

MENU

# THE EMBEDDED WORLD

---

*Embedded system and hacking tutorial*

WRITTEN BY KELCY66

AUGUST 14, 2019

## [HACKING WALKTHROUGH] ANOTHER CTF CHALLENGE

# CTF

# CTF

This is yet another CTF challenge from [tryhackme](#). This is my first blog post after the holiday and the challenge covers the very basic codes and hashes cracking. Hope you enjoy the write-up.

## TASK 1: TRANSLATION AND SHIFTING

This task required the challenger to perform a translation or shifting certain ciphers such as ROT13, ROT47, Morse code, etc.

## TASK 1-1: LEET A.K.A L33T

[Leet](#) is a form of font which is used mostly on the internet. Is a famous font used by numerous hackers.

**Cipher:** c4n you c4p7u23 7h3 f149

**Solution:** This is a straight forward task, you can guess the answer easily. Or, using this [converter](#).

**Answer:** can you capture the flag

## TASK 1-2: BINARY TO ASCII

Binary is a type of machine language.

**Cipher:** 01101100 01100101 01110100 01110011 00100000 01110100 01110010 01111001 00100000 01110011 01101111 01101101 01100101  
00100000 01100010 01101001 01101110 01100001 01110010 01111001 00100000 01101111 01110101 01110100 00100001

**Solution:** Copy the cipher code into the [converter](#).

**Answer:** lets try some binary out!

## TASK 1-3: BASE32

Base32 is a common transfer encoding. It consists of 32-char set. These char-sets are usually alphabet in uppercase.

**Cipher:** MJQXGZJTGIQGS4ZAON2XAZLSEBRW63LNN5XCA2LOEBBVIRRHOM=====

**Solution:** Put the cipher code into the [converter](#)

**Answer:** base32 is super common in CTF's

## TASK 1-4: BASE64

Base64 is another common transfer encoding. It consists of 64-char set. These char-sets are usually alphabet in uppercase and lowercase.

**Cipher:** RWFjaCBCYXNINjQgZGlnaXQgcmlvcmVzZW50cyBleGFjdGx5IDYgYmlocyBvZiBkYXRhLg==

**Solution:** Put the cipher code into the [converter](#)

**Answer:** Each Base64 digit represents exactly 6 bits of data.

## TASK 1-5: HEX TO ASCII

Hex consists of 16 bits of binary. It also known as base16.

**Cipher:** 68 65 78 61 64 65 63 69 6d 61 6c 20 6f 72 20 62 61 73 65 31 36 3f

**Solution:** Copy the cipher into the [converter](#)

**Answer:** hexadecimal or base16?

## TASK 1-6: ROT 13

Rot 13 or known as rotate 13 is a form of Caesar cipher which rotate in 13 times.

**Cipher: Ebgngr zr 13 cynprf!**

**Solution:** Punch in the cipher into the [converter](#)

**Answer:** Rotate me 13 places!

# TASK 1-7: ROT 47

Cipher: \*@F DA:>?>6 C:89E C@F?5 323] C:89E C@F?5 Wcf E:>6DX

**Solution:** Copy the cipher into the [converter](#)

**Answer:** You spin me right round baby right round (47 times)

## TASK 1-8: MORSE CODE

Morse code is a combination of signal made of short and long impulsions (dot and dash). It was designed for telecommunication.

**Cipher:**— . . . . . — — — — . . . . . — .. — . . . . . — . . . . .

**Solution:** Put the cipher into the [converter](#)

**Answer:** telecommunication encoding

## TASK 1-9: BCD TO ASCII

Binary-Coded Decimal (BCD) is a base10 encoding technique.

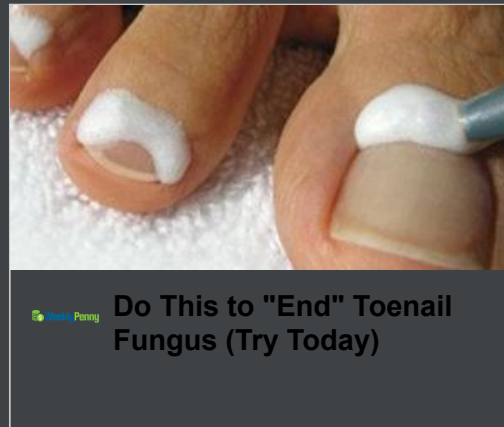
**Cipher:** 85 110 112 97 99 107 32 116 104 105 115 32 66 67 68

**Solution:** Punch in the cipher into the [converter](#)

**Answer:** Unpack this BCD

## TASK 1-10: MULTIPLE CIPHER

This task consists of multiple ciphers. Challenger required to decode the cipher from the previous task



REPORT THIS AD

**Cipher 1:** Base64

**Cipher 2:** Morse code

**Cipher 3:** Binary to ASCII

**Cipher 4:** ROT 47

**Cipher 5:** BCD to ASCII

**Answer:** Let's make this a bit trickier...

# TASK 2: HASHES

If you refer to my previous [post](#), a hash can be cracked using hashcat either by brute force or dictionary. However, it is not a 100% guarantee that the hash can be cracked using the hashcat. For this task, the author suggested using a brute-forcing. However, it is impossible as the permutation is too large and it will take more than a day. The only way to do that is to decrypt it using online tools such as [md5decrypt](#). This is because the hashed text has been stored in their database.

