTMASJOYWJOYSANTAJOYg... ]SANTASANTAHOOH  
NORTHPOLEPEACEONEARTHGOODWILLTOWARDSMENELFELFQWQ, .. ]PEACEONEARTHNR  
CHRISTMASCHRISTMASJOYSANTAWGOODWILLTOWARDSMENQQWQwjPEACEONEARTHSAN  
ELFPEACEONEARTHJOYJOYJOYWSANTAQQWPEACEONEARTHCHRISTMASGOODWILLTOWA  
CHRISTMASJOYJOYJOYQWGOODWILLTOWARDSMENSANTAQWGOODWILLTOWARDSMENJO  
PEACEONEARTHSANTACHRISTMASSANTAEELFELFQQWJOYWGOODWILLTOWARDSMENHOHO  
PEACEONEARTHELFELFSANTAQWJOYNORTHPOLEPEACEONEARTHELFANTSANTAHOOHOPEA  
NORTHPOLECHRISTMASelfNORTHPOLEELFJOYQWCHRISTMASGOODWILLTOWARDSMENN  
JOYJOYSANTAJOYSANTACHRISTMASJOYQWPEACEONEARTHNORTHPOLECHRISTMASJOY  
JOYPEACEONEARTHELFQWELFWCHRISTMASSANTASANTANORTHPOLEQWPEACEONEARTH

This allows us to answer the first question: BUGBOUNTY.

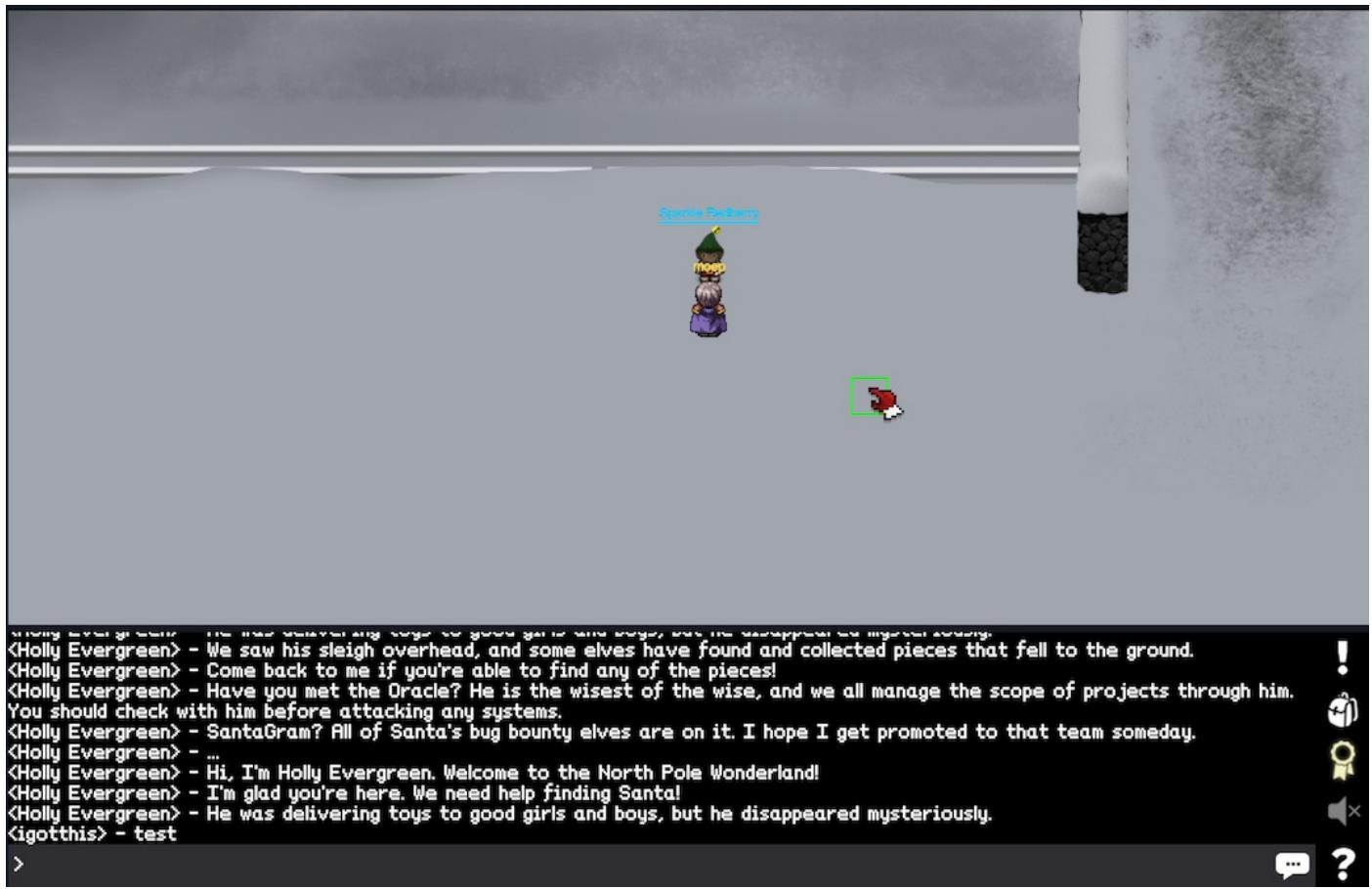
Next, it is time to take a first step outside (through the weird looking sack).



The next question is about a ZIP file. So in order to make progress, we started to walk around and literally speak to anybody there is.

First, we talked to Holly Evergreen. She said something about missing pieces that fell off Santa's sleigh, that we need to talk to the Oracle, and that basically all of Santa's bug bounty elves are on SantaGram.

Heading towards the left, you will find Sparkle Redberry.



He tells you about the NetWars challenge coins. To gather all of them is a new quest which you receive from him. Since they do not contribute to the answering of the questions, we will omit these coins for the rest of the write-up.

If you cross the bridge to the north (and keep going north a bit), you will run into Wunorse Openslae.



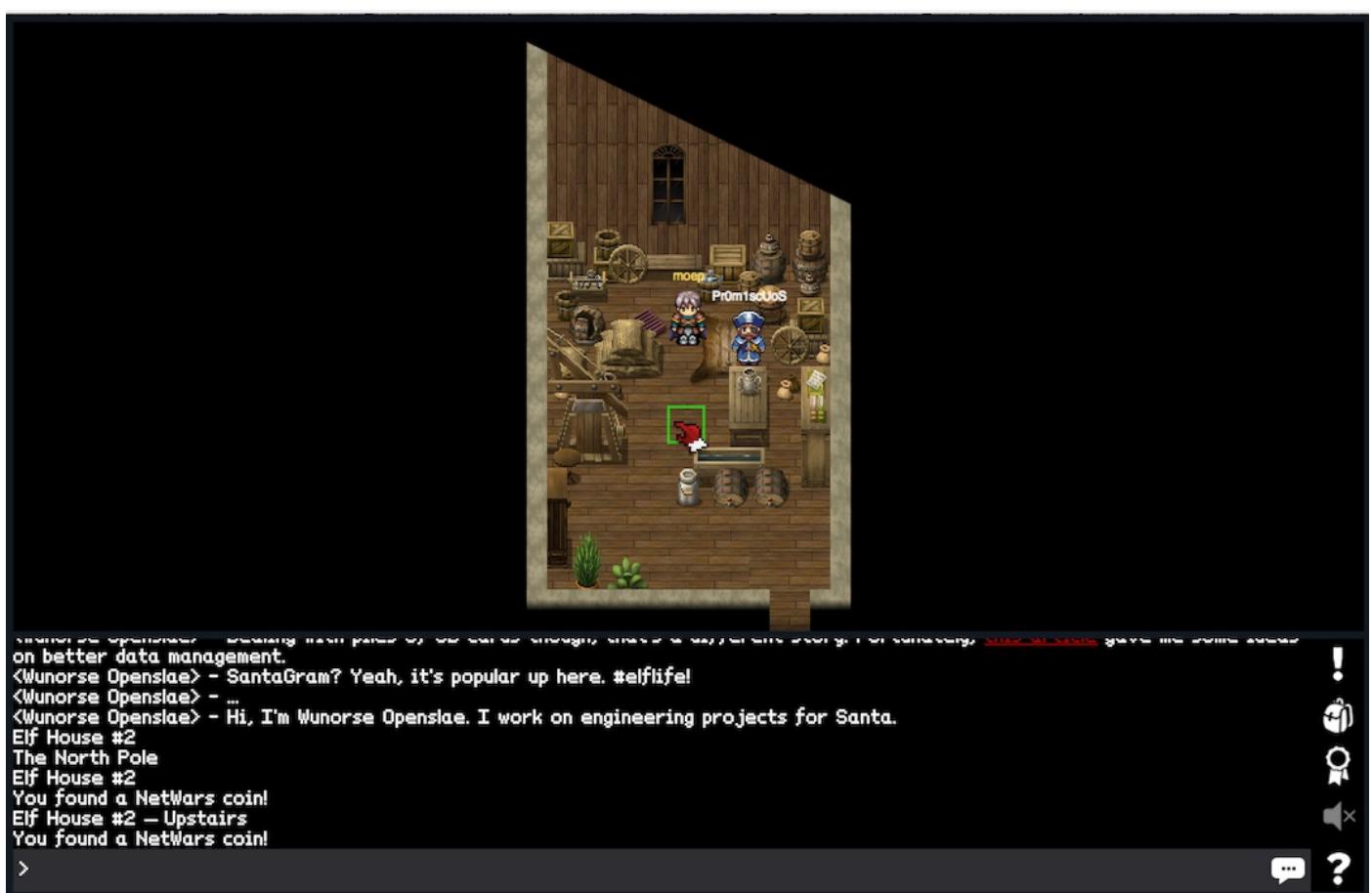
She mentions that Santa's sleigh is managed by a SCADA interface, for which you need a Cranberry Pi with a Cranbian Linux. You get a link to a [SANS website](#) which details how to mount a raspberry pi image. As of SantaGram, you get the intel that it is popular, and a hashtag:

#elflife! .

If you back off to the bridge again, and then go to the right, you will be able to enter Elf House #2 .



Enter it, go up the stairs and through the doorway, and you will find yourself in this room.

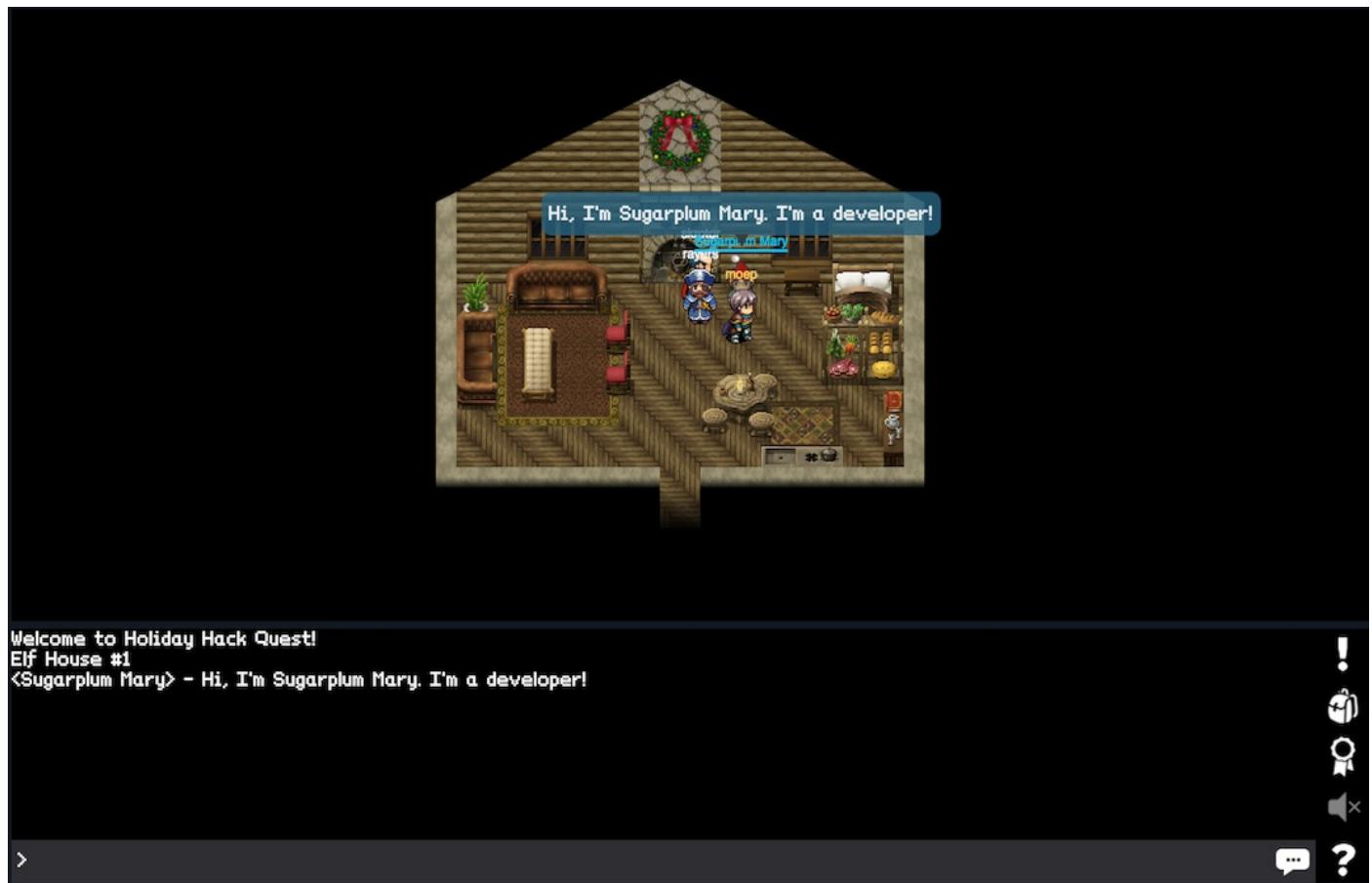


On the left of the position of my avatar, there lies a heatsink. Go collect it. We will need it later on to assemble our Cranberry Pi.

