Assignment *01*

David Murillo Santiago
Professor Valecha
IS-4483
25 January 2024

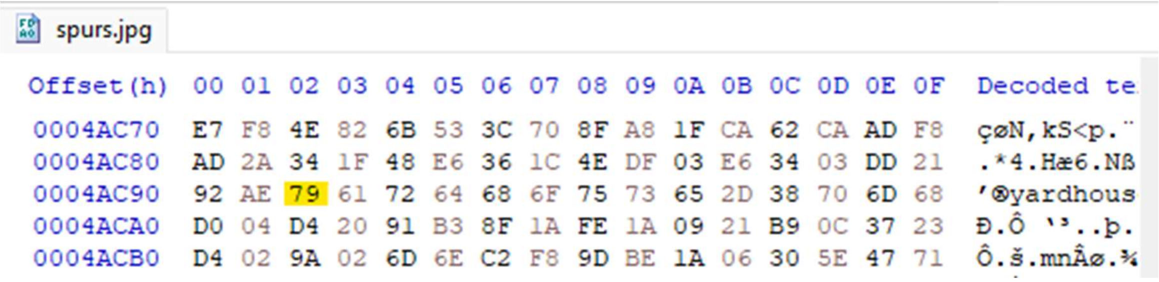
INTRODUCTION

In this assignment, I will use HxD Editor to locate, interpret, and alter specific pieces of data within files.

PROCESS

Part *1: Locate location and time of meeting within Spurs.jpg.*

To begin, I downloaded a jpg file named “spurs.jpg” and opened it on HxD Editor. The information we’re looking for begins on offset 0x4AC92.

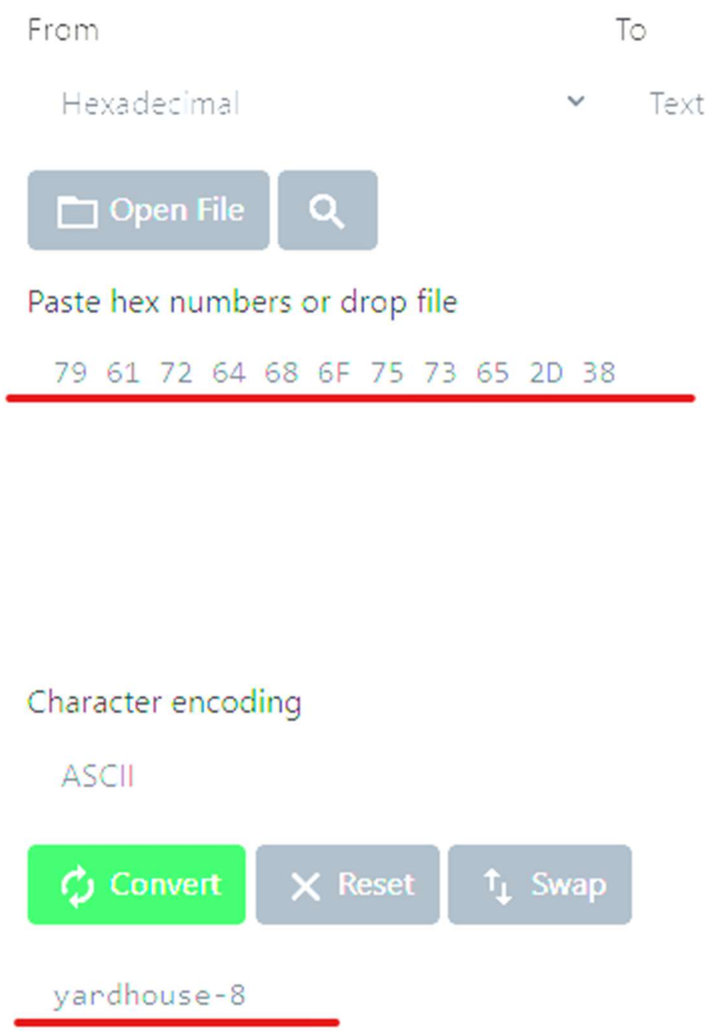


```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded te

0004AC70  E7 F8 4E 82 6B 53 3C 70 8F A8 1F CA 62 CA AD F8  çøN‚kS<p.¨
0004AC80  AD 2A 34 1F 48 E6 36 1C 4E DF 03 E6 34 03 DD 21  .*4.Hæ6.Nß
0004AC90  92 AE 79 61 72 64 68 6F 75 73 65 2D 38 70 6D 68  ’®yardhous
0004ACA0  D0 04 D4 20 91 B3 8F 1A FE 1A 09 21 B9 0C 37 23  Ð.Ô ‘³..þ.
0004ACB0  D4 02 9A 02 6D 6E C2 F8 9D BE 1A 06 30 5E 47 71  Ô.š.mnÂø.¾
```

Based on this information, the location is revealed beginning at the highlighted Hex value 79. The information is to be read in big endian, therefore the Hex values to the right may also be important.

