

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?"

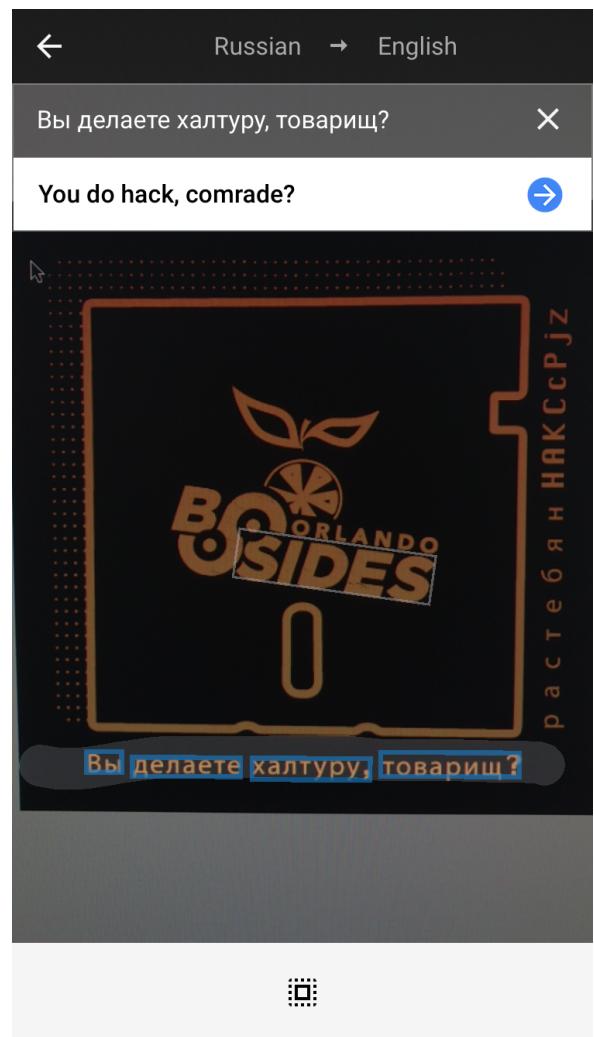
р а с т е б я н НАКCcPjz

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.

V2UgYXJlIGdsYWQgeW91IGZvdW5kIHVzLCBjb21yYWRILiBUYWtlIHRoZSBuZXh0IHN0ZXAuIA0KRmluZCBvdXIgcHVibGljIGtleSBhbhbmQgZW1haWwgdXMgdG8gcmVjZWl2ZSBmdXJ0aGVyIGluc3RydWN0aW9ucy4gDQpb21yYWRlQGJzaWRlc29ybGFuZG8ub3Jn

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.

Re: Autoresponse test for solutions sheet Inbox x Print Email

comrade <comrade+noreply@bsidesorlando.org> 11:59 PM (0 minutes ago) Star Reply Forward Save

[Russian](#) > [English](#) [Translate message](#) [Turn off for: Russian](#) x

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](tel:407-603-6879)

Товарищ, пожалуйста, наше сообщение ниже. Частный является публичным, понимаете?

<http://pastebin.com/sct1Ng5V>

Decode from Base64 format

Simply use the form below

V2UgYXJlIGdsYWQgeW91IGZvdW5kIHVzLCBjb21yYWRILiBUYWtlIHRoZSBuZXh0IHN0ZXAuIA0KRmluZCBvdXIgcHVibGljIGtleSBhbhbmQgZW1haWwgdXMgdG8gcmVjZWl2ZSBmdXJ0aGVyIGluc3RydWN0aW9ucy4gDQpb21yYWRlQGJzaWRlc29ybGFuZG8ub3Jn

DECODE UTF-8 You may also select input charset.
 Live mode OFF Decodes while you type or paste (in strict mode).
 UPLOAD FILE Decodes an entire file (max. 10MB).

START DOWNLOAD Doc to PDF

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

Cпасибо,

RedBear

<https://redbear4russia.wordpress.com/>

comrade@bsidesorlando.org

407-603-6879

When Translated:

Re: Autoresponse test for solutions sheet (Autoresponse test for solutions sheet)

Inbox x



 comrade <comrade+noreply@bsidesorlando.org>

11:59 PM (1 minute ago) 

to me

 Russian ▾ > English ▾ [View original message](#)

Always translate: Russian

Comrade, please, our message below. The private is public, you know?