Next, head over all the way to the left until you reach this house.

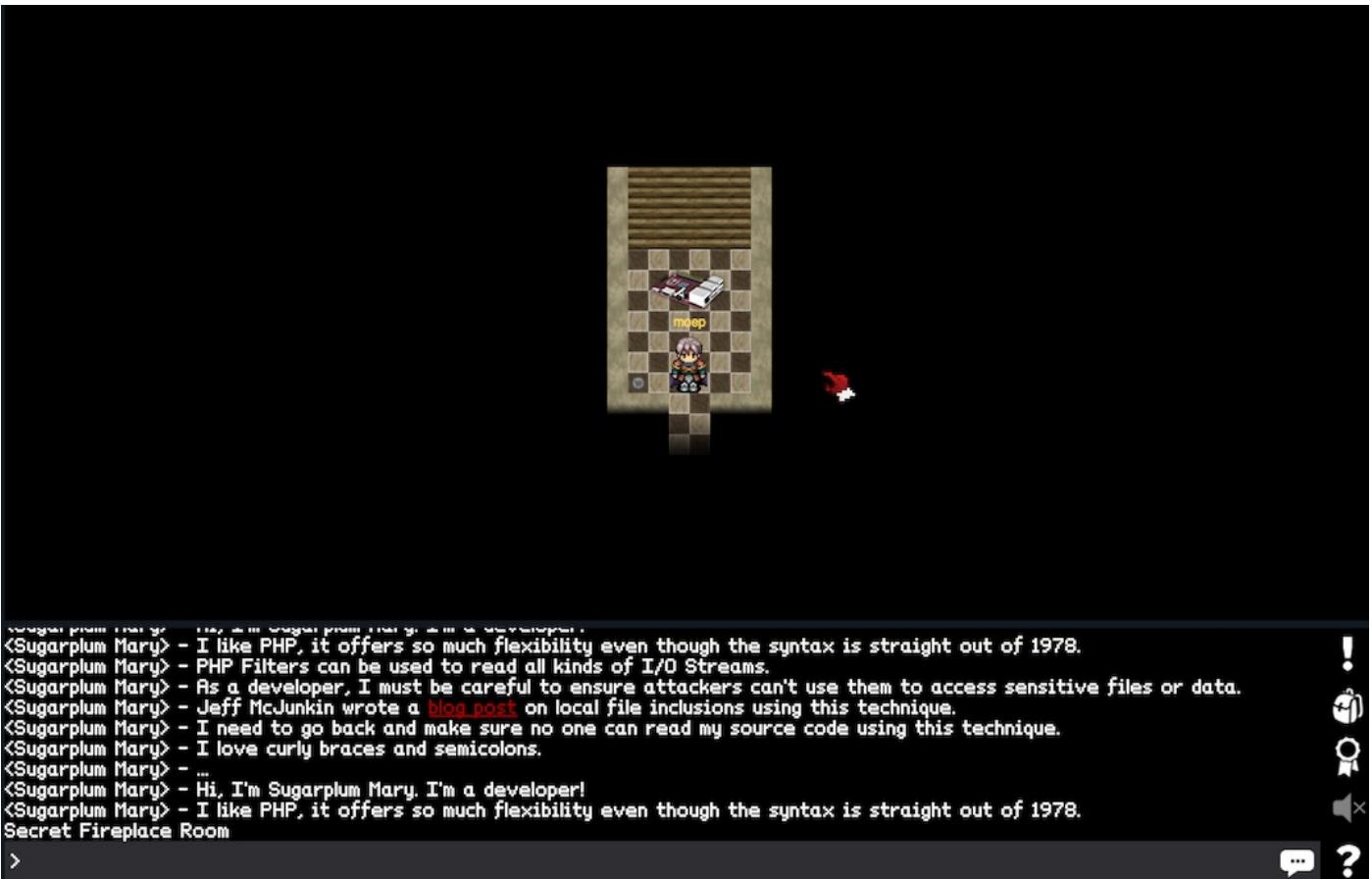


Enter it. Then talk to Sugarplum Mary.



She is a PHP developer (and apparently loves it). You will get a link to another [SANS website](#) which is about PHP local file inclusion vulnerabilities.

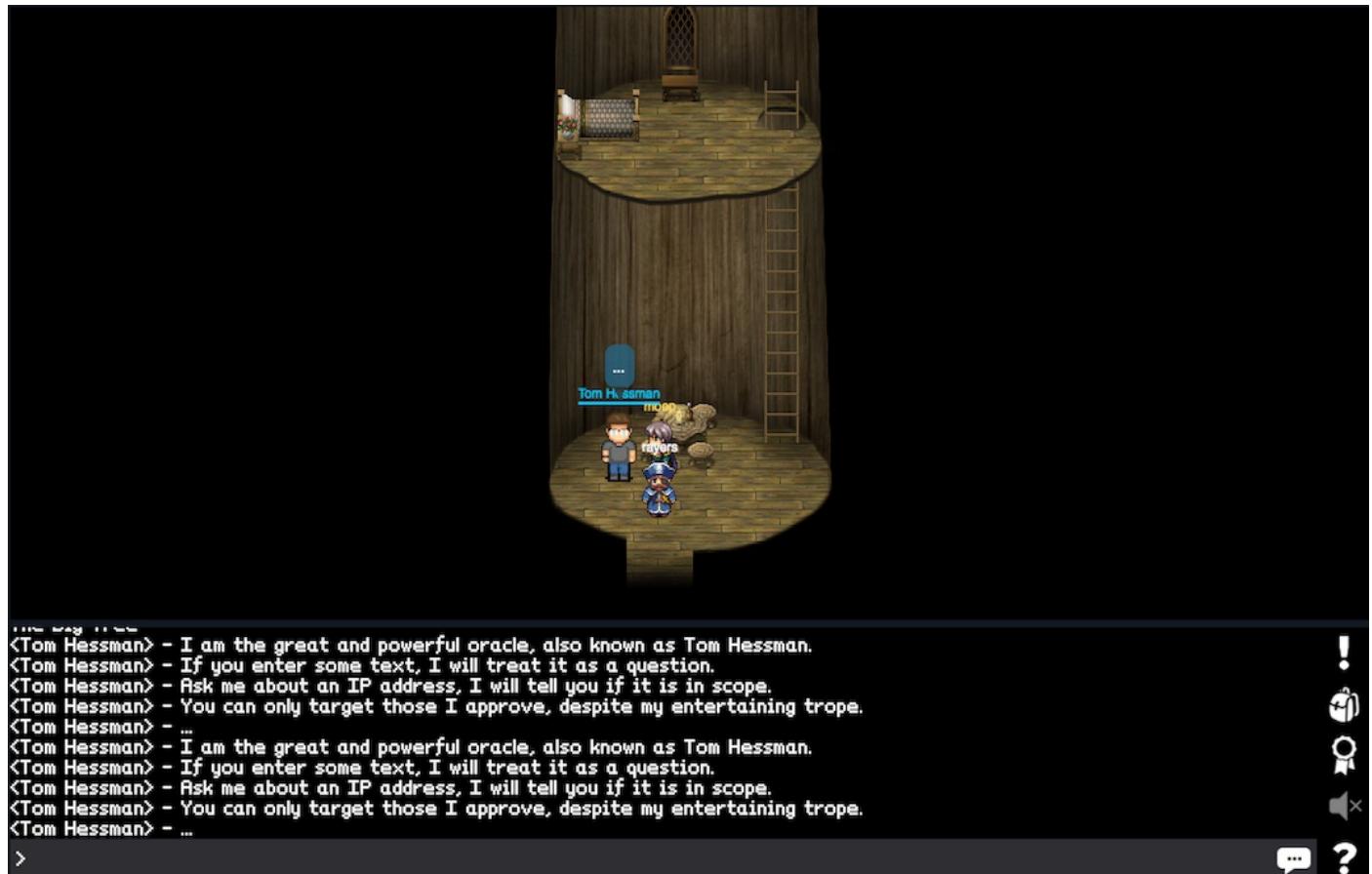
Besides PHP stuff, there is also a secret in this room. You can just walk through the fireplace and enter a small chamber. There you will find the Cranberry PI board.



Heading back all the way to the right, you will find the big tree.



Inside, you will find Tom Hessman who apparently is an oracle.



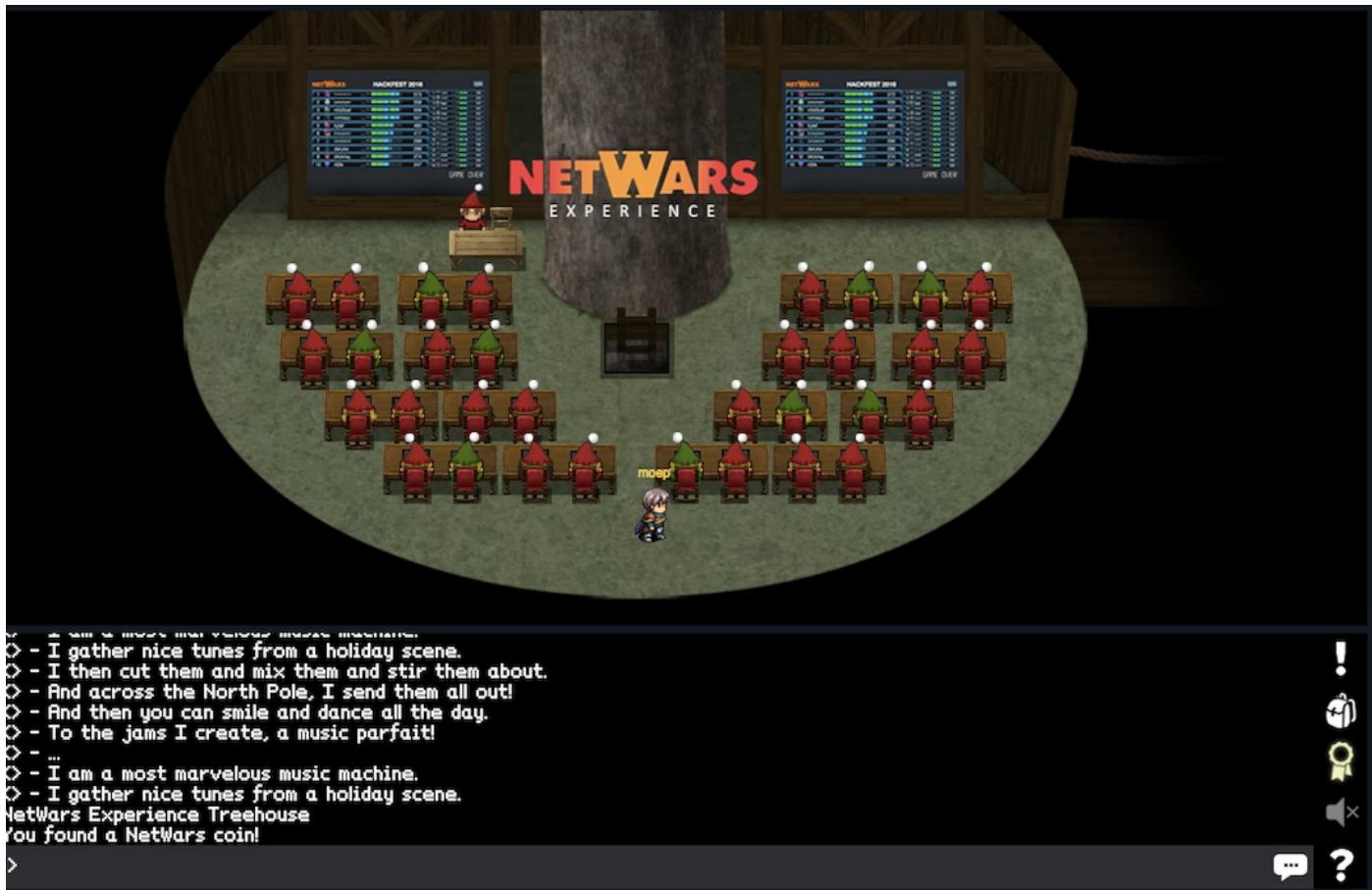
<Tom Hessman> - I am the great and powerful oracle, also known as Tom Hessman.  
<Tom Hessman> - If you enter some text, I will treat it as a question.  
<Tom Hessman> - Ask me about an IP address, I will tell you if it is in scope.  
<Tom Hessman> - You can only target those I approve, despite my entertaining trope.  
<Tom Hessman> - ...  
<Tom Hessman> - I am the great and powerful oracle, also known as Tom Hessman.  
<Tom Hessman> - If you enter some text, I will treat it as a question.  
<Tom Hessman> - Ask me about an IP address, I will tell you if it is in scope.  
<Tom Hessman> - You can only target those I approve, despite my entertaining trope.  
<Tom Hessman> - ...

He offers you to tell you whether a certain IP address is in scope or not. I guess this is a safety net so that SANS cannot be blamed for people going crazy with offensive security while blaming the SANS holiday hack challenge :D

If we go further north, there is a snow man. He holds a power cord, which we can collect.