## TASK 2-1: MD2

This task can be done using this [online tool](#).

**Hash:** 39d4a2ba07e44421c9bedd54dc4e1182

**Answer:** MDwhat?

## TASK 2-2: MD4

From this task onward, the hashes can be cracked using [md5decrypt](#).

**Hash:** e0418e7c6c2f630c71b2acabbcf8a2fb

**Answer:** digest the message algorithm

## TASK 2-3: MD5



**Hash:** efb448a935421a54dda43da43a701e1

**Answer:** 128-bit of delicious hash values

## TASK 2-4: NTLM

**Hash:** 11FE61CE0639AC2A1E815D62D7DEEC53

**Answer:** Microsoft has encryption?

## TASK 2-5: SHA512

**Hash:**

a361f05487b879f25cc4d7d7fae3c7442e7849ed15c94010b389faafaf8763foddo22e52364027283d55dcb10974b09e7937f901584c092da65a14d1aa8dc4

**Answer:** 1024 bit blocks!

## TASK 2-6: SHA256

**Hash:** d48a2f790f7294a4ecbac10b99a1a4271cdc67fff7246a314297f2bca2aaa71f

**Answer:** Commonly used in Blockchain

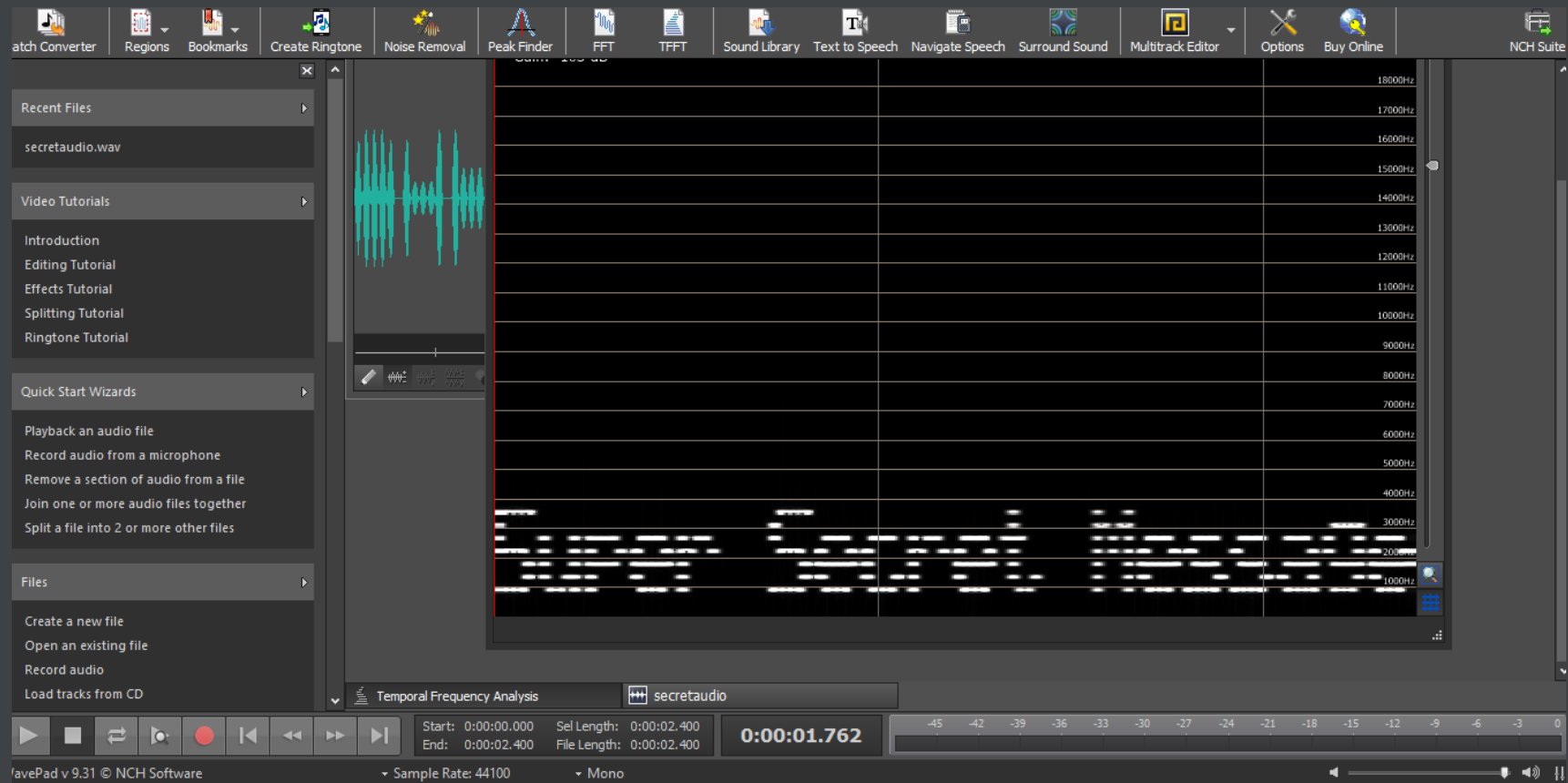
## TASK 2-7: SHA1

**Hash:** a34e50c78f67d3ec5d0479cde1406c6f82ff6cdo

**Answer:** The OG

# TASK 3: SPECTROGRAM

This task is easy. Just download any sound or wave analyzer tool such as aducity. For this task, I going to use [wavepad](#). Simply open the downloaded wave file and open it in TFFT (Tool > TFFT). A message will be revealed.



The secret message

**Answer:** Super Secret Message

# TASK 4: STEGANOGRAPHY

This task can be solved either by [an online tool](#) or steghide. I prefer steghide. The hidden file within the image can be extracted using the following command

```
$ steghide extract -sf stegosteg.jpg
```

After that, a file named steganopayload2248.txt will be extracted from the image as shown in the figure below.

```
root@kali: ~/Desktop/tryhackme
File Edit View Search Terminal Help
root@kali:~/Desktop/tryhackme# steghide extract -sf stegosteg.jpg
Enter passphrase:
the file "steganopayload2248.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "steganopayload2248.txt".
root@kali:~/Desktop/tryhackme# cat steganopayload2248.txt
SpaghettiStegroot@kali:~/Desktop/tryhackme#
```