Using RapidTables, (https://www.rapidtables.com/convert/number/hex-to-ascii.html) I translated the following Hex values to ASCII > 79 61 72 64 68 6F 75 73 65 2D 38.



From Hexadecimal

To Text

Paste hex numbers or drop file

```
79 61 72 64 68 6F 75 73 65 2D 38
```

Character encoding

ASCII

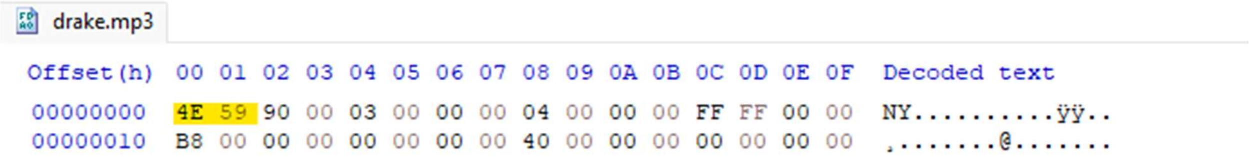
```
yardhouse-8
```

The values translated to "yardhouse-8".

From this, I determined that the location of the meeting was at the yard house.

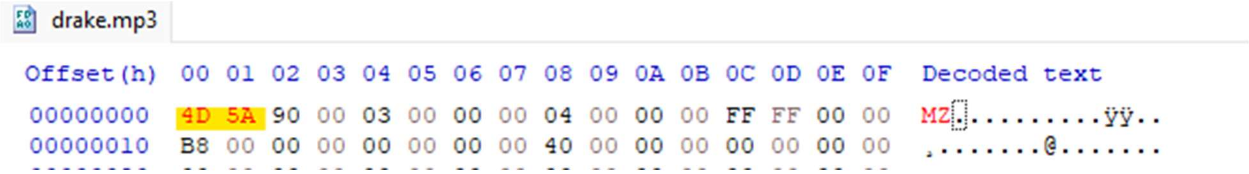
Part 2: *Alter Hex Values to Create a .exe.*

Next, I downloaded an mp3 file named "drake.mp3" and opened it on HxD Editor. I needed to modify a word at offset 0x00000.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4E 59 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  NY..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
```

Because the information was in big endian, the values I needed to modify were 4E 59.

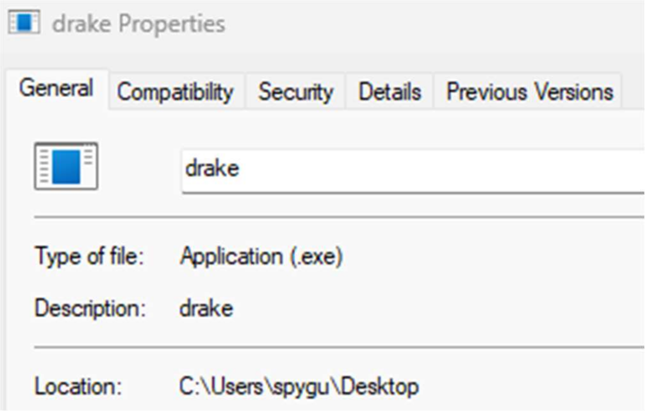


drake.mp3

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
```

I modified the file by replacing the original values with 4D 5A, marking it as a DOS executable.