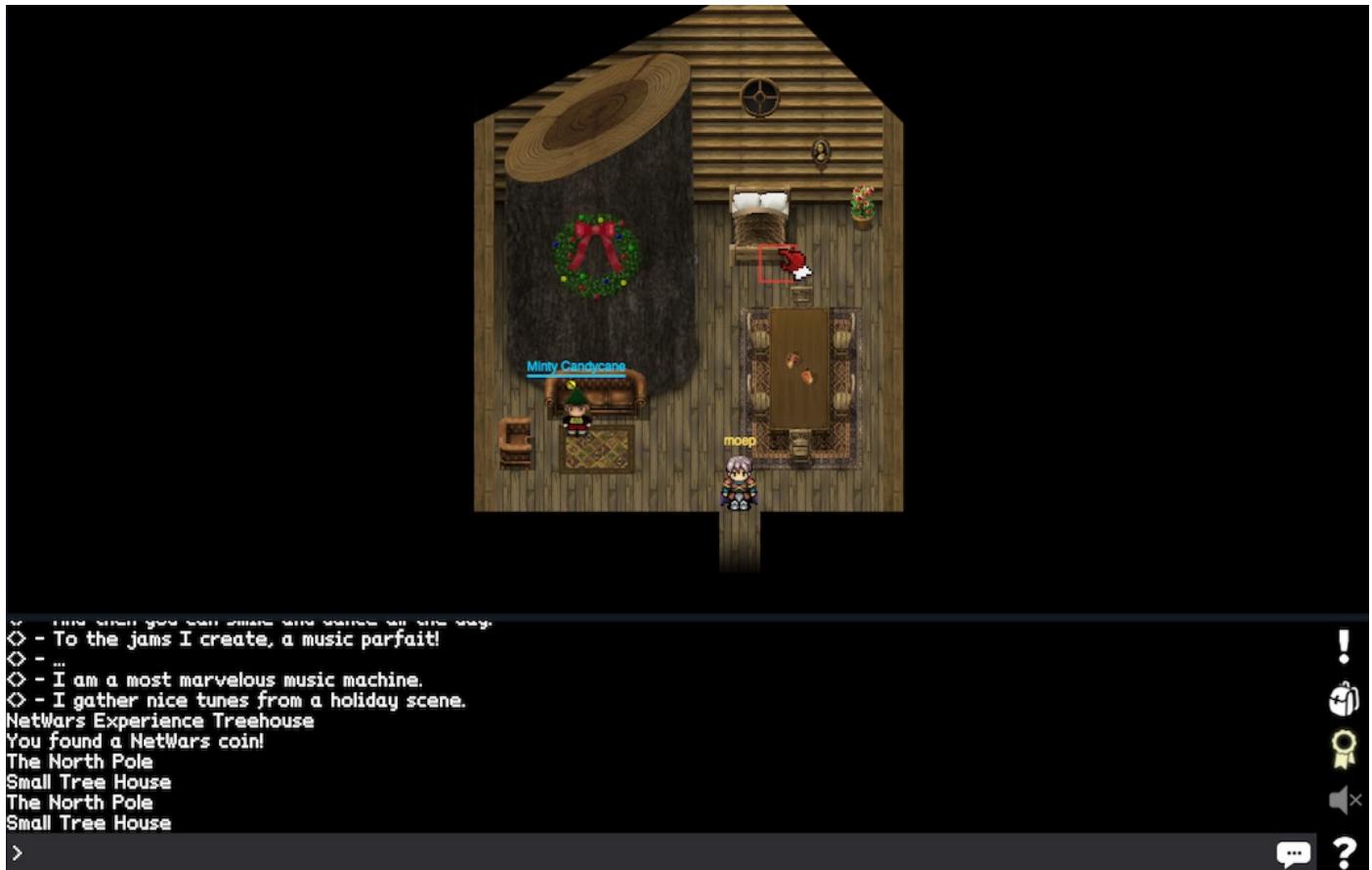


Up the three, you will enter the NetWars room.



You can leave it on the right side. Follow the path and enter the next

house.



Minty Candycane is the NPC. She talks about tools such as NMAP, John the Ripper and also provides a link to the [RockYou dictionary](#).

Exit the house again and continue to follow the path. You will go up all the way to the top of a mountain.



Talk to Bushy Evergreen on the right. He will provide you with two links regarding Android hacking ([here](#) and [here](#)).

Head over to the left and collect the SD card.



(Bushy Evergreen) - Shiny spends most of her time on app reverse engineering. I prefer to analyze apps at the Android bytecode layer.

(Bushy Evergreen) - My favorite technique? Decompiling Android apps with [Apktool](#).

(Bushy Evergreen) - JadX is great for inspecting a Java representation of the app, but can't be changed and then recompiled.

(Bushy Evergreen) - With Apktool, I can preserve the functionality of the app, then change the Android bytecode small files.

(Bushy Evergreen) - I can even change the values in Android XML files, then use Apktool again to recompile the app.

(Bushy Evergreen) - Apktool compiled apps can't be installed and run until they are signed. The Java keytool and jarsigner utilities are all you need for that.

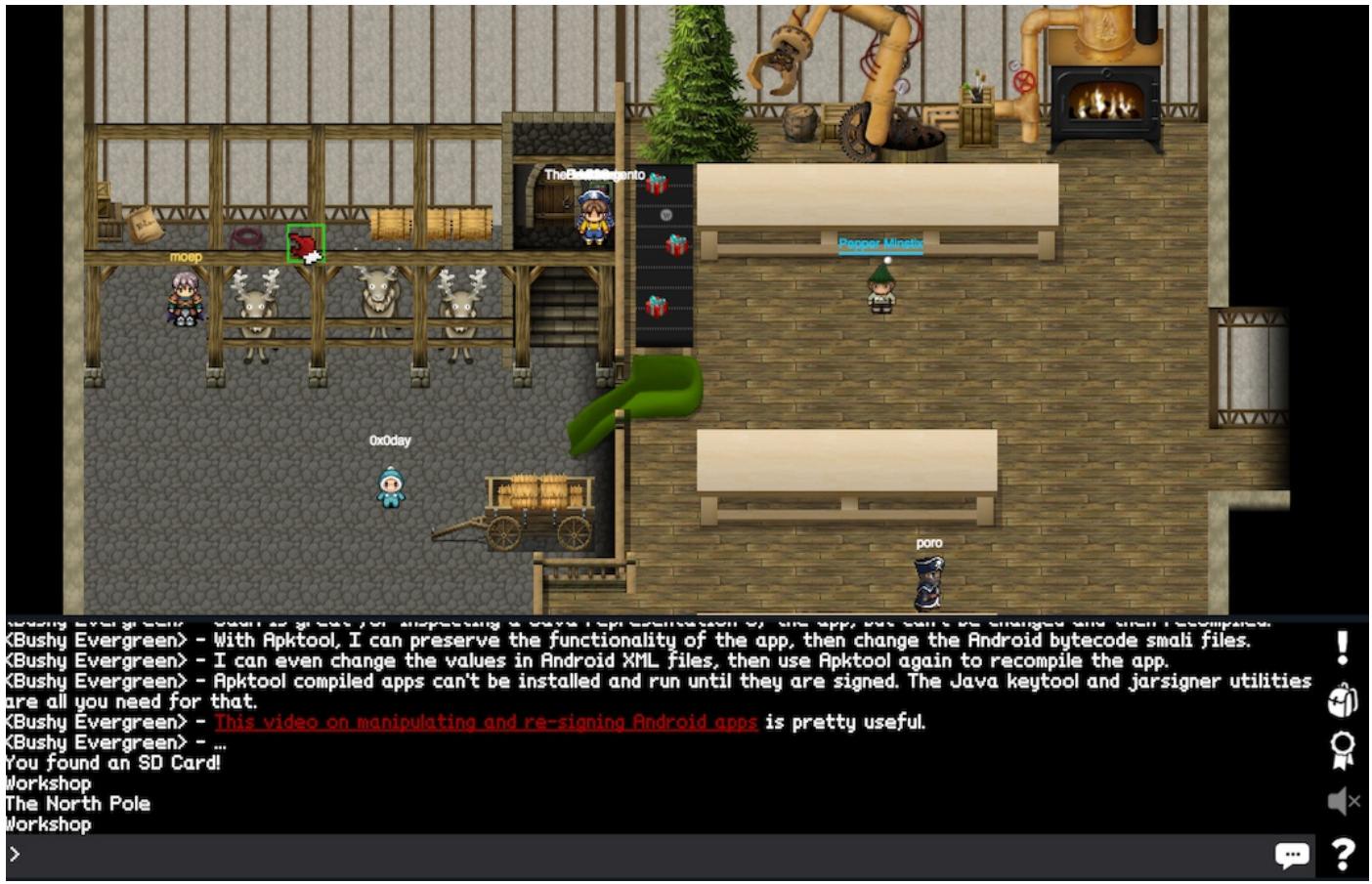
(Bushy Evergreen) - [This video on manipulating and re-signing Android apps](#) is pretty useful.

(Bushy Evergreen) - ...

>



Enter the house, go to the top left corner, and collect the HDMI cable.



(Bushy Evergreen) - With Apktool, I can preserve the functionality of the app, then change the Android bytecode small files.

(Bushy Evergreen) - I can even change the values in Android XML files, then use Apktool again to recompile the app.

(Bushy Evergreen) - Apktool compiled apps can't be installed and run until they are signed. The Java keytool and jarsigner utilities are all you need for that.

(Bushy Evergreen) - [This video on manipulating and re-signing Android apps](#) is pretty useful.

(Bushy Evergreen) - ...

You found an SD Card!

