Challenge: Is sophisticated Russian answering machine...

The challenge will take the user through clues that include the BSides Orlando 2017 t-shirt, PasteBin links with Base64 encoded text, an auto responding email address with an encrypted message, a poorly placed key pair, and a corporate phone number that leads to strange DTMF tones.

Step 1. T-Shirt

The text to the side of the BSides Orlando t-shirt points, when translated, to a PasteBin link. Even if the text can't be translated searching Google for HAKCcPjz will find the PasteBin link.

This can be done with Google Translate on a phone by taking a picture and highlighting the text.

Вы делаете халтуру, товарищ?

(Fun Fact: Google translate will translate the below to "You do hack, comrade?" or “You are doing a hack, comrade?” However when translated by someone fluent in Russian it reads, "You do crappy job, comrade?"

р а с т е б я н HAKCcPjz

The second part of the text translates from Cyrillic to

p a s t e b i n HAKCcPjz"

Since PasteBin or Paste Bin does not translate properly the letters were spaced out.

The second part is the PasteBin shortlink and just this part can be used to search Google and locate the next part of the challenge.

Step 2. First Base64 Encoded PasteBin - Who is comrade?

The PasteBin link (http://pastebin.com/HAKCcPjz) will lead you to a paste titled: Считаете ли вы, что вы ищете?

The title roughly translates to “Do you think that you are looking for?”

The text of the PasteBin link is base64 for encoded.

V2UgYXJlIGdsYWQgeW91IGZvdW5kIHVzLCBjb21
yYWRlLiBUYWtlIHRoZSBuZXh0IHN0ZXAuIA0KR
mluZCBvdXIgcHVibGljIGtleSBhbmQgZW1haWwgd
XMgdG8gcmVjZWl2ZSBmdXJ0aGVyIGluc3RydWN
0aW9ucy4gDQpjb21yYWRlQGJzaWRlc29ybGFuZG
8ub3Jn

The CTF team can use any Base64 decoding tool. To test we used https://www.base64decode.org/

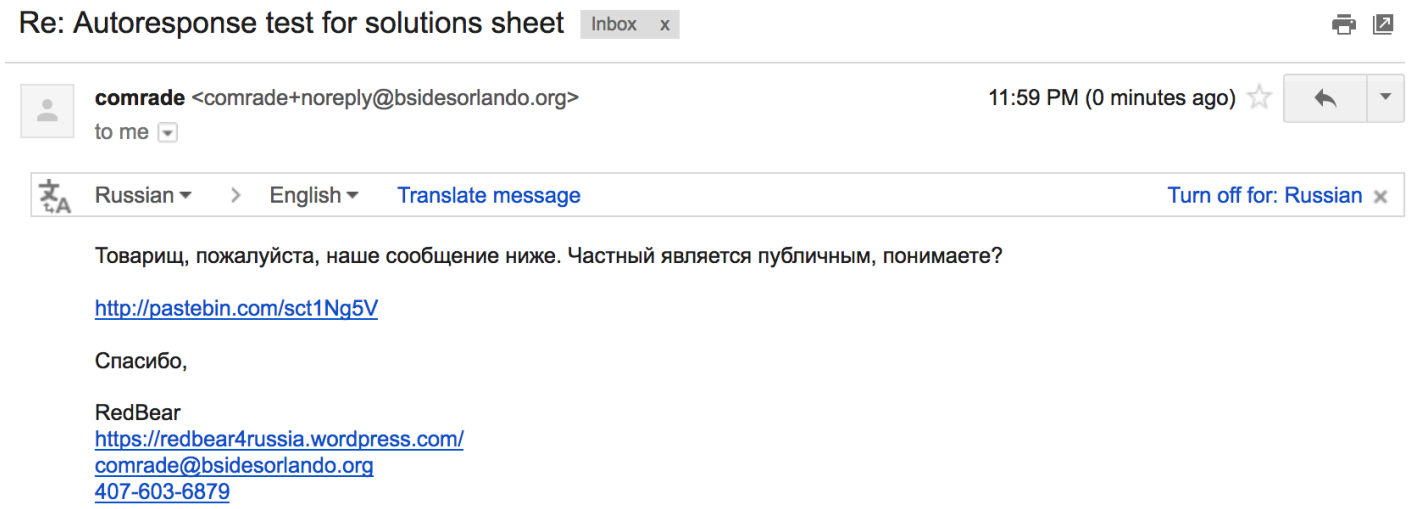
After decoding they will get this text:

> *We are glad you found us, comrade. Take the next step.*
> *Find our public key and email us to receive further instructions.*
> *comrade@bsidesorlando.org*

Challenge 3: Email RedBear

This is a bit of deception based on misconfiguration. The public key is not on any key ring site.

However, if they try emailing the address they will get a response back via an auto responder. There is a new PasteBin link and some clues.

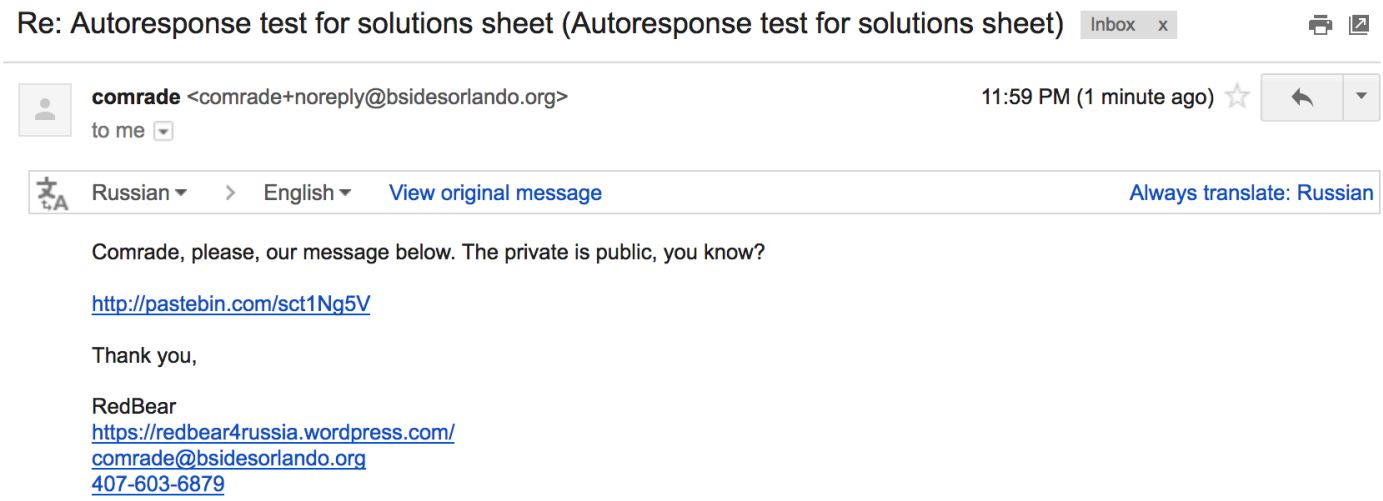


> *Товарищ, пожалуйста, наше сообщение ниже. Частный является публичным, понимаете?*
>
> http://pastebin.com/sct1Ng5V

Спасибо,

RedBear
https://redbear4russia.wordpress.com/
comrade@bsidesorlando.org
407-603-6879

When Translated:



Challenge 4: Keys and Codes and Clues

Challenge four is where some sleuthing comes in. The CTF team will need to look at the email signature and explore each link.

Clues in the email signature they receive when Comrade responds to their email –

- Google translate for Товарищ, пожалуйста, наше сообщение ниже. Частный является публичным, понимаете? becomes "Comrade, please, our message is below. Private is public, you know?"
    - This should give them a hint later when they are looking for the keys associated with comrade@bsidesorlando.org

- http://pastebin.com/sct1Ng5V has the block of PGP encrypted text that contains the flag.