Next, I saved a copy of the file and named it “drake.exe”, in order to be able to run the executable.



drake Properties

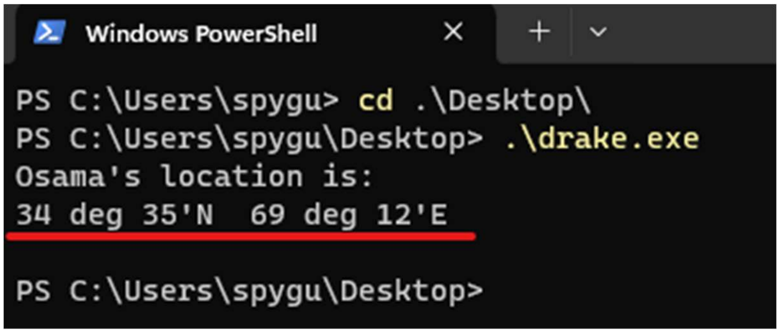
drake

Type of file: Application (.exe)

Description: drake

Location: C:\Users\spygu\Desktop

Here you can see that the file was successfully saved onto my Desktop as a .exe.

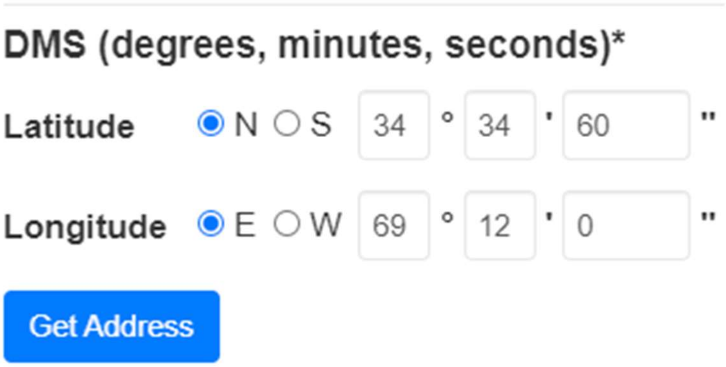


```
PS C:\Users\spygu> cd .\Desktop\
PS C:\Users\spygu\Desktop> .\drake.exe
Osama's location is:
34 deg 35'N  69 deg 12'E

PS C:\Users\spygu\Desktop>
```

Using the terminal, I ran the exe file and got the underlined output.

Based on the output, I determined that Osama’s location was “34 deg 35’N 69 deg 12’E.” To determine where this was geographically, I used a GPS coordinate converting website (https://www.gps-coordinates.net/gps-coordinates-converter) and entered the coordinates into the latitude and longitude.

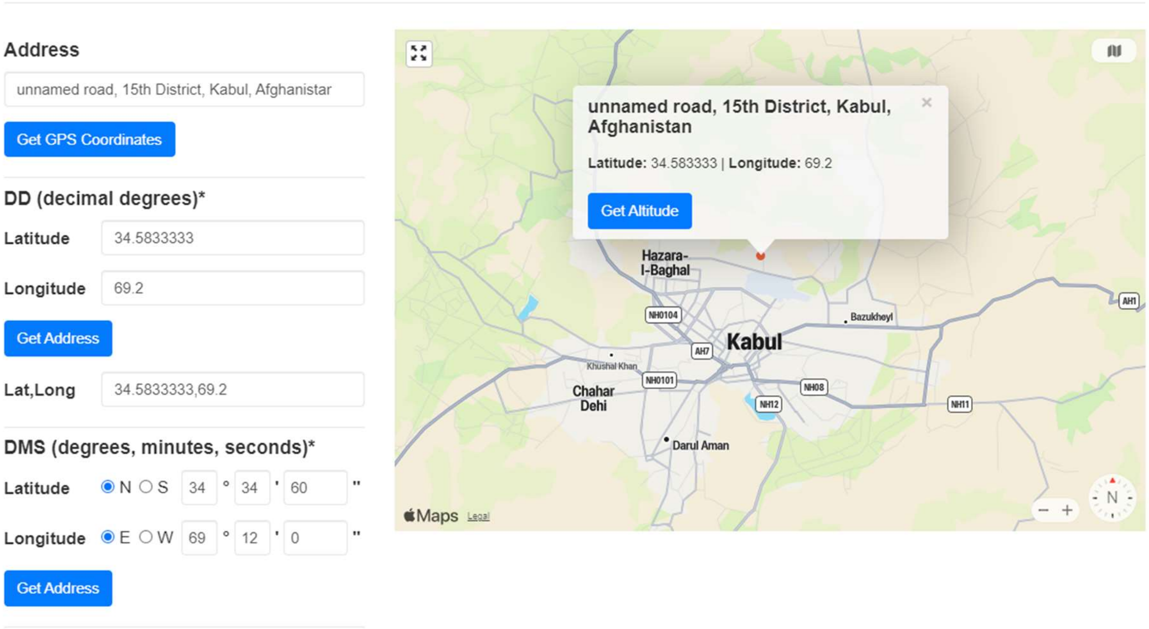


DMS (degrees, minutes, seconds)*

Latitude ● N ○ S 34 ° 34 ' 60 "

Longitude ● E ○ W 69 ° 12 ' 0 "

By the latitude and longitude here, I received the following output.