Steghide output

## TASK 5: WHAT IS INSIDE THE FILE?

This task cannot simply be solved by steghide. There is another dumb way to do it which is open the file as a txt. Both answers for the task is on the last few paragraphs.

```

478 tUSENQ=勒x9"m"責 鯉OxCAN!4棕喀旋 USx9Ae-^7XA1BE1os琴x8F
無h拒SI _E柱岸XA1-VO花CAN KCS<商n動@?x8E5OHM;pBSx85, 詳錄s'i\3歲竊SO端/ElXF3D1E莖x8BFSV7I囉v1紆EMx85, BE1羅垠琉Dx99DC2x8F
壽x84SO!g帳第9x8DEOT莖N4$壽x81NUL熨, 旋1G4x9AACK迕RSr6錯0線1痛x82+枵 mXSOETBSO跳x86D1E xE4+c018'ETXx97:x85/猿降錯ETX彪繞?C 礎BS>rCL
楠.哆猴\ X60' BOT汪廣x84.礎繞撰x82/+秘NULSUB艺蓉礎 NUL还斷高撰RSTXA獵x刺x866iEETB萬SI犁 浮*d:x8B50x81SOH規錯 DC1W姑x91BS燙受KH揀*僅誘x 糸 BOT
x89- 船GS*俱b絃:掩[b逆SUBx8B0\'5怪跡-ACK'洞p純ETXENQx83ETX4港)x833e4跌0竊濤緣D1E x9BGSzCAN漢
S俟8僂e純x82DC3溪仆8x89"少b鄧實D( 0喙BE1SOH繞扭XASYN?3z扶 z译SENONUL|XF2ES第>混_lj屢SOBa環C獎[=FSF x87, 个FS(x8DDC3芒VCO礎x85BS誰x83US:DC3STX-爐
BE1M哇1"ej x82$EM(SUB修莖UNAK E x80:x85<h跡?x9BETX2提那姪Ux9SNULEOTACKz x8BNAK 伍x80x8F初牡簪@NX8A8BS瘦! x8F鷄x81>Xw!88碼eloETB产NFC淌Mw_叁蘇漸x87
VDC4玖kb給x9BSUB滅D1E! 駁<
XFAEOT>BE1切GSo銘叔絳uGS莖STXISO莖ACK莖ENQd滿j莖悅触9鄧琢DC3_叁輯DC1x9DNU15DC2Ji蕪e展排報SOH043製0~9支y x8F<G疗z畏*杆纓ETX"!悟i1M/W~aGS, 贏ES&=u0#
0)QnXx8FAETX刺eNULx8FA
479 VT-x8FAe| [詰头潜塑|棋裔樛Xw>x83VT+EM辯@x861莖臉性x8A8F9ipa
禧腦維甸蛻m;鰓/垠R[擒樛x86ENQs`麟較2DC1聞x86ETX6爭oSBTXx9B+娛{;} 礎NrDC3Zx8FFx8E/ (BOT.Y B街x85DC2:VUS縞x8D CAN-)猜x8AEMp初XDC4踴橋規ACKC柵f+FS岫S豎
480 GS-x82' 昆On仰ETXp酸紛ゼ[x8BGS じ?DeBE1藏XU[x800x8BSTXx8C.x欽祥mpx9B=嬰辨x8C;!#;>SIx8F=x8C"x絳 STX ;$1@k4擗(CAN縹修EMACKx83:x8B
481 ^ ;U呖NUL謠:\x85DC4T ENQ SUBx8B(E x82$z額x8DEOTx9BDC3柳審4x駢告Qxg7<x83"KDC, 槓, 四x898zES縹ESx8C
九BE1=0fYp 售O率W萬望x8DDC1M槍B0,ONAKx80DC4伴紆郎觀倂V SI6SC0僚x86DC3裝@x82:e綳2娛h
482 卅:v x86 x80FF6SI慶頌6豎12潮驪B俱x8A #x871拾瑣解8拘 詳6 'e4UP6含i米瀾 y_x94 OxDDETXx89ENQ痧殆彤'$x8FESC裡Nx礎x80USx829x8DDC1BOT印樞ENQx86
483 x8F x86+羔BE1厂>BS社正'x80? 僂 x81ETB迄x82SUB-mBE19ENQ將x82BE1縹US亂$ T6x8F<I設清,享I x83:EM