Workshop

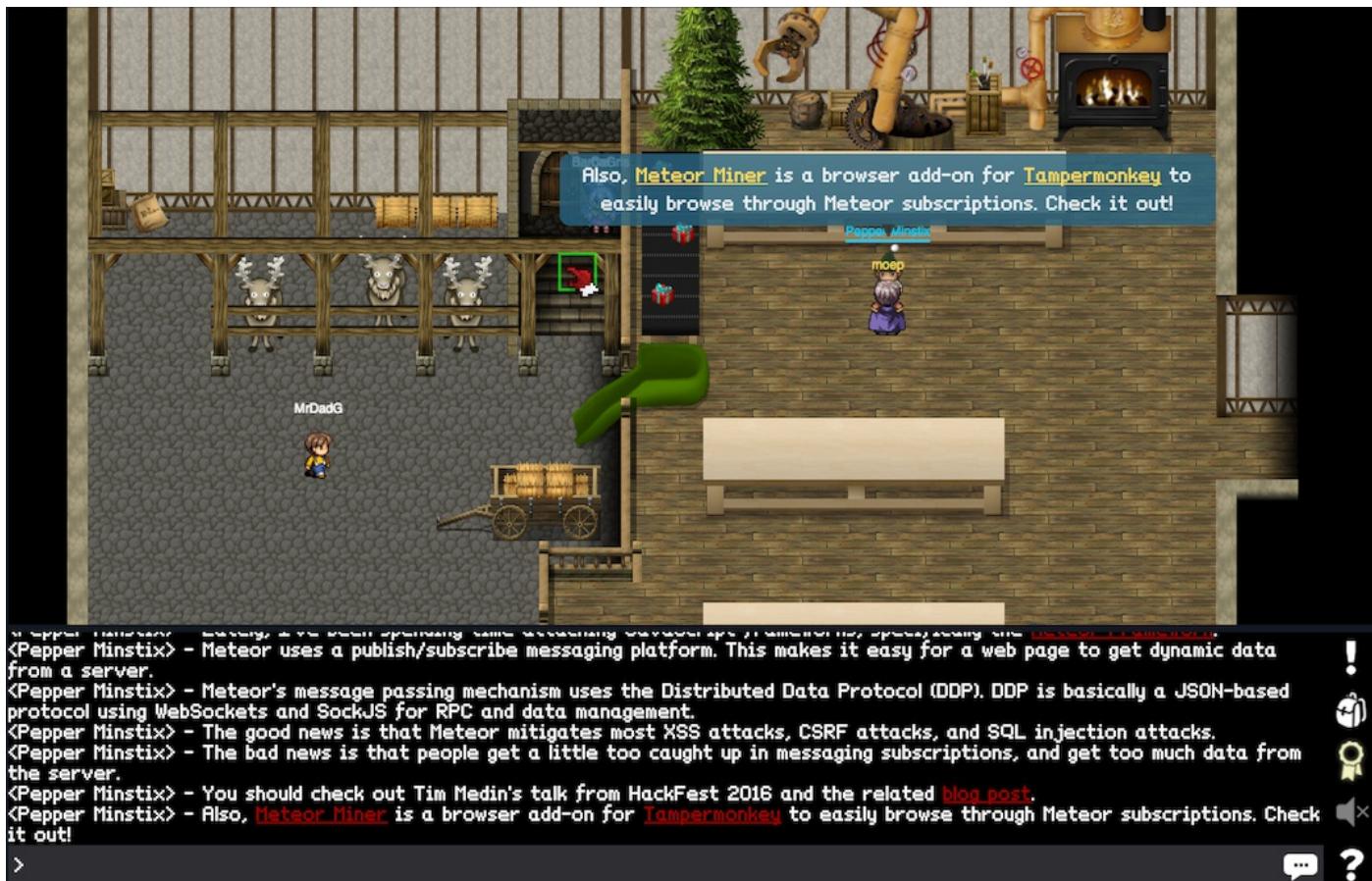
The North Pole

Workshop

>

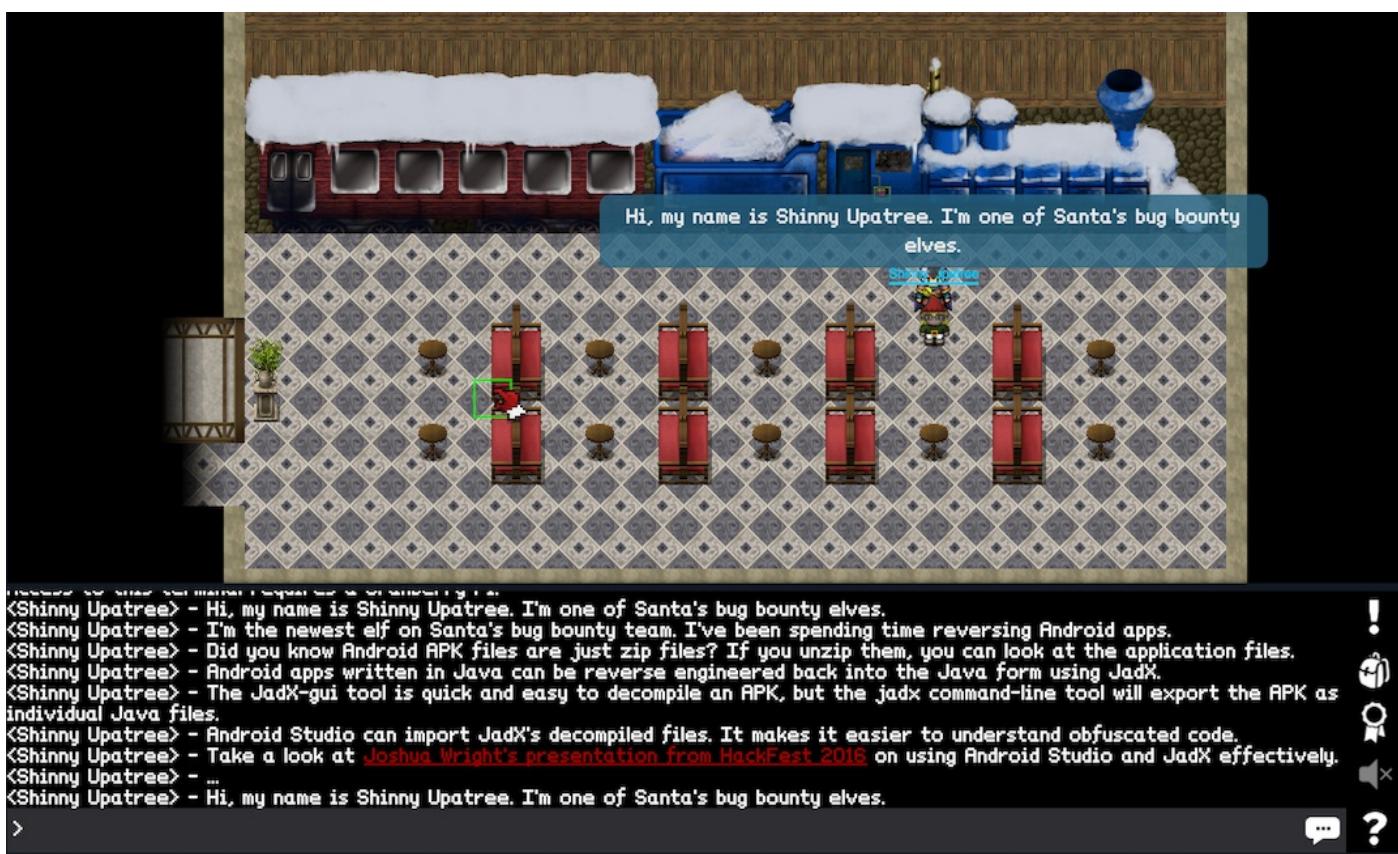


Go back to the center of the room and talk to Pepper Minstix.



He will provide with links to Meteor, SANS training on hacking Meteor, a tool called MetorMiner and to TamperMonkey.

Enter the room on the right.



You cannot interact with the train (as it requires a Cranberry Pi). Talking to Shinny Upatree in the room gives you a link to a .pptx file.

At this point, we decided that we did enough reconnaissance (by actually walking around and talking to NPCs). Let's get back to the very first intel that we gathered. We checked the Twitter account, but we omitted the Instagram account. Let's do that now.

The image shows a Instagram profile for the user 'santawclaus'. The profile picture is a Santa Claus figurine. The bio reads: 'SantaClaus Father Christmas, St Nicholas, Elf Supreme. twitter.com/santawclaus'. Below the profile are three thumbnail images: a laptop screen showing a map, a large illuminated Christmas tree at night, and a snowman standing by a fireplace.

If you look closely on the left most image, you will get two important pieces of intel:

1. The name [www.northpolewonderland.com](http://www.northpolewonderland.com) which is printed on the sheet of paper that show the NMAP scan result.
2. The file name [SantaGram\\_v4.2.zip](http://www.northpolewonderland.com/SantaGram_v4.2.zip)

If you browse to <http://www.northpolewonderland.com/>, you will see Santa's business card again. If you browse to [http://www.northpolewonderland.com/SantaGram\\_v4.2.zip](http://www.northpolewonderland.com/SantaGram_v4.2.zip), you can actually download a file.

We first check what type of file we got:

```
file SantaGram_v4.2.zip
SantaGram_v4.2.zip: Zip archive data, at least v2.0 to extract
```

So it seems to be a ZIP file indeed. However, it has a password on it.

```
unzip SantaGram_v4.2.zip
Archive: SantaGram_v4.2.zip
[SantaGram_v4.2.zip] SantaGram_4.2.apk password:
```

Using the secret message from the tweets as password gives us the content. To be fair, at first I went down a completely different road. I tried to break the ZIP password with John the Ripper. We already got a hint to the [RockYou dictionary](#). In order to get a hash out of the ZIP file that we can crack, Google let us to

<http://www.cybercrimetech.com/2014/07/how-to-cracking-zip-and-rar-protected.html>. Using zip2john , I got the following hash.

```
SantaGram_v4.2.zip:$pkzip2$1*2*3*0*1df34a*2271ee*ede16a54*0*4b*8*1
```

Unfortunately, just throwing john and the rockyou wordlist on the hash did not yield any results. But just calling john hashfile did the trick. It took approximately 20minutes on my MacBook Pro to complete.

But be it as it may - directly using the password from the tweets was likely the intended way to do things :)

Digging further, we can now have a deeper look at the apk file. Earlier, Bushy Evergreen mentioned apktool . Let's give it a try.

```
apktool d SantaGram_4.2.apk
```

This gives us the extracted contents of the file in the folder `SantaGram_4.2`. The next two questions are about contents of the APK file (username/password and the name of the audible component). By browsing the directory structure, we soon found the file `res/raw/discombobulatedaudio1.mp3`. Which seems to be the answer to question 4.

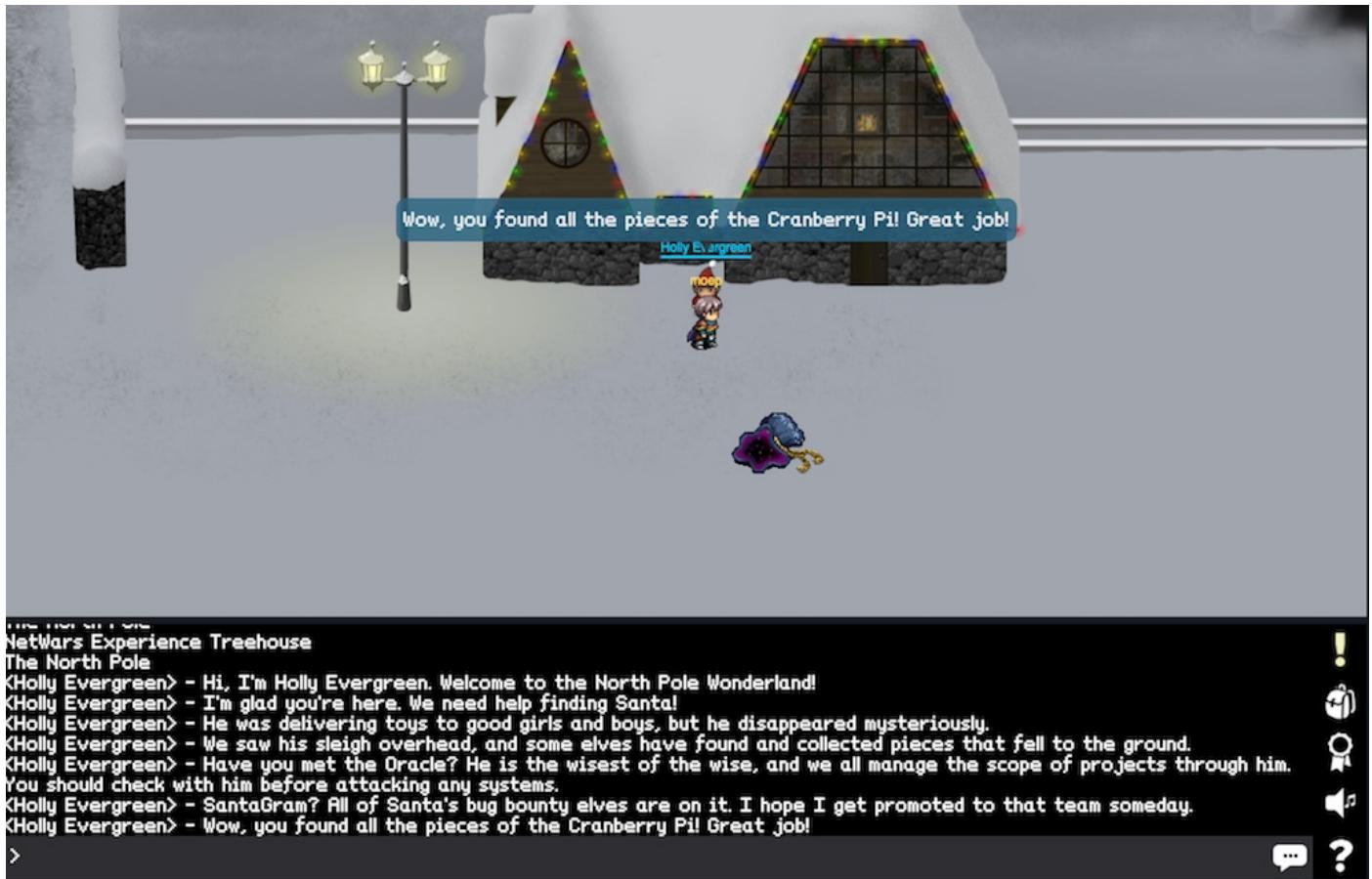
Now for the username and password. We suspected them to be in the code (rather than hidden in some other resources). So we navigated to the folder that contains the `smali` files. We even further navigated to the folder that I guess represents the Java classes that are in the `com.northpolewonderland.santagram` Java package. After that, `grep` did the trick.

In `SantaGram_4.2/smali/com/northpolewonderland/santagram`:

```
grep -C3 -rin "password" .
./b.smali-414-
./b.smali-415-    invoke-virtual {v0, v1, v2}, Lorg/json/JSONObject;
./b.smali-416-
./b.smali:417:    const-string v1, "password"
./b.smali-418-
./b.smali-419-    const-string v2, "busyreindeer78"
./b.smali-420-
-- 
[...]
```

Inspecting the file, we get the next flag: `username=guest`, `password=busyreindeer78`.

Next, we can have a look at the Cranberry Pi. As it turns out, we do have collected all the necessary pieces. We can return the quest to Holly Evergreen (right in front of the first house).



We also get a download link to the [Cranbian image](#). Since the next question is about the username of what seems to be a local account on the Cranbian image, it is a good idea to mount it. Earlier in the game, we already got a link to a [howto](#) for that.

Unfortunately, the `fdisk` utility on OS X does not work the way that is mentioned in the howto. So I had to switch to a Kali VM for the first time during this holiday hack.

```
fdisk -l cranbian-jessie.img
Disk cranbian-jessie.img: 1.3 GiB, 1389363200 bytes, 2713600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disklabel type: dos
Disk identifier: 0x5a7089a1

Device          Boot  Start    End Sectors  Size Id Type
cranbian-jessie.img1      8192  137215  129024   63M  c W95 FAT32
cranbian-jessie.img2      137216 2713599 2576384 1.2G  83 Linux
```

In order to mount the Linux image, we have to calculate the offset in bytes.

```
echo $((512*137216))
70254592
```

And then mount the image.

```
mount -v -o offset=70254592 cranbian-jessie.img mnt/
mount: /dev/loop0 mounted on ... ./mnt
```

Now, a `cat` on the `mnt/etc/shadow` file reveals the password hash for the `cranpi` user.

```
cranpi:$6$2AXLbEoG$zZlWSwrUSD02cm8ncL6pmaYY/39DUai30GfnBbDNjtx2G99
```

This is a pretty strong hash, as `hashid` confirms:

```
hashid cranpi.hash
--File 'cranpi.hash'--
Analyzing '$6$2AXLbEoG$zZlWSwrUSD02cm8ncL6pmaYY/39DUai30GfnBbDNjtx
[+] SHA-512 Crypt
--End of file 'cranpi.hash'
```