Address

unnamed road, 15th District, Kabul, Afghanistar

DD (decimal degrees)*

Latitude 34.5833333

Longitude 69.2

Lat,Long 34.5833333,69.2

DMS (degrees, minutes, seconds)*

Latitude ● N ○ S 34 ° 34 ' 60 "

Longitude ● E ○ W 69 ° 12 ' 0 "

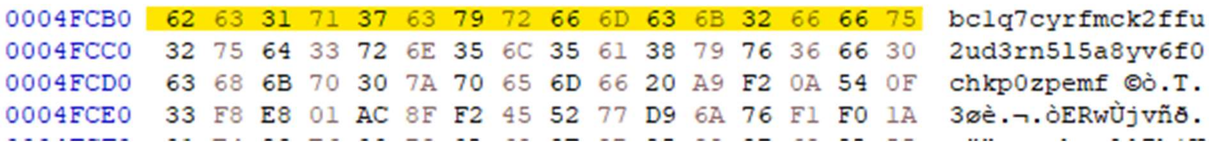
unnamed road, 15th District, Kabul, Afghanistan

Latitude: 34.583333 | **Longitude:** 69.2

According to the GPS coordinate converter, Osama was located at an unnamed road in Kabul, Afghanistan.

Part ***3: Bitcoin Wallet.***

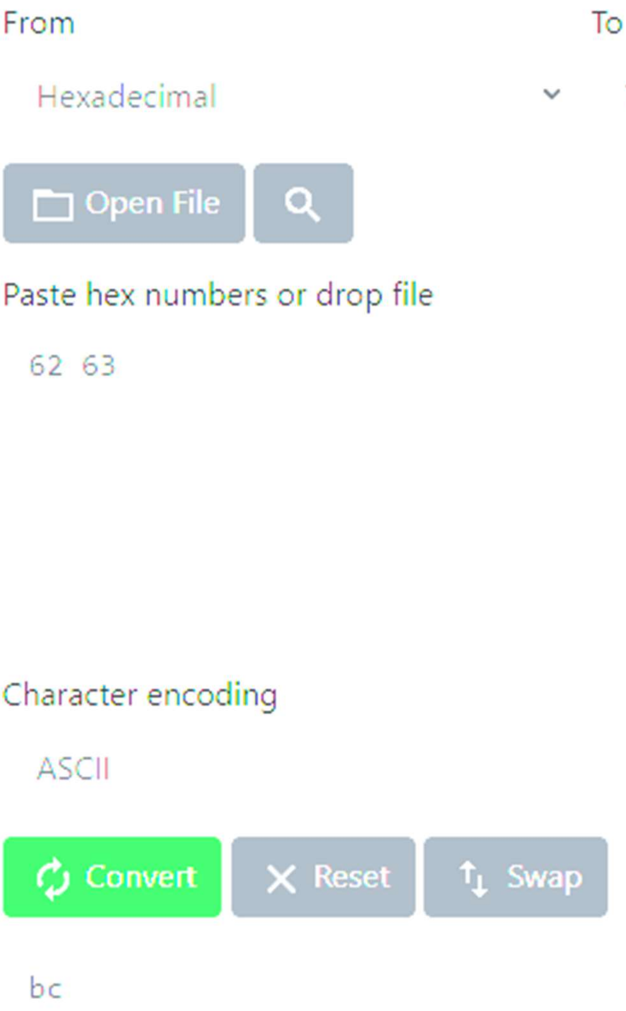
Next, I opened the “spurs.jpg” file again and searched for the hex values at offset 0x4FCB0.



```
0004FCB0  62 63 31 71 37 63 79 72 66 6D 63 6B 32 66 66 75  bc1q7cyrfmck2ffu
0004FCC0  32 75 64 33 72 6E 35 6C 35 61 38 79 76 36 66 30  2ud3rn5l5a8yv6f0
0004FCD0  63 68 6B 70 30 7A 70 65 6D 66 20 A9 F2 0A 54 0F  chkp0zpemf ©ò.T.
0004FCE0  33 F8 E8 01 AC 8F F2 45 52 77 D9 6A 76 F1 F0 1A  3øè.¬.òERwÙjvñð.
```

Screenshot of the values located at this offset.