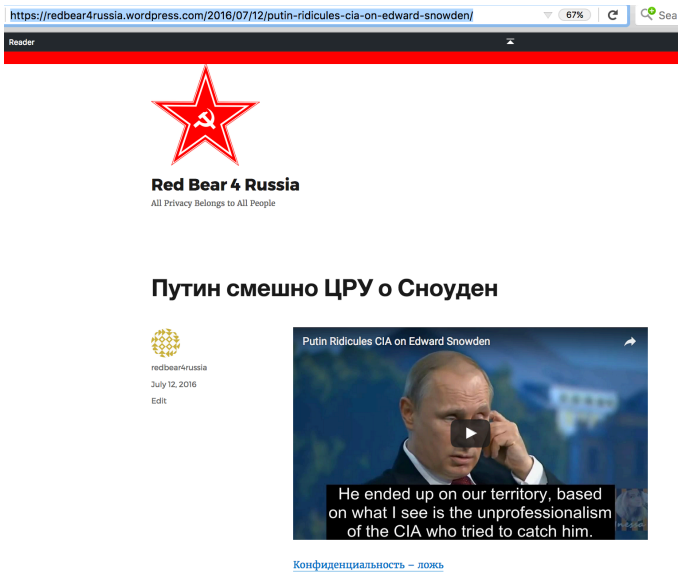
    -----BEGIN PGP MESSAGE-----

    hQIMAzz46AGKDB26ARAAw/MTugTyzyIxkizI5vQQA8+Zld33PYIlSGI9z5wV6boI
    G2PkB5y73UdinBPCzjIzX+k5Gzbq1zjFLDxgT9Fk26ea9O9MDDul5TW82cXcYG+r
    aVm1XTWDDVLZ9VCt6CENdCoJpsQ4nrBD9KO76uGuiQUPCfjjub/gmS+uRTWu/45c

Q5AKIhnwe+UESbPUw+xOl5SiyQcVUjf/8PnD6biwimRi8dN72bXU9/VHNhJ8sNX5
o7Z0AUpmGxfhhxPjL8luC4cFxi9/f/4DSVNcqUsfYb29dq5R9C1LmebpZjIvyzUC
mEeOdw/iNSuHgS+j8CLSrwx2GTSeuLZd+blM9KS/QXlBNXtWf9uRQDmtByBC+SSL
k6Gey9rTbflrOw2AjxPwR8if4U0UiB4b7EVFhEJz1p1/Ihwk+Q3zuDiA6P5LFM8y
VKiZWSvnW2bQ0noLMolQXdkEz1qsLEsqHPjfJiFe7+bCowOypg8M84U3W169Uq/v
N2WKhrCzUzItb0n6zWuCFmRUHRnT7+k/xzZwPa3NkfSdFLq5Kz48bPkbiI70BPpW
QlVcsnhDhkoM7u/fKbChVq0YIB4xWLOkOV9oDvj3qaWsF60bm04phjXcU9kdRi3Z
Fm7qE1s6fnWsyAD8s+0rOO1HK1w1SZ/ZGwS6G2bumDC9ssqOu/xFOPvmYjo+Be3S
6QGtYogeXZYZn6PDcPtKNG8dmD2AGBIyVRKYM1pIWXAfqBr+J1qYRPlPqzVAXE1z
8hTABE0V+SxOwk+qV2/tp4nINCv3/2UHNUChWc06thFMMjLqeXoIrFjyPFnVzOSS
WFl/6m9mzd9M77Kpq9EEKNF9BD0PjljObzSBBE+noURMn2NyU6wPdhQM2MUXtPdP
zQOGdZ/aX2KEBjEmAwhsdhlwf3nXhsL577C+rP8E2MMPiSSId9ds47mf1hnjI9np
6FRJxn80MFBmrue9tIkwI8K+0qxhPApPz2IA7Fbz/lAmEVtzOOqtIQVq2PkHgVhD
AWin5IZOrLD3kcxItGxsnEZD2WT/qceYIpw3mvjBshAw7IrVh29OOB5ffBKENj+9
KwWRRCpaifgoWvoKaeJV24LC082ZFad4wuhGHUisu0gco+wDgBswqyWpYb25NwHy
KLZCqXr1rcGnKVIuNhSrzpRRZqNcL8FRVWMlRhcqvskIsvMKXV+843kv2Ap2u7W2
5lFQfKEGJ21CLMvNAg+B6q2LeYmPpZ6DMnVNvwnV6CBQJ39w7SCeLRFd1FVz0tQj
Pa7iE0Pi9O7p025CHrY80nhgqjGuiOANE38vgv9UGN5kpJXAAl3LqYpX/vap3YCc
G9zCfywe/xBfvMJFV4CkeNEQDB6ba3Tqiu9Rzv4B9nAgwDhEI5DRyYK9rpdPQZyR
WncK0rt8kOm33lPGE8b1YNq/bWCtYof1SXagKGpITvUWSE9gWsDODSY4SNZB7utZ
bCyhKCPNiW44TrgDm2fJz6Ymcp8VdkBhVG/QZNLBn0xOfgNoU/4HtjZ2TmxCt2AH
KyT76rZorLIGyLqlSUP4Wg2OUT6PQ6MxWI/zjTkKK+rtiDoWTRYWhvVV0fpN11WG
qOl4HuUYB1k/2Eg7z3YqTO7+li/zcunIusEDOSbXlSyfJVNfPM5EI3V+D+IP+uXk
XG5sCpuXnk2Hw2fRK6L6/EnrhnlC6DAjudSleEUUDKj3YjitF7L+YUR9lQ==
=umxR
-----END PGP MESSAGE-----