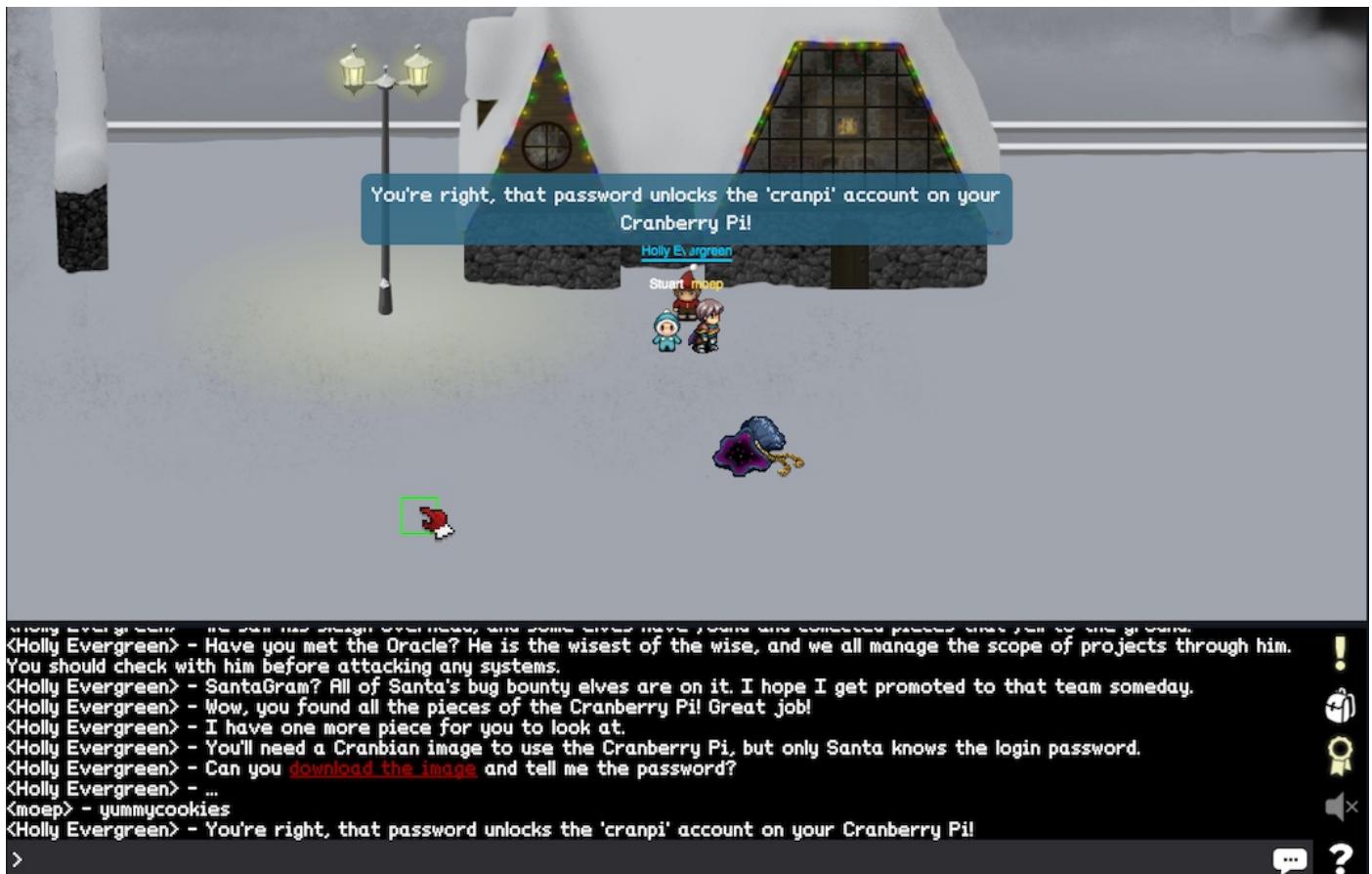
Nevertheless, I gave it a try with John the Ripper and with hashcat. The cracking speed was - well - a desaster: Speed/sec.: 441 plains, 441 words for hashcat. John had a similar speed. All this on an early 2015 MacBook Pro with a 2,7 GHz Intel Core i5. The John the Ripper speed declined however during the course of the cracking. So I stopped the process. It took hashcat 66 minutes to crack the hash, giving us the answer to question 5: yummycookies .

```
$6$2AXLbEoG$zZ1WSwrUSD02cm8ncL6pmaYY/39DUai30GfnBbDNjtx2G99qKbhnid
```

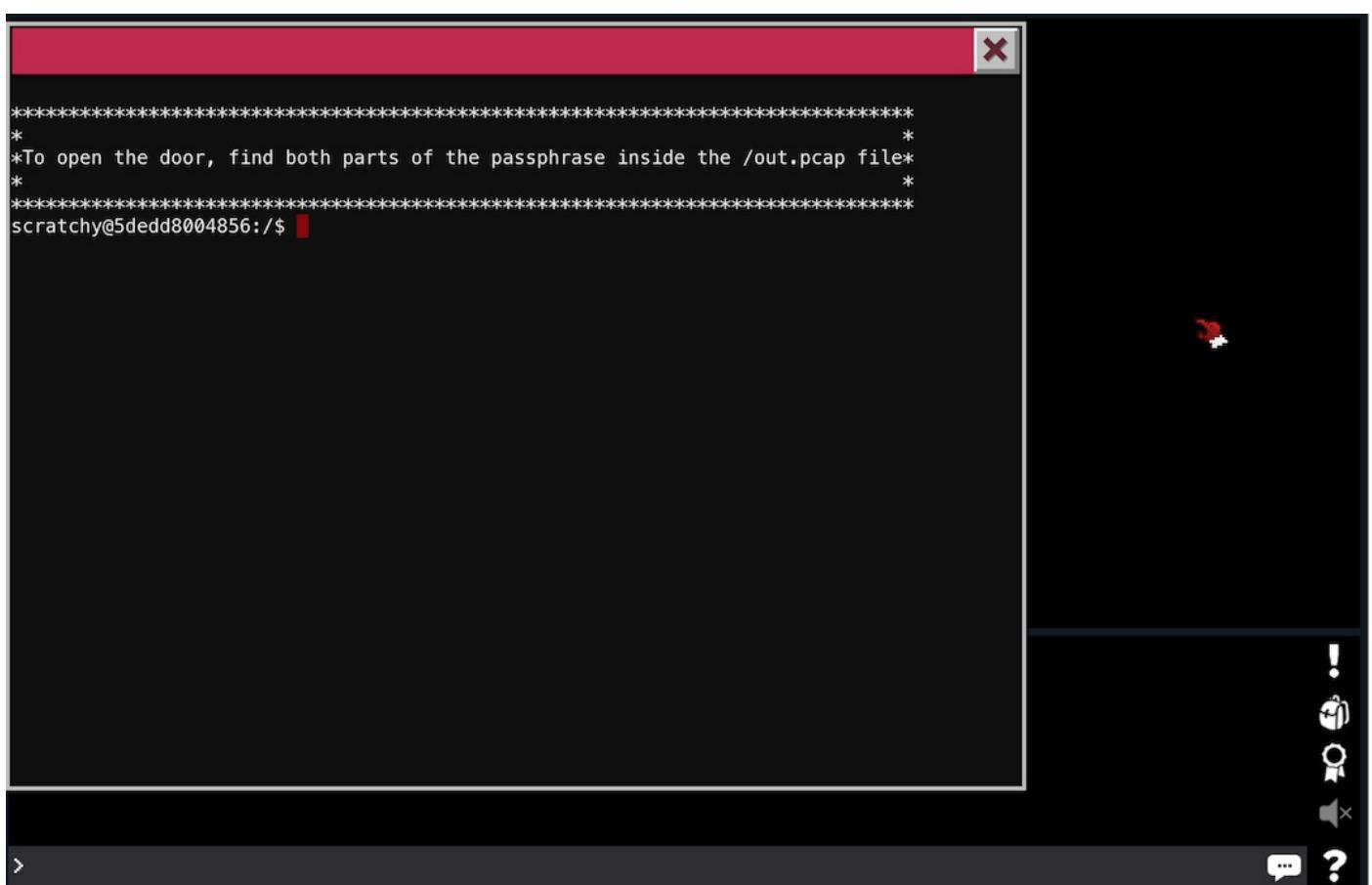
All hashes have been recovered

```
Input.Mode: Dict (02_rockyou.txt)
Index.....: 1/5 (segment), 3627172 (words), 33550343 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 452 words
Progress...: 1814156/3627172 (50.02%)
Running...: 00:01:06:46
Estimated.: 00:01:06:51
```

In order to proceed, you need to tell the password to Holly Evergreen.



With that out of the way, we can use the Cranberry Pi to interact with the terminals. We start at the elf house number 2.



We find ourselves at a terminal, which seems to be a freshly spawned Docker container. The task is to find two parts of a passphrase inside the `/out.pcap` file.

```
scratchy@2a1a07f0bfaa:/$ ls -al out.pcap
-r----- 1 itchy itchy 1087929 Dec  2 15:05 out.pcap
scratchy@2a1a07f0bfaa:/$ id
uid=1001(scratchy) gid=1001(scratchy) groups=1001(scratchy)
scratchy@2a1a07f0bfaa:/$
```

The first obstacle are the file permissions. We are the user `scratchy`, but the file can only be read by the user `itchy`. In such cases, it is a good idea to check `sudo` as well as to look for binaries with the `s-bit` set. `sudo -l` gives us some pretty useful information.

```
scratchy@2a1a07f0bfaa:/$ sudo -l
sudo: unable to resolve host 2a1a07f0bfaa
Matching Defaults entries for scratchy on 2a1a07f0bfaa:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/b
User scratchy may run the following commands on 2a1a07f0bfaa:
    (itchy) NOPASSWD: /usr/sbin/tcpdump
    (itchy) NOPASSWD: /usr/bin/strings
scratchy@2a1a07f0bfaa:/$
```

As user `scratchy`, we are allowed to run the commands `tcpdump` and `strings` as the user `itchy`, without having to authenticate via a password. Perfect. Let's start with `strings`. Since we are operating in a somewhat limited environment (for example there is no `less`), we will print the output to a file and use `vim` to have a look at it.

```
scratchy@2a1a07f0bfaa:/$ sudo -u itchy strings out.pcap >/tmp/out.
```

```
sudo: unable to resolve host 2a1a07f0bfaa
scratchy@2a1a07f0bfaa:/$
```

We see some HTTP traffic. And already in line 32, we get the first half of the passphrase: santas1i . From there on, you could almost guess the full passphrase. But we will do it the hard way and actually look for the second half. Things start to get trickier here, because the second half seems to be hidden in a binary file.

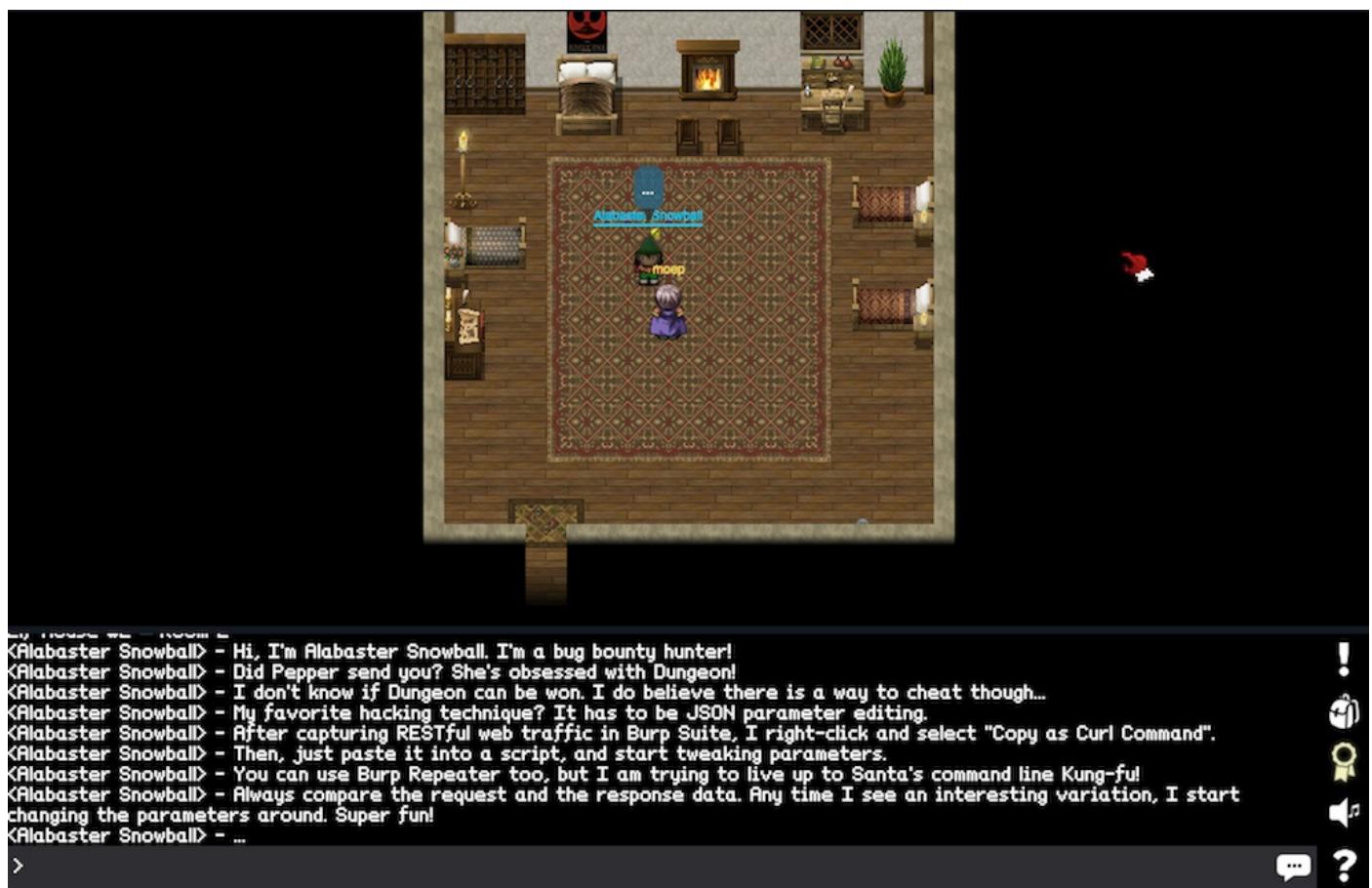
```
DGET /secondhalf.bin HTTP/1.1
User-Agent: Wget/1.17.1 (darwin15.2.0)
Accept: */*
Accept-Encoding: identity
Host: 192.168.188.130
Connection: Keep-Alive
ZAX
THTTP/1.0 200 OK
TServer: SimpleHTTP/0.6 Python/2.7.12+
ZAX"
,#"=X
TDate: Fri, 02 Dec 2016 11:28:00 GMT
Content-type: application/octet-stream
ZAXr
,#o=X
UContent-Length: 1048097
Last-Modified: Fri, 02 Dec 2016 11:26:12 GMT
```

It took me almost 3 hours to get behind that. I struggled with tcpdump for a long time. Trying to extract the binary file for further processing. After I did not make any reasonable progress, I noticed in the chat that another player was having issues with this particular challenge, too. The answer he got was basically: 'Do not overthink it. Read the manpages of your tools. Try harder.' Well - I did :).