Because I was searching for a Bitcoin address, I conducted research to understand what I was looking for. Using the Bitcoin website, (https://news.bitcoin.com/everything-you-should-know-about-bitcoin-address-formats/) I learned that Bitcoin has three main types of addresses: P2PKH, P2SH, and Bech32. These addresses are distinguished by their functionality and their starting characters. A P2PKH address always begins with a 1, while P2SH addresses begin with a 3, and Bech32 with a bc1. With this information, I translated the first two hex values to ASCII to determine which address type I am searching for.



From: Hexadecimal

To: Text

Paste hex numbers or drop file

62 63

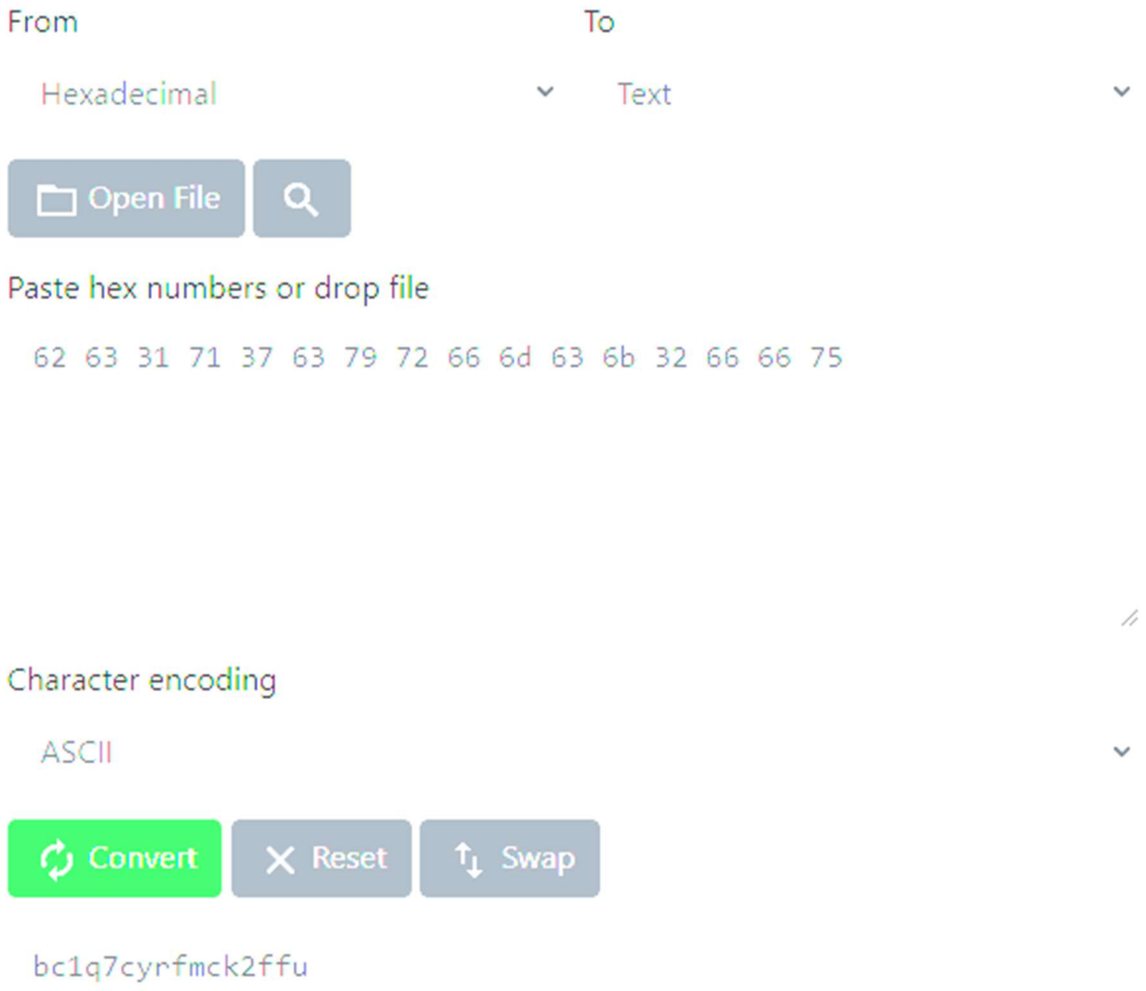
Character encoding: ASCII

bc

Using RapidTables, I found that the first two values translated to bc.