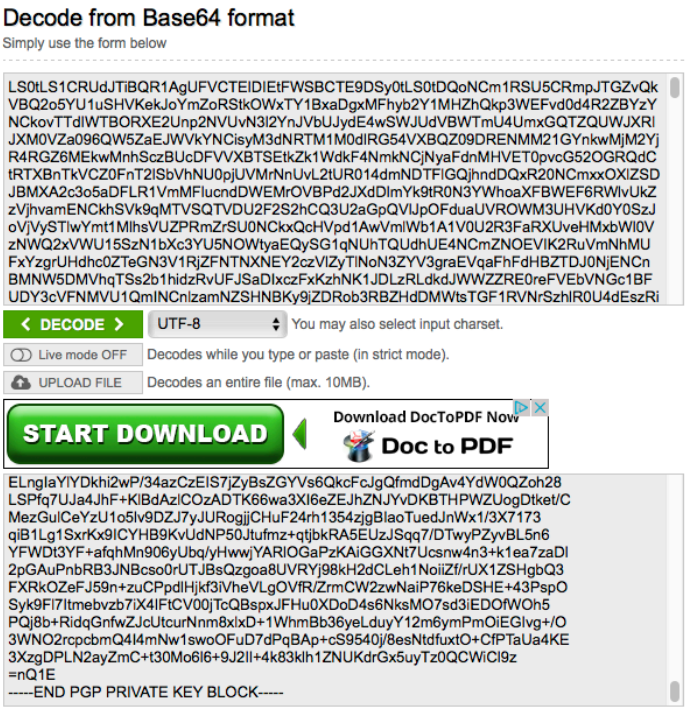
They will need to find the private key, not the public, and the password to decrypt the message.

The flag is in this message.



- https://redbear4russia.wordpress.com is a blog setup for the challenge.
  - It has a number of distraction channel style posts back dated for a few years.
  - The blog subtitle is “All Privacy Belongs to All People” further referencing privacy issues.
  - There are only 20 posts so it isn’t hard to review.
  - However, this post has an extra link - https://redbear4russia.wordpress.com/2016/07/12/putin-ridicules-cia-on-edward-snowden/

- This post is a clue as it is the only one that talks about Snowden, it is the only one with an additional link, and when translated it says “Confidentiality is a lie” this is the same type of riddle like messaging from the email about “Private being Public”
- When they click on the link they get this PasteBin link: http://pastebin.com/BjkiX0gf
- That is also base64 encoded.
- Decoding that text using https://www.base64decode.org/ will get you the public and private key pair for comrade@bsidesorlando.org
- All that is left to find the private key password.