I had a look at the `tcpdump` again and noticed that the `User-Agent` suggest the binary was downloaded to an OS X El Capitan system. So maybe the binary file was also compiled for that specific architecture, or maybe another one? Be it as it may, this lead me to look at the manpage for `strings` again, where I noticed that you can specify the encoding with the `-e` option. Since Intel x86 processors use little endian, I started with the respective options. And I got a hit.

```
scratchy@681628e3e251:/ $ sudo -u itchy strings -e l out.pcap
sudo: unable to resolve host 681628e3e251
part2:tittlehelper
```

So the password for the door in the same room is `santaslittlehelper`. Behind the door, you meet Alabaster Snowball.



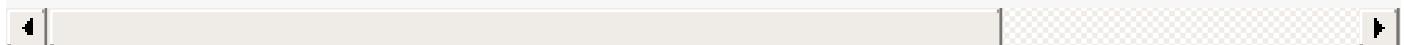
He tells you something about JSON, Burp and how to export request from Burp so that you can directly use them as a `cURL` command on the

shell. Also, he mentions a dungeon (which I apparently have not found yet).

On to the next terminal. This time, the task is '*To open the door, find the passphrase file deep in the directories.*' It is located in the building on the top of the mountain. This was easier than expected. A simple `find` lists all the directories.

```
*****
*
* To open the door, find the passphrase file deep in the directori
*
*****
elf@5f09ad2e85a2:~$ find
.
./.bashrc
./doormat
./doormat/..
./doormat/.. /
./doormat/.. / \\
./doormat/.. / /\ \\
./doormat/.. / /\ \\/Don't Look Here!
./doormat/.. / /\ \\/Don't Look Here!/You are persistent, aren't y
./doormat/.. / /\ \\/Don't Look Here!/You are persistent, aren't y
./doormat/.. / /\ \\/Don't Look Here!/You are persistent, aren't y
.txt
./doormat/.. / /\ \\/Don't Look Here!/You are persistent, aren't y
./doormat/.. / /\ \\/Don't Look Here!/You are persistent, aren't y
./doormat/.. / /\ \\/Don't Look Here!/secret
./doormat/.. / /\ \\/Don't Look Here!/files
./doormat/.. / /\ \\/holiday
./doormat/.. / /\ \\/temp
./doormat/.. / /\santa
./doormat/.. / /\ls
./doormat/.. / /\opt
./doormat/.. / /\var
./doormat/.. /bin
```

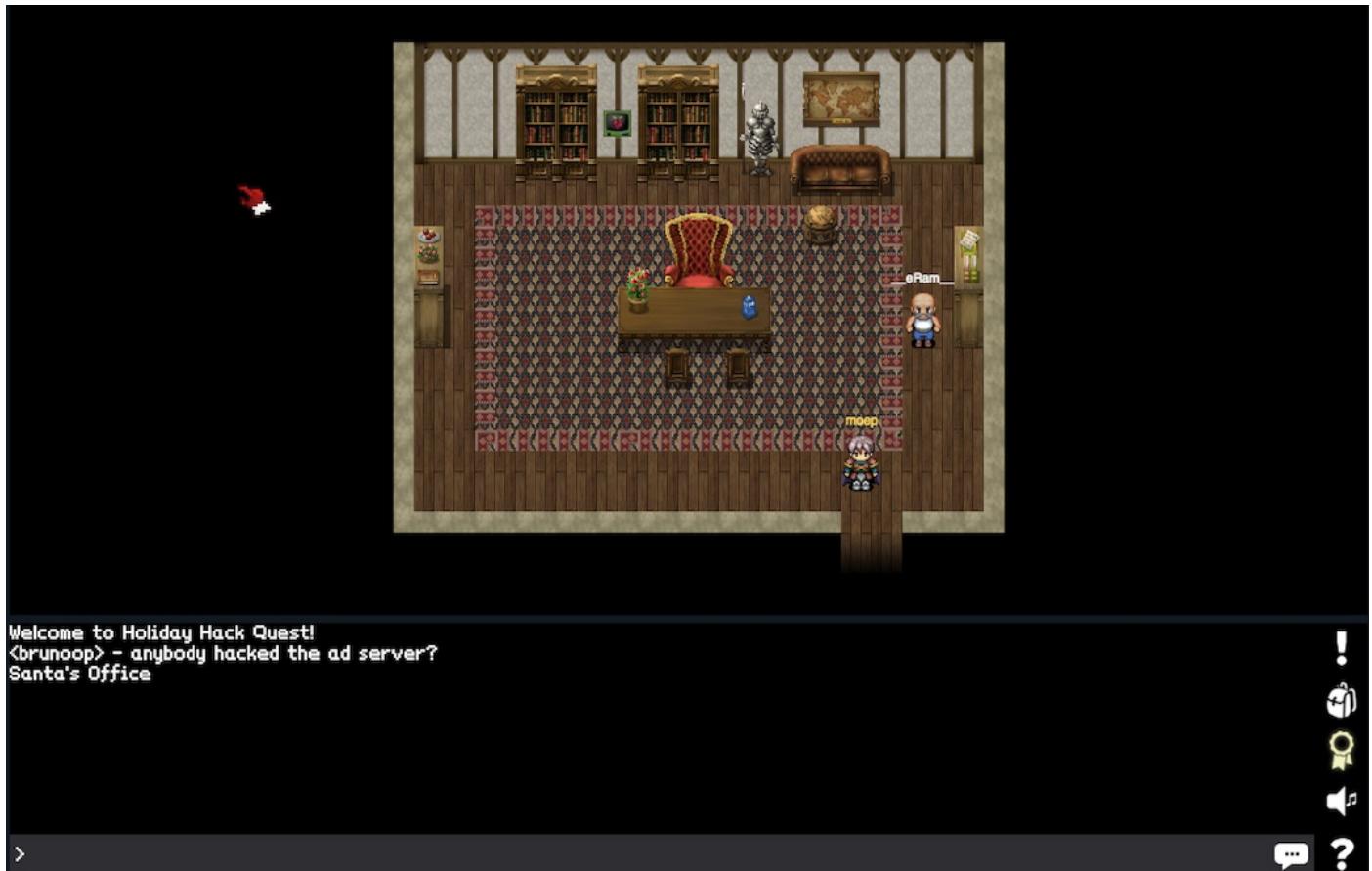
```
./.doormat/. /not_here  
./.doormat/share  
./.doormat/temp  
.var  
.temp  
.profile  
.bash_logout  
elf@5f09ad2e85a2:~$
```



In order to access the file with the password, I choose to use the `print0` option of `find`, so that a binary 0 is used as delimiter (instead of space).

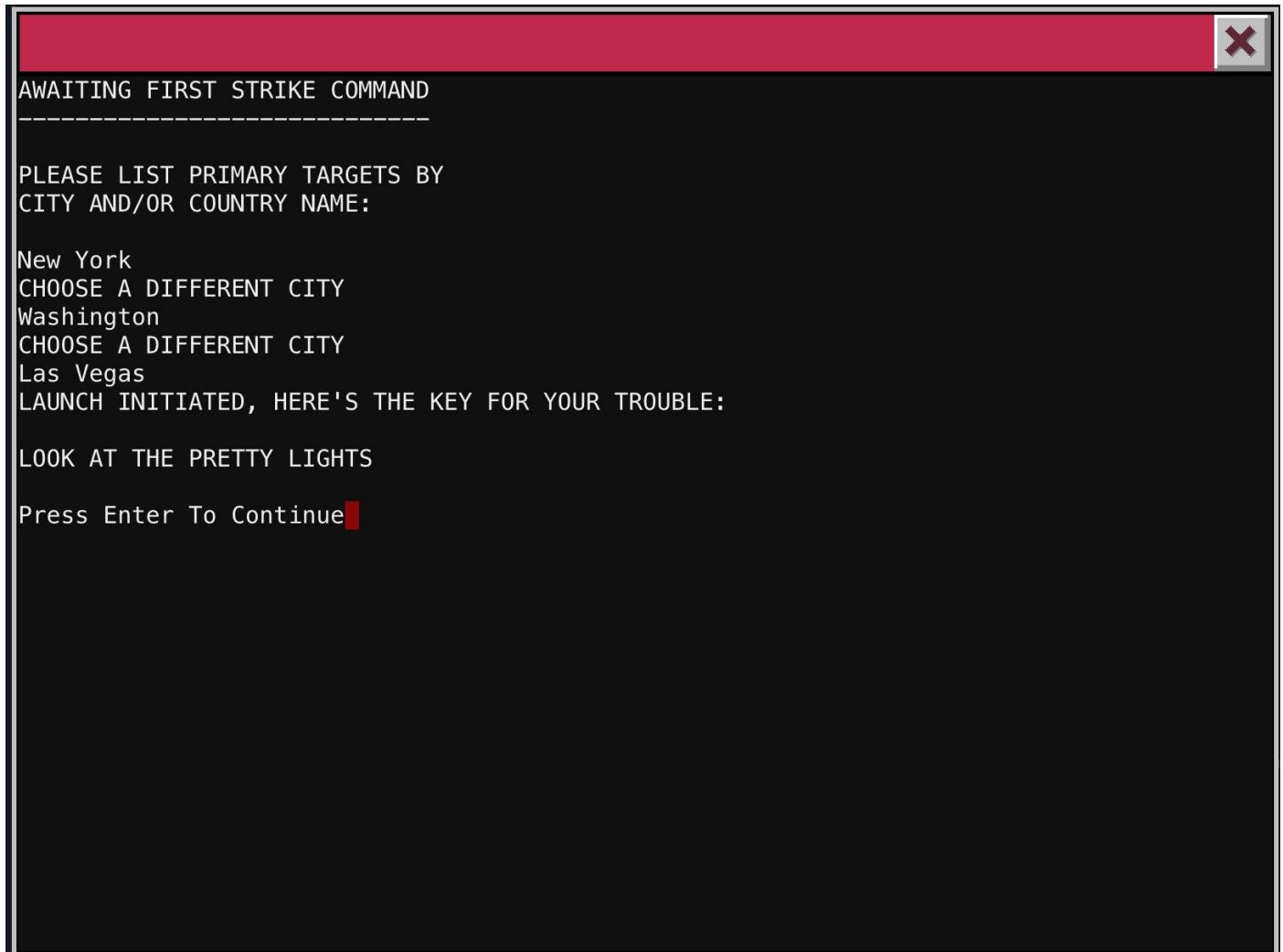
```
elf@5f09ad2e85a2:~$ find . -iname '*for_*' -print0 | xargs -0 cat  
key: open_sesame
```

So the password is `open_sesame`. The reward is access to Santa's office.



In it, there is another terminal. When you interact with it, you can actually

replay a part of the movie Wargames. The challenge here is simply to look up a good [transcript](#) of the movie or to watch the respective [YouTube clips](#).



The flag you get is: `LOOK AT THE PRETTY LIGHTS` .

Back in the workshop, I noticed that there is a second terminal.



```
sudo: unable to resolve host 9447814e2199
*****
* Find the passphrase from the wumpus. Play fair or cheat; it's up to you. *
*****
elf@9447814e2199:~$
```

Start the game `wumpus`. I just played it, until I finally got the Wumpus.  
The passphrase is `WUMPUS IS MISUNDERSTOOD`.

\*whoosh\* (I feel a draft from some pits).  
\*sniff\* (I can smell the evil Wumpus nearby!)  
There are tunnels to rooms 3, 9, and 10.  
Move or shoot? (m-s)

You are in room 6 of the cave, and have 5 arrows left.  
\*whoosh\* (I feel a draft from some pits).  
\*sniff\* (I can smell the evil Wumpus nearby!)  
There are tunnels to rooms 3, 9, and 10.  
Move or shoot? (m-s) s2  
\*thunk\* The arrow can't find a way from 6 to 2 and flies randomly into room 10!

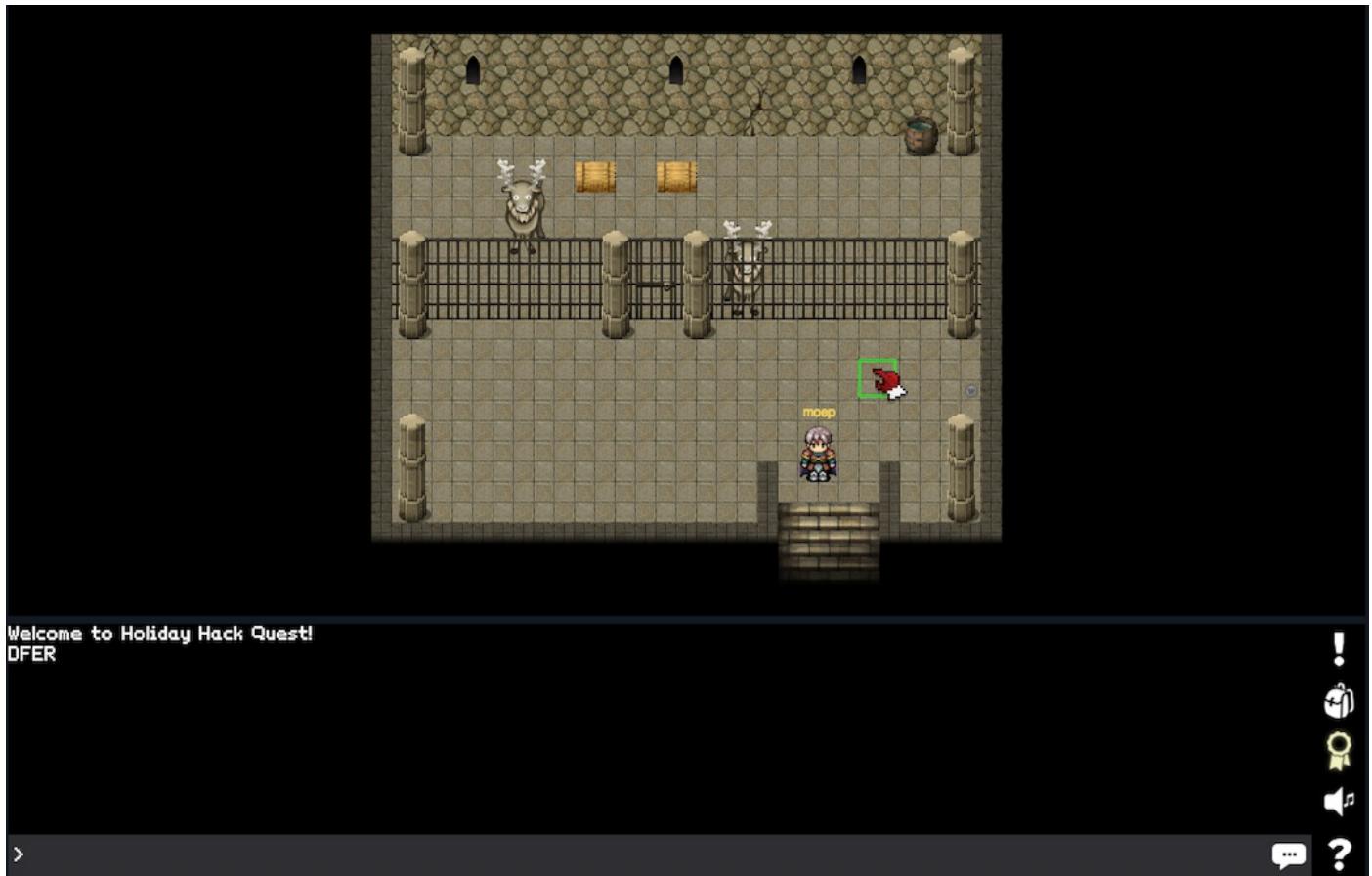
You are in room 6 of the cave, and have 4 arrows left.  
\*whoosh\* (I feel a draft from some pits).  
\*sniff\* (I can smell the evil Wumpus nearby!)  
There are tunnels to rooms 3, 9, and 10.  
Move or shoot? (m-s) s3  
\*thwock!\* \*groan\* \*crash\*