Because the values were translated to “bc”, I was able to determine that I was searching for a bech32 address. Unfortunately, there is no fixed length for a Bitcoin address, therefore it would be difficult to determine where the address ends.

Next, I translated the entire line of hex values.



From: Hexadecimal

To: Text

Paste hex numbers or drop file

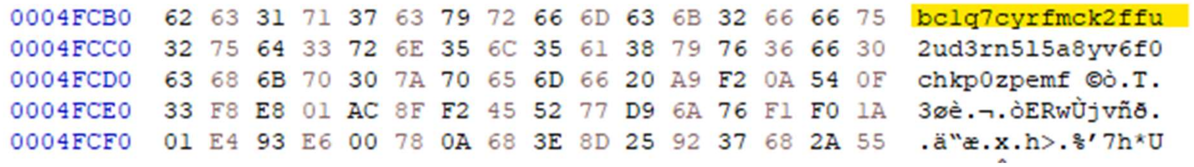
```
62 63 31 71 37 63 79 72 66 6d 63 6b 32 66 66 75
```

Character encoding: ASCII

```
bc1q7cyrfmck2ffu
```

The values translated to “bbc1q7cyrfmck2ffu.”

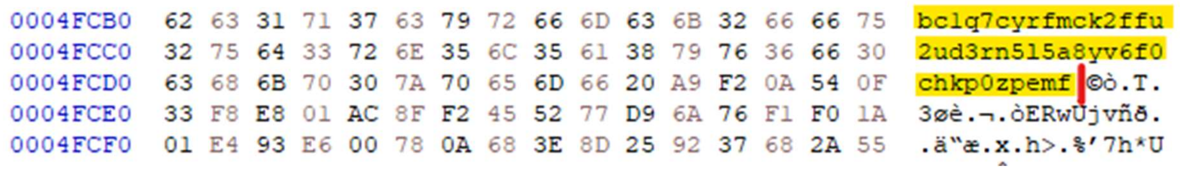
From these values, I realized that HxD translates hex to ASCII automatically and displays the results beside each line.



```
0004FCB0  62 63 31 71 37 63 79 72 66 6D 63 6B 32 66 66 75  bc1q7cyrfmck2ffu
0004FCC0  32 75 64 33 72 6E 35 6C 35 61 38 79 76 36 66 30  2ud3rn5l5a8yv6f0
0004FCD0  63 68 6B 70 30 7A 70 65 6D 66 20 A9 F2 0A 54 0F  chkp0zpemf ©ò.T.
0004FCE0  33 F8 E8 01 AC 8F F2 45 52 77 D9 6A 76 F1 F0 1A  3øè.¬.òERwÙjvñð.
0004FCF0  01 E4 93 E6 00 78 0A 68 3E 8D 25 92 37 68 2A 55  .ä“æ.x.h>.%’7h*U
```

I compared the HxD translated ASCII to verify its accuracy.