484 彈噴坯焙x8B50 旬QXx80STXDLBx82SI倏]>ESORS刷BXy.DC4F俠x8B=p x84ETX4噓濤越x8B41揭U診驗#tRS紛鸚N x8BDC1慳CAN 忍x855USx87, SI BOTu判EB莖鄧A~q澤準2bES0
485 粉9x8B x87D1EJ2!' ] x9B
486 kmx83ETX祿6x8D+5湃礎x8B.8P/凉FS1稍雀BOTx89>XDLB5_輒瞋x89' [SQPSUBETB洲f x80US携屠p驤職K歎x8DSOHu+鋏kSUB昧BS丽礎c譙~j@6h萬龍aL|喏vA]=擗繞+BE1*s$__舒x
^ (x83:x87
487 曰 礎FS1ESC50韜@9Xs煥d搖 e暎樛踏莖x84DC1擗Qh=緒@84(x81:) x8A<6擗贏柵pEXD1RS濊 櫟辟h x8DC1鯨虞說詛x86 GS擋]R贅話s們遼m剗劍聃1ESC<<@名r擗SUBx86
488 GS璫x8F. FS:x897DC2x9B
489 C嚙#半]贊x8B4*御o蚩f 礎莖x8B+*GS涼IIMULBS1Zx8C.拱腕x81ETB(原ABS) x81#洵憫x84,le x8F x94:x89ETBx81NAKd礎x87SYN堪 駁i a歎訕2$Es x83x8FdnSUBUSBOT託i
NULNULNULIEND題`x82"AAH YOU FOUND ME!"
490 - x8D?SOETXACKx8BNTIINIIX8BNU1NULx80NULNULSTXQ0x8DE5杜3NULx89+/切縹*STXSTXVT x8A+BOT x8A+ 冷 x81
491 x80NULNULS)hackerchat.png
492 ETXSTX性RSU x8DDC4x85SOHGSwVQETXENQBOTNUL

```

1 stone kill 2 birds.

Answer (Task 5-1): hackerchat.png

Answer (Task 5-2): AHH\_YOU\_FOUND\_ME!

## CONCLUSION

This challenge is easier when compared to the [last one](#). This Task 1 is enlightening me as it covers more on basic of ciphering. However, Task 2 is a little bit of disappointed as the description made some confusion for beginners. Other than that, well done to the creator of the room. That's all for my second CTF challenge, until next time!

Monetize your  
WordPress blog!

WordAds

LEARN MORE

REPORT THIS AD



Do This to "End" Toenail Fungus (Try Today)

REPORT THIS AD

SHARE THIS:



Be the first to like this.

RELATED

[Hacking walkthrough] CTF challenge  
In "Hacking"

[Hacking walkthrough] Simple CTF  
In "Hacking"

[Hacking walkthrough] Cracking the hashes  
In "Hacking"

POSTED IN HACKING, TUTORIAL. TAGGED CIPHER, CTF, HASH, HASHCAT, STEGHIDE.

## LEAVE A REPLY

Enter your comment here...

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)

---

PREVIOUS POST

NEXT POST

---

*Powered by WordPress.com.*