A horrible roar fills the cave, and you realize, with a smile, that you have slain the evil Wumpus and won the game! You don't want to tarry for long, however, because not only is the Wumpus famous, but the stench of dead Wumpus is also quite well known, a stench plenty enough to slay the mightiest adventurer at a single whiff!!

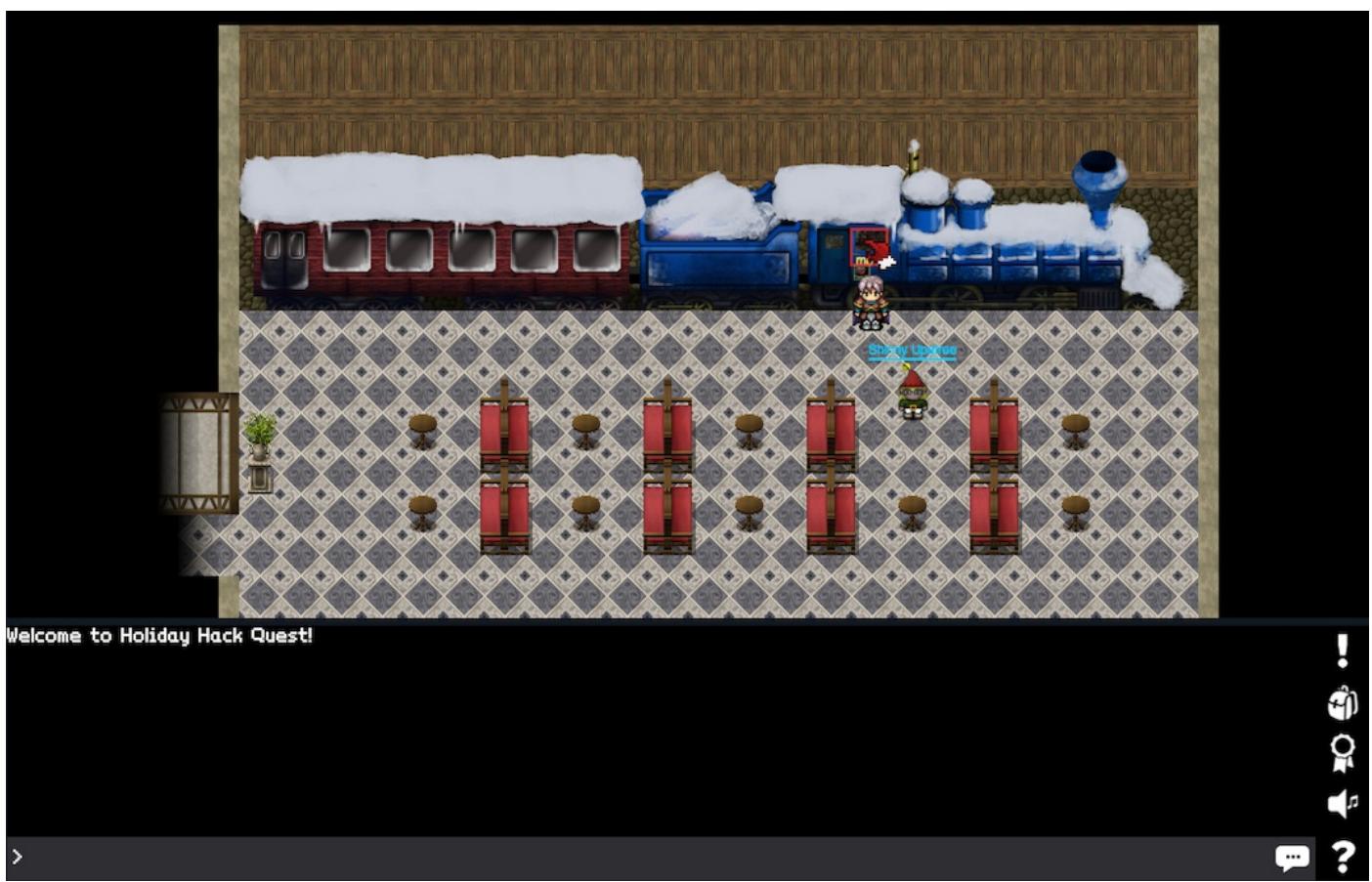
Passphrase:  
WUMPUS IS MISUNDERSTOOD

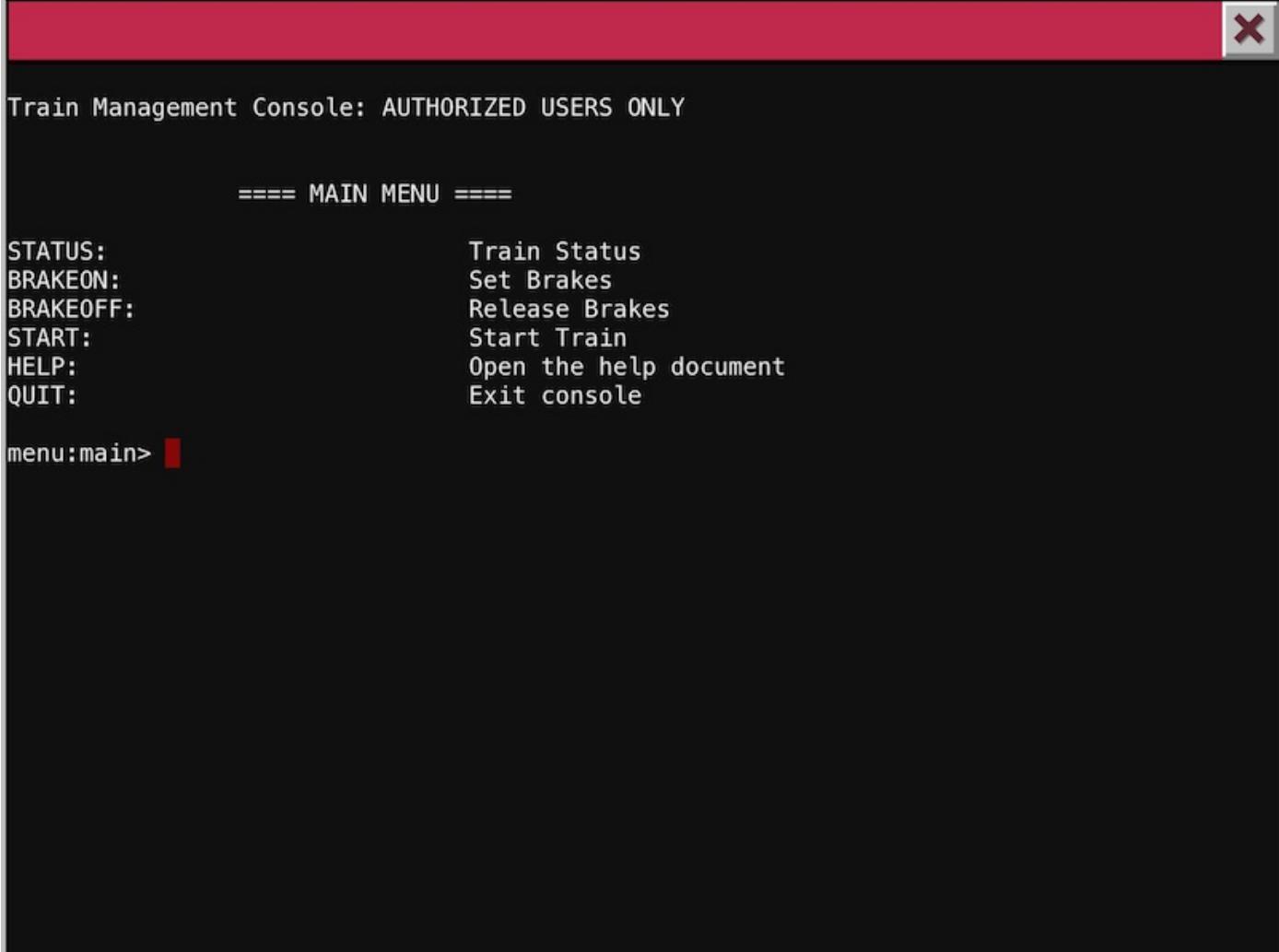
Care to play another game? (y-n) █

With the passphrase, we can pass the door next to the terminal.



Right now, I could not find anything of interest in it. Next, we will check out the terminal at the train.





```
Train Management Console: AUTHORIZED USERS ONLY

===== MAIN MENU =====

STATUS: Train Status
BRAKEON: Set Brakes
BRAKEOFF: Release Brakes
START: Start Train
HELP: Open the help document
QUIT: Exit console

menu:main> █
```

If we set the brakes to off, and then try to start the train, we are asked for a password which we do not know. The hint to make progress is buried in the `HELP` message.

**HELP** brings you to this file. If it's not here, this console cannot do it, unLESS you know something I don't.

So it seems that the `less` command is executed to display the message. Which is neat, cause we can do SHELL commands this way by leveraging the `! <command>` feature of `less` [as described in the mangpage](#). An `ls -al` gives the following.

```
menu:main> HELP
total 40
drwxr-xr-x 2 conductor conductor 4096 Dec 10 19:39 .
drwxr-xr-x 6 root         root      4096 Dec 10 19:39 ..
```

```
-rw-r--r-- 1 conductor conductor 220 Nov 12 2014 .bash_logout
-rw-r--r-- 1 conductor conductor 3515 Nov 12 2014 .bashrc
-rw-r--r-- 1 conductor conductor 675 Nov 12 2014 .profile
-rwxr-xr-x 1 root      root     10528 Dec 10 19:36 ActivateTrain
-rw-r--r-- 1 root      root     1506 Dec 10 19:36 TrainHelper.tx
-rwxr-xr-x 1 root      root     1588 Dec 10 19:36 Train_Console
!done (press RETURN)
```

We get the password by doing a `grep -in pass Train_Console`.

```
menu:main> HELP
7:PASS="24fb3e89ce2aa0ea422c3d511d40dd84"
72:                      read -s -p "Enter Password: " pass
73:                      [ "$password" == "$PASS" ] && QUES
ivateTrain || echo "Access denied"
!done (press RETURN)
```

And off we go, back in time to 1978.



MONTH	DAY	YEAR	HOUR	MIN
NOV	16	1978	0 AM	+ : + + +
				10   :   21
			X PM	+ + + + +

DESTINATION TIME

MONTH	DAY	YEAR	HOUR	MIN
JAN	04	2017	X AM	+ + + + +
				11   :   23
			0 PM	+ + + + +

PRESENT TIME

MONTH	DAY	YEAR	HOUR	MIN
NOV	16	1978	0 AM	+ + + + +
				10   :   21
			X PM	+ + + + +

LAST TIME DEPARTED

DISCONNECT CAPACITOR DRIVE  
BEFORE OPENING

+-----+

+XX XX+

|XXX XXX|

++ XXX XXX +-+

XXX XXX

XXXXX

XXX

XXX

XXX

SHIELD EYES FROM LIGHT

XXX

XX+-+

+-----+

|ACTIVATE!|

+-----+

Press Enter to initiate time travel sequence.



							SHIELD EYES FROM LIGHT
							XXX
							XX++
MONTH	DAY	YEAR	HOUR	MIN			
+-----+ +-----+ +-----+   0 AM +-----+ +-----+							
NOV     16     1978     10   :   21							
+-----+ +-----+ +-----+   X PM +-----+ +-----+							
LAST TIME DEPARTED							+-----+  ACTIVATE!  +-----+

Press Enter to initiate time travel sequence.

-->Activating TIME TRAVEL sequence NOW.....