<http://pastebin.com/sct1Ng5V>

Thank you,

RedBear

<https://redbear4russia.wordpress.com/>

comrade@bsidesorlando.org

407-603-6879

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-----

hQIMAz46AGKDB26ARAAw/MTugTyzyIxkizI5vQQA8+Zld33PYIlSGI9z5wV6boI
G2PkB5y73UdinBPCzjIzX+k5Gzbq1zjFLDxgT9Fk26ea909MDDul5TW82cXcYG+r
aVm1XTWDDVLZ9VCt6CENdCoJpsQ4nrBD9K076uGuiQUPCfjjub/gmS+uRTWu/45c

Q5AKIhnwe+UESbPUw+xOl5SiyQcVUjf/8PnD6biwimRi8dN72bXU9/VHNhJ8sNX5
 o7Z0AUpmGxfhhxPjL8luC4cFxi9/f/4DSVNcqUsfYb29dq5R9C1LmebpZjIvyzUC
 mEeOdw/iNSuHgS+j8CLSrwx2GTSeuLZd+bIM9KS/QXIBNXtWf9uRQDmtByBC+SSL
 k6Gey9rTbflrOw2AjqPwR8if4U0UiB4b7EVFhEJz1p1/Ihwk+Q3zuDiA6P5LFM8y
 VKiZWSvnW2bQ0noLMolQXdEz1qsLEsqHPjfjiFe7+bCowOypg8M84U3W169Uq/v
 N2WKhrCzUzItb0n6zWuCFmRUHRnT7+k/xzZwPa3NkfSdFLq5Kz48bPkbiI70BPpW
 QIVcsnhDhkoM7u/fKbChVq0YIB4xWLOkOV9oDvj3qaWsF60bm04phjXcU9kdRi3Z
 Fm7qE1s6fnWsyAD8s+0rO01HK1w1SZ/ZGwS6G2bumDC9ssq0u/xFOPvmYjo+Be3S
 6QGtYogeXZYZn6PDcPtKNG8dmD2AGBIyVRKYM1pIWXAfqBr+J1qYRPlPqzVAXE1z
 8hTABE0V+SxOwk+qV2/tp4nINCv3/2UHNUChWc06thFMMjLqeXoIrFjyPFnVzOSS
 WFl/6m9mzd9M77Kpq9EEKNF9BD0PjljObzSBBE+noURMn2NyU6wPdhQM2MUXtPdP
 zQOGdZ/aX2KEbjEmAwhsdhlwf3nXhsL577C+rP8E2MMPiSSIId9ds47mf1hnjI9np
 6FRJxn80MFBBmrue9tlkwI8K+0qxhPAPz2IA7Fbz/lAmEVtzOOqtIQVq2PkHgVhD
 AWin5IZOrLD3kcxItGxsnEZD2WT/qceYIpw3mvjBshAw7IrVh2900B5ffBKEnj+9
 KwWRRCpaifgoWvoKaeJV24LC082ZFad4wuhGHUisu0gco+wDgBswqyWpYb25NwHy
 KLZCqXr1rcGnKVIuNhSrzpRRZqNcl8FRVWMIRhcvskIsvMKXV+843kv2Ap2u7W2
 5lFQfKEGJ21CLMvNAg+B6q2LeYmPpZ6DMnVNvwnV6CBQJ39w7SCeLRFd1FVz0tQj
 Pa7iE0Pi907p025CHrY80nhgqjGuiOANE38vgv9UGN5kpJXAAI3LqYpX/vap3YCc
 G9zCfywe/xBfvMJFV4CkeNEQDB6ba3Tqiu9Rzv4B9nAgwDheI5DRyYK9rpdpQZyR
 WncK0rt8k0m33IPGE8b1YNq/bWCtYof1SXagKGpITvUWSE9gWsDODSY4SNZB7utZ
 bCyhKCPNiW44TrgDm2fJz6YmcP8VdkBhVG/QZNLBn0xOfgNoU/4HtjZ2TmxCt2AH
 KyT76rZorLIGyLqlSUP4Wg2OUT6PQ6MxWI/zjTkKK+rtiDoWTRYWhvVV0fpN11WG
 q0l4HuUYB1k/2Eg7z3YqT07+li/zcunIusEDOSbXIyfJVNfPM5EI3V+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/>

Путин смешно ЦРУ о Сноуден

Putin Ridicules CIA on Edward Snowden

He ended up on our territory, based on what I see is the unprofessionalism of the CIA who tried to catch him.

Конфиденциальность – ложь

- 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 is to find the private key password.