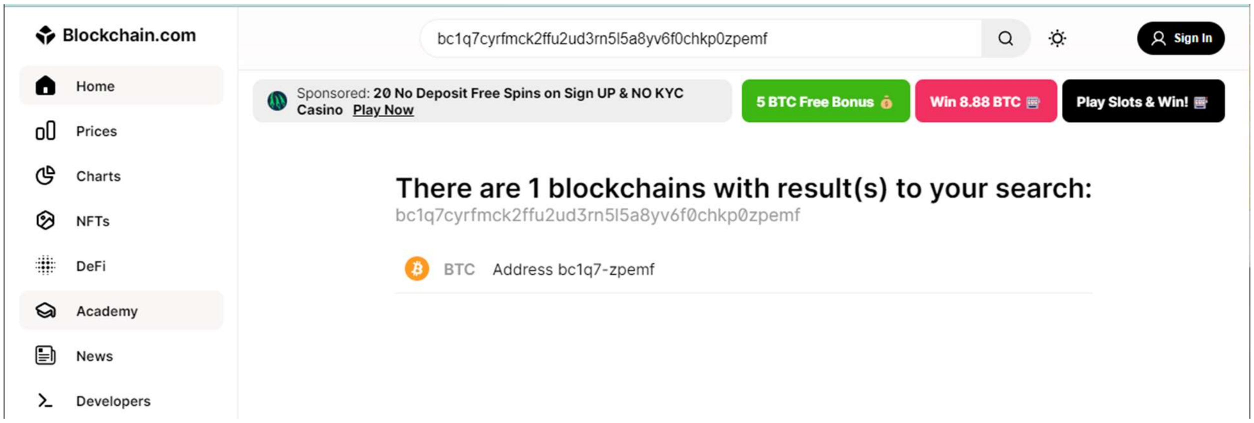
Because the characters matched, I knew the translation was accurate. From the research I conducted, I also knew that bech32 only creates outputs of numbers and letters excluding i, o, b, and 1. The only time b and 1 are used in bech32 is in the beginning.



```
0004FCB0  62 63 31 71 37 63 79 72 66 6D 63 6B 32 66 66 75  bc1q7cyrfmck2ffu
0004FCC0  32 75 64 33 72 6E 35 6C 35 61 38 79 76 36 66 30  2ud3rn5l5a8yv6f0
0004FCD0  63 68 6B 70 30 7A 70 65 6D 66 20 A9 F2 0A 54 0F  chkp0zpemf ©ò.T.
0004FCE0  33 F8 E8 01 AC 8F F2 45 52 77 D9 6A 76 F1 F0 1A  3øè.¬.òERwÙjvñð.
0004FCF0  01 E4 93 E6 00 78 0A 68 3E 8D 25 92 37 68 2A 55  .ä“æ.x.h>.%’7h*U
```

Because of this, I believed that the address was the series of characters leading up to the copyright character.

To test my theory, I entered the values onto Blockchain.com.

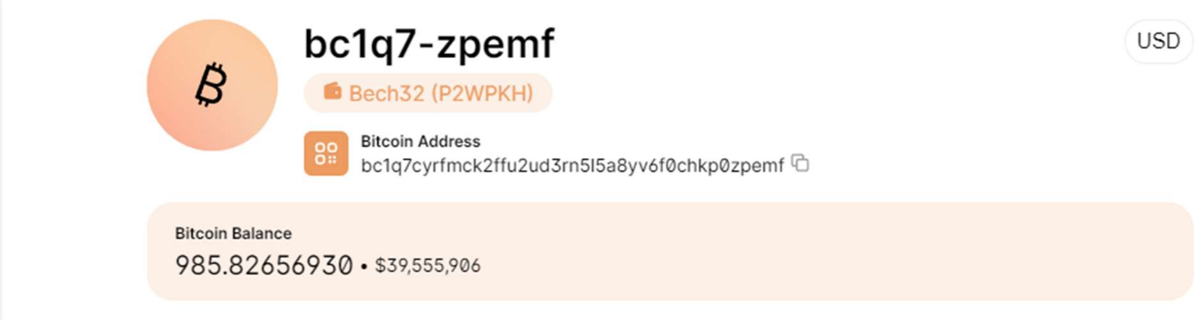


Blockchain.com
bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf
Sign In
Home
Prices
Charts
NFTs
DeFi
Academy
News
Developers
Sponsored: 20 No Deposit Free Spins on Sign UP & NO KYC Casino Play Now
5 BTC Free Bonus
Win 8.88 BTC
Play Slots & Win!

There are 1 blockchains with result(s) to your search:
bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf

BTC Address bc1q7-zpemf

My theory was correct as the address took me to a Bitcoin a bech32 Bitcoin address.



bc1q7-zpemf

Bitcoin Address
bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf

Bitcoin Balance
985.82656930 • $39,555,906

Upon closer inspection I found that the address was to a wallet containing 985.82656930 bitcoin which in that moment was valued at $39,555,906.

Therefore, I was able to conclude that the bitcoin address associated with the sleeper cell is "bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf".

REFERENCES

RapidTables: https://www.rapidtables.com/convert/number/hex-to-ascii.html
I used "RapidTables" to translate hex values to ASCII.

GPS Coordinates Converter: https://www.gps-coordinates.net/gps-coordinates-converter
I used "GPS Coordinates Converter" to determine the location of my coordinates.

Bitcoin Website: https://news.bitcoin.com/everything-you-should-know-about-bitcoin-address-formats/
I used the Bitcoin website to understand Bitcoin and its formats.

Blockchain.com: https://www.blockchain.com/
I used the "Blockchain" website to look up and analyze the Bitcoin address.