- The phone number 407-603-6879 is for redprox.com (red is obviously a theme). When they call the number they will hear some audio that will move them on to the next challenge.

At this point the CTF team has the PGP message containing the flag and the public/private key pair to decrypt it. However, they do not have the password. The phone number in RedBears email signature will lead them to that.

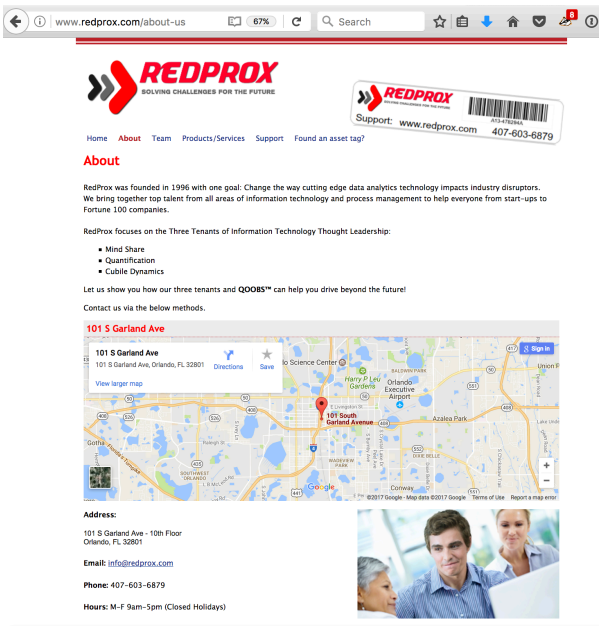
Challenge 5: RedBear’s Voicemail – Clues to lead to message with DTMF

When they call 407-603-6879 they will hear a man with a Russian accent giving them further instructions.

- They will be told to go to www.redprox.com
- He will say, “Find picture. Franco’s brother. Help woman. Is very helpful little man. Ask him what you need to know.”

If they look around on redprox.com they will find this page: http://www.redprox.com/about-us

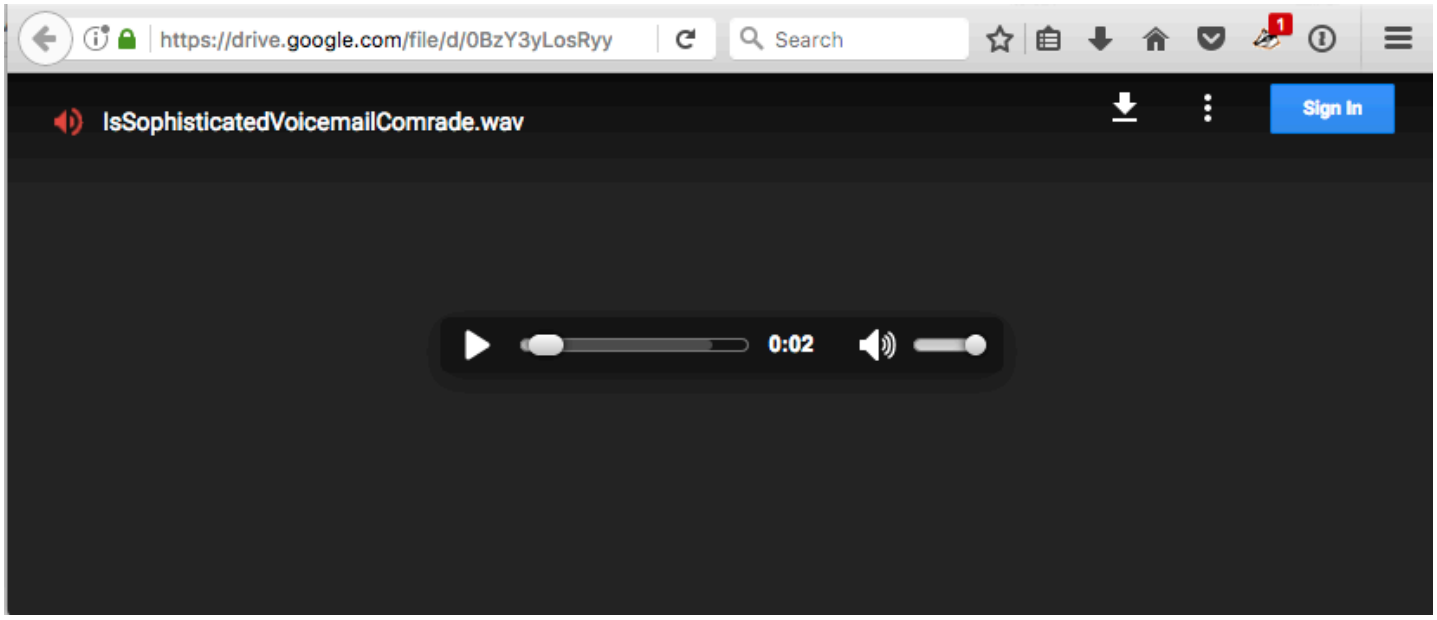
On this page at the bottom is a picture of James Franco’s brother helping a woman.