\*\*\*\*\* TIME TRAVEL TO 1978 SUCCESSFUL! \*\*\*\*\*

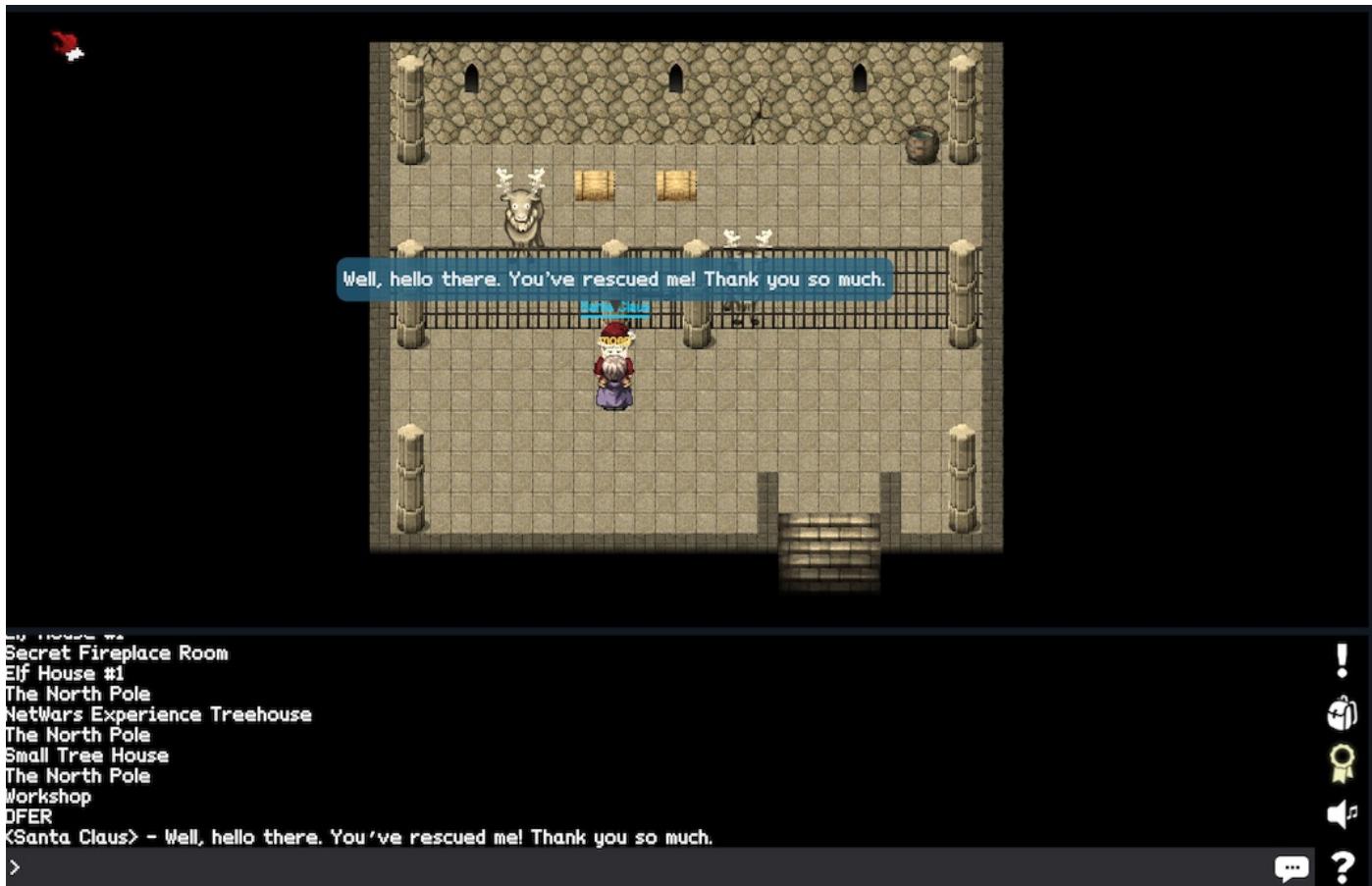
===== MAIN MENU =====

STATUS:	Train Status
BRAKEON:	Set Brakes
BRAKEOFF:	Release Brakes
START:	Start Train
HELP:	Open the help document
QUIT:	Exit console

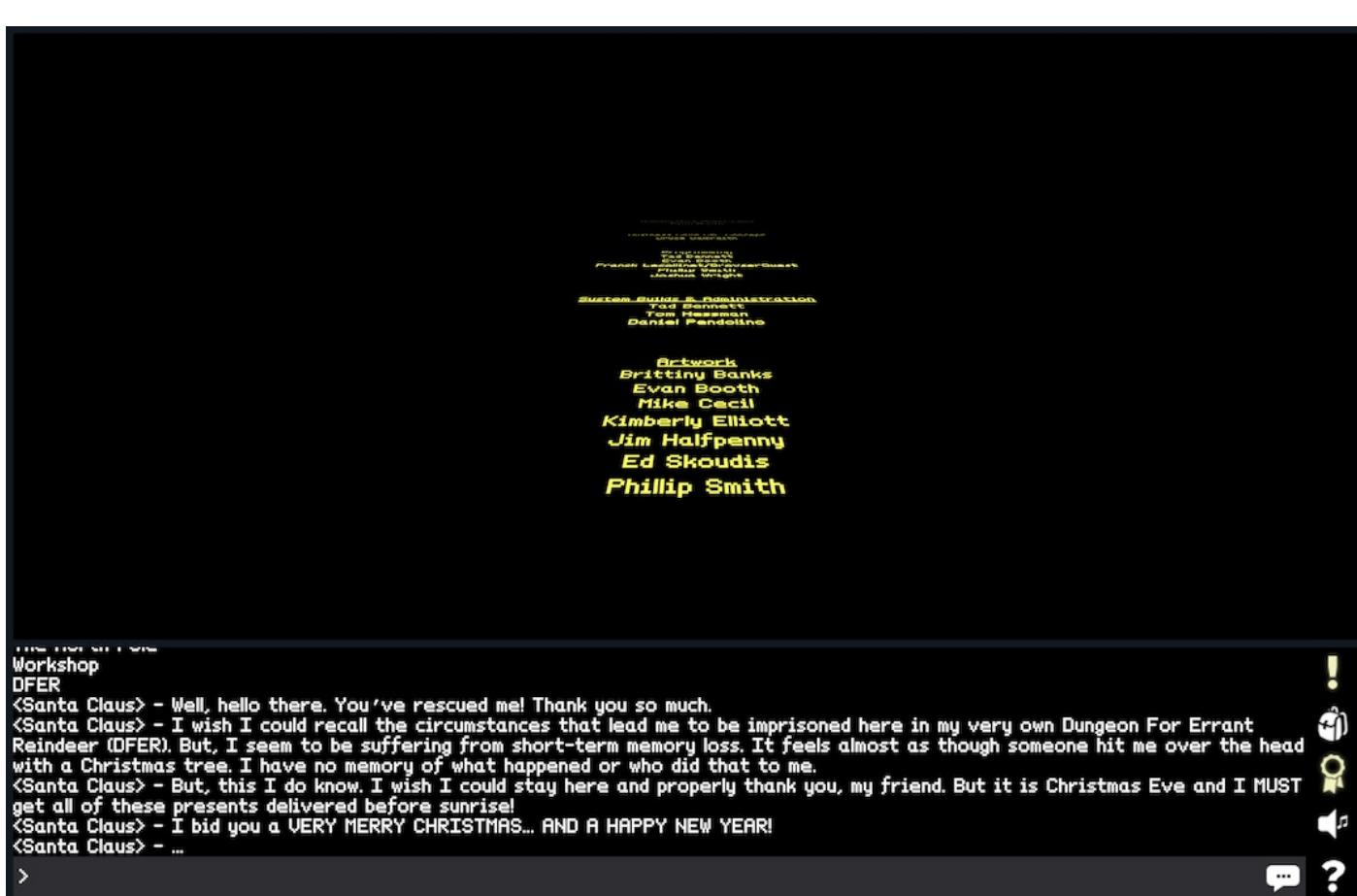
menu:main> █

&token=335BC464-BB2C-11E6-A4A6-CEC0C932CE01 10.240.0.19

While searching the place, you will finally find Santa in the back room of the train station.



Plus - see some credits.



Unfortunately, he does not remember who kidnapped him. In order to

tackle questions 7 and 8, we have to have a look at the SantaGram app again (as clearly point out in the story text on the website). Going through the decompiled app, searching for URLs lead me to the file

```
./res/values/strings.xml .
```

```
<string name="analytics_launch_url">https://analytics.northpolewonderland.com</string>
<string name="analytics_usage_url">https://analytics.northpolewonderland.com</string>
<string name="appVersion">4.2</string>
<string name="app_name">SantaGram</string>
<string name="appbar_scrolling_view_behavior">android.support.design.widget.AppBarLayout$ScrollingViewBehavior</string>
<string name="banner_ad_url">http://ads.northpolewonderland.com/af</string>
<string name="bottom_sheet_behavior">android.support.design.widget.BottomSheetBehavior</string>
<string name="character_counter_pattern">%1$d / %2$d</string>
<string name="debug_data_collection_url">http://dev.northpolewonderland.com/debug</string>
<string name="debug_data_enabled">false</string>
<string name="dungeon_url">http://dungeon.northpolewonderland.com</string>
<string name="exhandler_url">http://ex.northpolewonderland.com/ex</string>
<string name="title_activity_comments">Comments</string>
```

Which gave us some new targets to attack.

```
→ SantaGram_4.2 git:(master) ✘ dig +short analytics.northpolewonderland
104.198.252.157
→ SantaGram_4.2 git:(master) ✘ dig +short ads.northpolewonderland
104.198.221.240
→ SantaGram_4.2 git:(master) ✘ dig +short dev.northpolewonderland
35.184.63.245
→ SantaGram_4.2 git:(master) ✘ dig +short dungeon.northpolewonderland
35.184.47.139
→ SantaGram_4.2 git:(master) ✘ dig +short ex.northpolewonderland.
104.154.196.33
```

After checking each of the IP address with the oracle (Tom Hessman),

we had the permission to test.

## analytics.northpolewonderland.com

### 104.198.252.157

```
nmap 104.198.252.157 --script=default
```

```
Starting Nmap 7.31 ( https://nmap.org ) at 2017-01-04 13:55 CET
Nmap scan report for 157.252.198.104.bc.googleusercontent.com (104.198.252.157)
Host is up (0.13s latency).

Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 5d:5c:37:9c:67:c2:40:94:b0:0c:80:63:d4:ea:80:ae (DSA)
|   2048 f2:25:e1:9f:ff:fd:e3:6e:94:c6:76:fb:71:01:e3:eb (RSA)
|_  256 4c:04:e4:25:7f:a1:0b:8c:12:3c:58:32:0f:dc:51:bd (ECDSA)

443/tcp  open  https
| http-git:
|   104.198.252.157:443/.git/
|     Git repository found!
|       Repository description: Unnamed repository; edit this file !
|_    Last commit message: Finishing touches (style, css, etc)

| http-title: Sprusage Usage Reporter!
|_Requested resource was login.php
| ssl-cert: Subject: commonName=analytics.northpolewonderland.com
| Subject Alternative Name: DNS:analytics.northpolewonderland.com
| Not valid before: 2016-12-07T17:35:00
|_Not valid after: 2017-03-07T17:35:00
|_ssl-date: TLS randomness does not represent time
| tls-nextprotoneg:
|_  http/1.1

Nmap done: 1 IP address (1 host up) scanned in 15.29 seconds
```

It now started to become juicy. After all, we got a full blown git repo! But - well I was running out of time. So I had to stop here. *sadface*

Thanks to you for the entertaining challenge.

## Part 1: A Most Curious Business Card

---

**1) What is the secret message in Santa's tweets?**

BUGBOUNTY

**2) What is inside the ZIP file distributed by Santa's team?**

A file named `SantaGram_4.2.apk`.

## Part 2: Awesome Package Konveyance

---

**3) What username and password are embedded in the APK file?**

```
username=guest  
password=busyreindeer78
```

**4) What is the name of the audible component (audio file) in the SantaGram APK**

file?

discombobulatedaudio1.mp3

## Part 3: A Fresh-Baked Holiday Pi

---

**5) What is the password for the "cranpi" account on the Cranberry Pi system?**

yummycookies

**6) How did you open each terminal door and where had the villain imprisoned Santa?**

- Terminal in Elf House 2
  - Realize via `sudo -l` that you can do `tcpdump` and `strings` as user `itchy`
  - A simple `strings` call gives you part 1: `santasli`
  - A `strings` call with `-e 1` (for 16bit little endian) gives you part 2: `ttlehelper`
  - `tcpdump` helps to understand what traffic was captured and gives you a hint to the endianess thing
- Terminal 1 in the Workshop
  - Do a `find` to learn the directory structure
  - Do `find . -iname '*for_*' -print0 | xargs -0 cat` to access the password
- Terminal 2 in the Workshop

- I literally just played the Wumpus game.
- Terminal Santa's Office
  - Use a transcript of Wargames / YouTube to give the correct answers

## **Part 4: My Gosh... It's Full of Holes**

---

**7) ONCE YOU GET APPROVAL OF GIVEN IN-SCOPE TARGET IP ADDRESSES FROM TOM HESSMAN AT THE NORTH POLE, ATTEMPT TO REMOTELY EXPLOIT EACH OF THE FOLLOWING TARGETS:**

The Mobile Analytics Server (via credentialled login access) The Dungeon Game The Debug Server The Banner Ad Server The Uncaught Exception Handler Server The Mobile Analytics Server (post authentication) For each of those six items, which vulnerabilities did you discover and exploit?

REMEMBER, YOU ARE AUTHORIZED TO ATTACK ONLY THE IP ADDRESSES THAT TOM HESSMAN IN THE NORTH POLE EXPLICITLY ACKNOWLEDGES AS "IN SCOPE." ATTACK NO OTHER SYSTEMS ASSOCIATED WITH THE HOLIDAY HACK CHALLENGE.

**8) What are the names of the audio files you discovered from each system above? There are a total of SEVEN audio files (one from the**

**original APK in Question 4, plus one for each of the six items in the bullet list above.)**

Please note: Although each system is remotely exploitable, we DO NOT expect every participant to compromise every element of the SantaGram infrastructure. Gain access to the ones you can. Although we will give special consideration to entries that successfully compromise all six vulnerabilities and retrieve their audio files, we happily accept partial answers and point out that they too are eligible for any of the prizes.