Decode from Base64 format

Simply use the form below

```
LS01LS1CRUdJTiBQR1AgUFVCTEIDIEtFWSBCTE9DSy0tLS0tDQoNCm1RSU5CRmpJTGZvQk
VBQ2o5YU1uSHVKejoYmZoRSIkJOWxTY1BxaDgxMFhyb2Y1MHzQkp3WFvfd0d4R2ZByzY
NCkovTTdlWTBORXE2Unp2NVUvn3i2YnJvbJyjdE4wSWJUdVBWhTmU4UmxBGQTZOUWXRl
JXM0Vza096QW5ZaJWVvYNCisyl3dnRTM1M0d1RG54VXBQZ09DRENMM21GYnkwmJm2Yj
R4RGZ6MEkwMnhszcBUCDFVXBTSEtKzktWdkf4NmknCjNyafdnMHVET0pvcG520GRQdC
iRTXBnTKVC20FrT2lSbVhNUopjuVMrnJ2UR014dmNDTFIGQjhndDQxR20NCmxoxQIZSD
JBMXA2c3o6aDFLR1VmFlucondWEMr0VBPd2XdImYk9r0N3YWhoaXFBEF6RWlvUkZ
zVjhvamENCkhSVk9qMTVSQTVU2F2S2hCQ3U2aGpQVJpOFduaUVROWM3UHVkd0Y0SzJ
oVjVytSiwmt1MhsVUZPRmzrSUOcxHvpdAwmlWb1A1V0U2R3FaRXuefMxbWI0V
zNWQ2xvWU15S1bLc3YU5NOWtyaEqySG1qNuHTQUDhUE4NCmzNOEVIK2RuVmNHmu
FxYzgrUIdhc02TeGn3V1RjZFTNTXNEY2czvIzTIn0N3ZYV3graEvqaFhdHBZTDJ0NjEncn
zNW05DMVhQTSs2b1hidzRvUfJhsDaIxFcKzHkN1JDLzRLdkdJWWZZRE0reFVeBvNGc1BF
UDV3ycFNMVU1QmNcnlZamNZShNBKy9ZDRob3RBZHdMWtsTGF0RVN-SzHRL0U4dEszRi
-----END PGP PRIVATE KEY BLOCK-----
```

DECODE **UTF-8** You may also select input charset.
 Live mode OFF Decodes while you type or paste (in strict mode).
 UPLOAD FILE Decodes an entire file (max. 10MB).

START DOWNLOAD **Doc to PDF**

- 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.

Home About Team Products/Services Support Found an asset tag? 407-603-6879

REDPROX
SOLVING CHALLENGES FOR THE FUTURE

About

RedProx was founded in 1996 with one goal: Change the way cutting edge data analytics technology impacts industry disruptors. We bring together top talent from all areas of information technology and process management to help everyone from start-ups to Fortune 100 companies.

RedProx focuses on the Three Tenants of Information Technology Thought Leadership:

- Mind Share
- Quantification
- Cubicle Dynamics

Let us show you how our three tenants and QOOPS™ can help you drive beyond the future!

Contact us via the below methods:

101 S Garland Ave

101 S Garland Ave, Orlando, FL 32801 [Directions](#) [Save](#) [To Science Center](#)

View larger map



Address:
101 S Garland Ave - 10th Floor
Orlando, FL 32801

Email: info@redprox.com

Phone: 407-603-6879

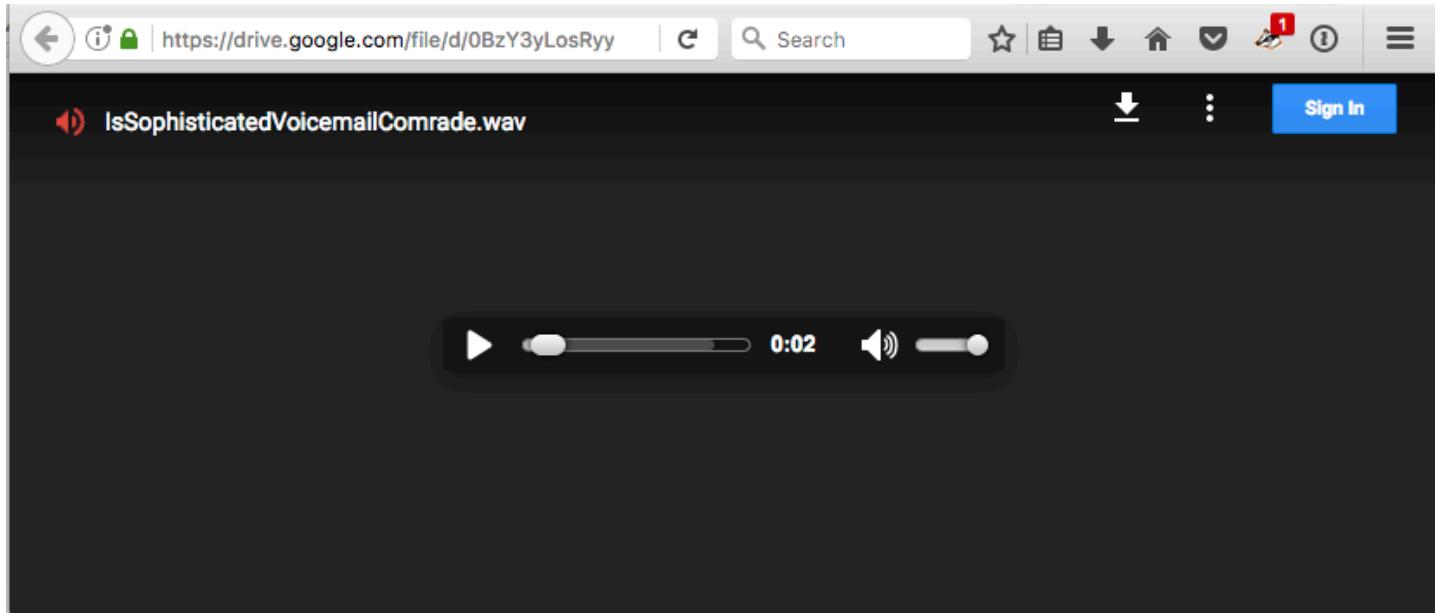
Hours: M-F 9am-5pm (Closed Holidays)



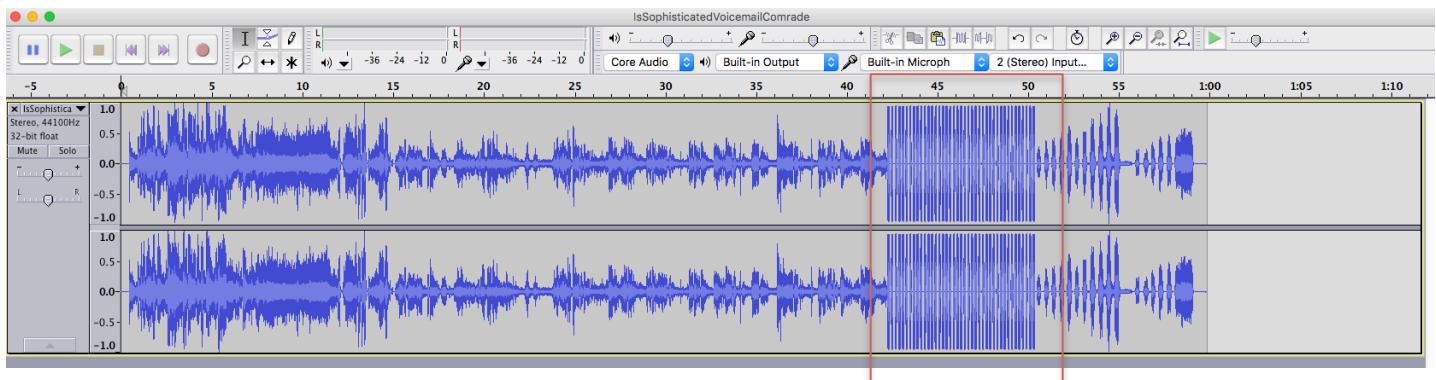
When they click on the picture they will be redirected to a GoogleDrive Wav file.

https://drive.google.com/open?id=0BylWx7bsw_S80VlqSmZ6aTlFTlE

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)