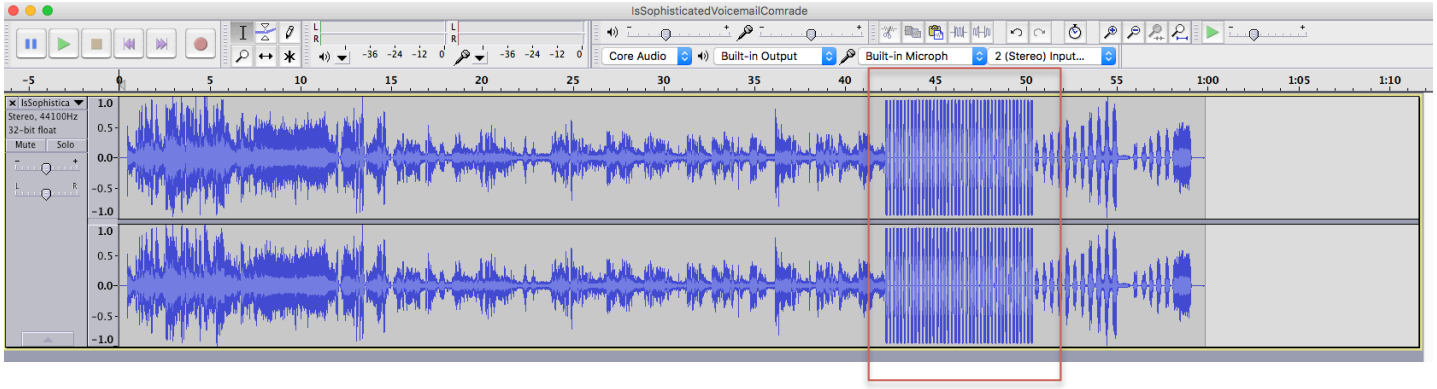
When they click on the picture they will be redirected to a GoogleDrive Wav file.

https://drive.google.com/open?id=0BylWx7bsw_S8OVlqSmZ6aTlFTlE

They will hear the Redprox intro. If they continue listening it will cut to static, they will hear some Russian voices, then a DTMF code. (The DTMF codes are the private key password)

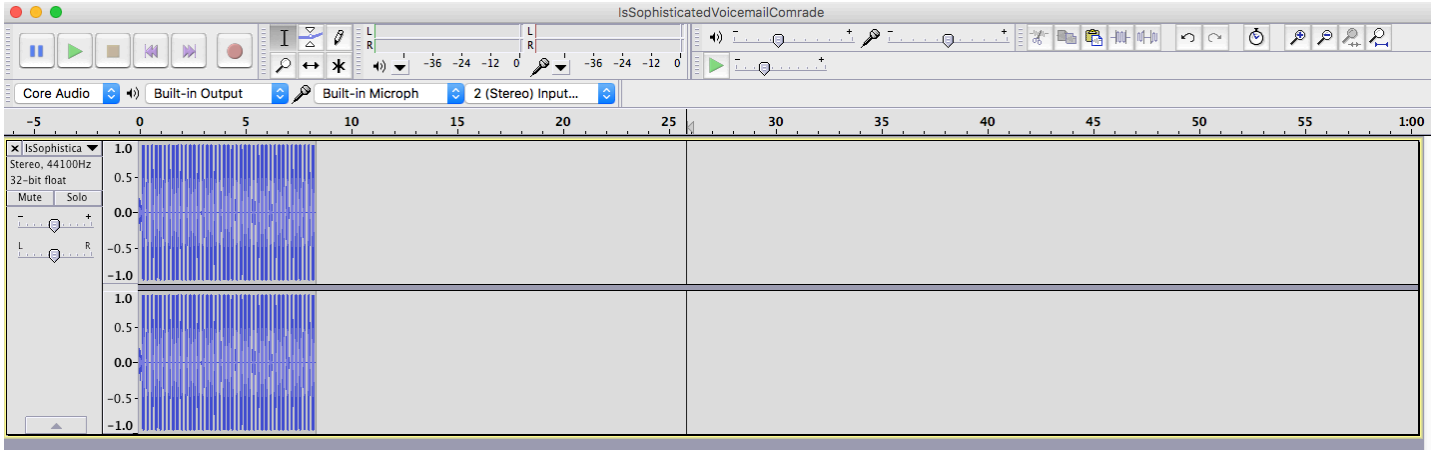


Download the wav file and open it in an audio editor like Audacity.

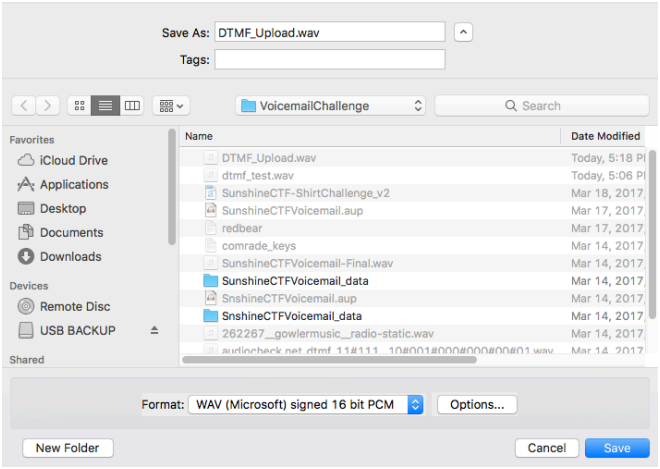


The area highlighted above is the segment of DTMF.

Remove any audio before or after this segment and export it as a separate wav file.



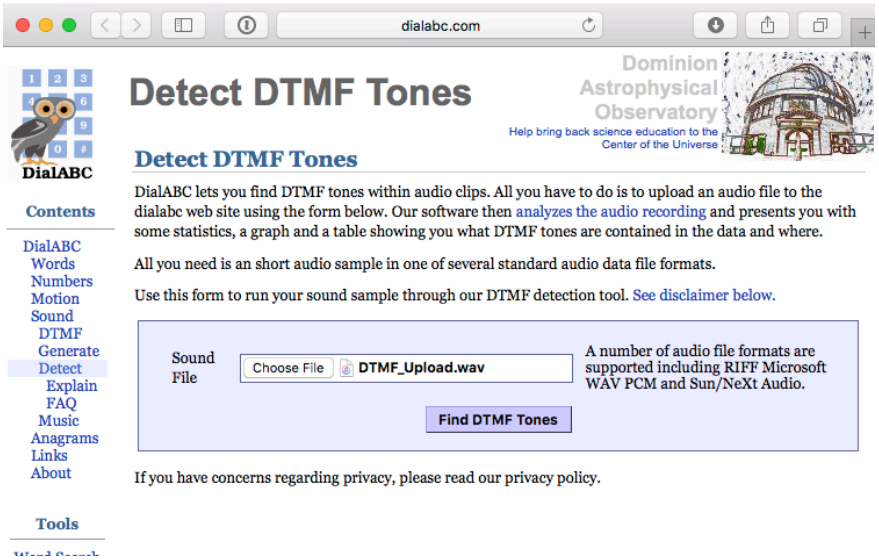
NOTE: The above is **CRITICAL.** Attempting to simply upload the whole WAV will attempt to translate other sounds into DTMF. They should only try and decode the very obvious DTMF pattern. Only the above DTMF signal will reveal the private key password.