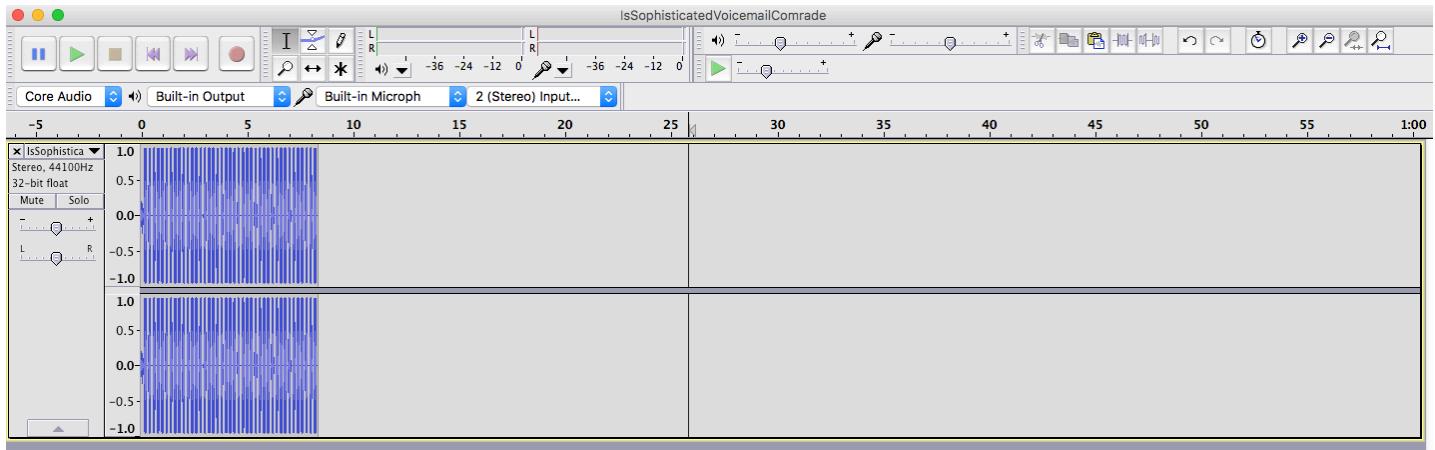


Download the wav file and open it in an audio editor like Audacity.



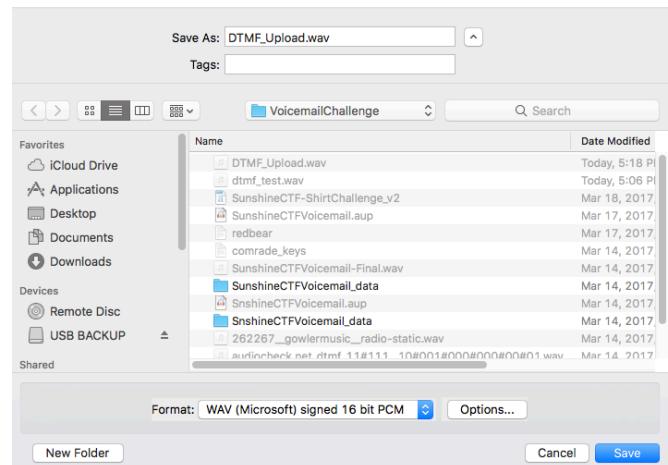
The area highlighted above is the segment of DTMF.

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.

Detect DTMF Tones

DialABC lets you find DTMF tones within audio clips. All you have to do is to upload an audio file to the dialabc web site using the form below. Our software then analyzes the audio recording and presents you with some statistics, a graph and a table showing what DTMF tones are contained in the data and where.

All you need is an short audio sample in one of several standard audio data file formats.

Use this form to run your sound sample through our DTMF detection tool. See disclaimer below.

Sound File A number of audio file formats are supported including RIFF Microsoft WAV PCM and Sun/NeXT Audio.

If you have concerns regarding privacy, please read our privacy policy.

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>

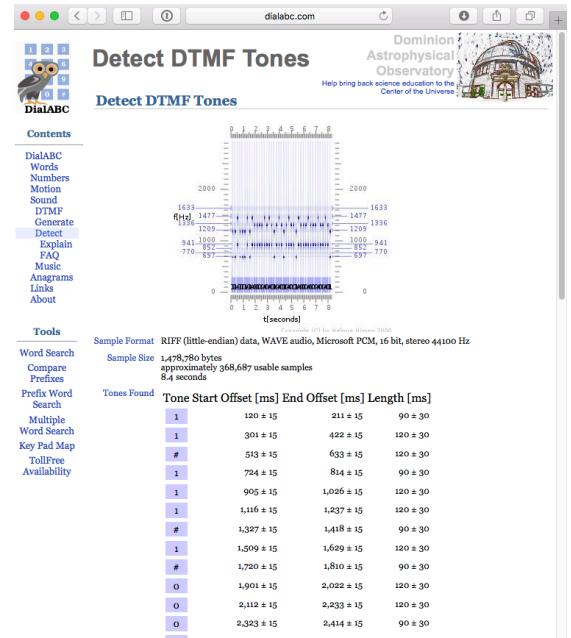
The CTF team will get:

GREAT REJOICING FOR MOTHER RUSSIA, COMRADE! FOR GREAT VICTORY OF PROLETARIAT 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.scphilips.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>