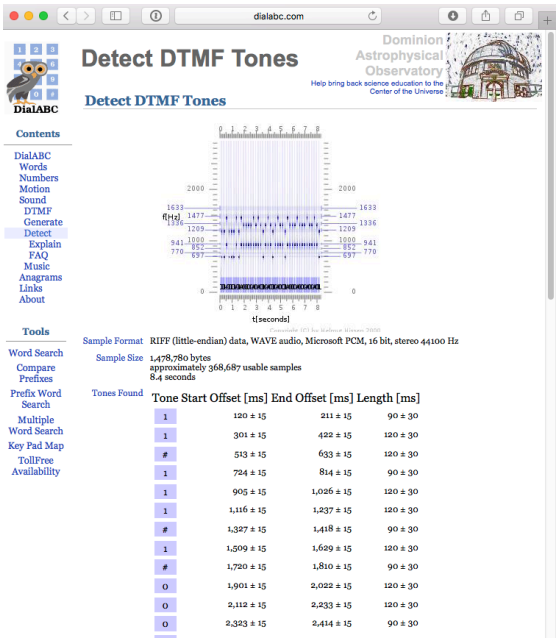
Export the file as a wave. We named it DTMF_Upload.wav

Next, you will need to decode the DTMF. We used http://dialabc.com/sound/detect/index.html

Go to this website and upload the DTMF_upload.wav file.



This will decode the DTMF into a string.



The decoded DTMF should equal:

11#111#1#0000#0#010#010#001#000#000#00#01

This is the password for the private key.

(Fun Fact: If you translate the DTMF to Morse where 1= dash, #=separator, and 0= dot you get this in morse. In morse translators the pipe is a space.

The below can be put into a Morse code translator at http://www.unit-conversion.info/texttools/morse-code/#data

--|---|-|....|.|.-.|.-.|..-|...|...|..|.-

You will then get MOTHERRUSSIA

Challenge 6: Decrypt the encrypted text

Using a PGP/GPG tool of your choice (for this test we used GPG Suite for Mac) use the key pair found at http://pastebin.com/BjkiX0gf in Base64 for comrade@bsidesorlando.org and the password 11#111#1#0000#0#010#010#001#000#000#00#01 to open the PGP encrypted text found here: http://pastebin.com/sct1Ng5V

The CTF team will get:

> GREAT REJOICING FOR MOTHER RUSSIA, COMRADE! FOR GREAT VICTORY OF PROLITARIAT TO BE HAVING !
>
> sun{J00_C4lled_The_R3d_Ph0n3_lntitiate_Launch?}

You will get the flag **sun{J00_C4lled_The_R3d_Ph0n3_lntitiate_Launch?}**

This is the flag for the BSides Orlando T-Shirt Challenge

Additional Notes:

Below are links to some of the tools used for creation and testing.

Used to generate DTMF tones - http://onlinetonegenerator.com/dtmf.html

Tool to detect DTMF tones - http://dialabc.com/sound/detect/

Used to translate M O T H E R U S S I A to something we could use in DTMF - http://morsecode.scphillips.com/translator.html

Dmitry Medvedev talking about Aliens - https://www.youtube.com/watch?v=NcvVzXzzJZk

Used for static in the voicemail wave file - https://www.freesound.org/search/?q=static

Create DTMF - http://www.audiocheck.net/audiocheck_dtmf.php

PasteBin Link for PGP encrypted flag - http://pastebin.com/sct1Ng5V

Second Paste with key in base64 with Pub/Pri Key - http://pastebin.com/BjkiX0gf