GigaHack Cybersecurity challenge 2024

Team members:

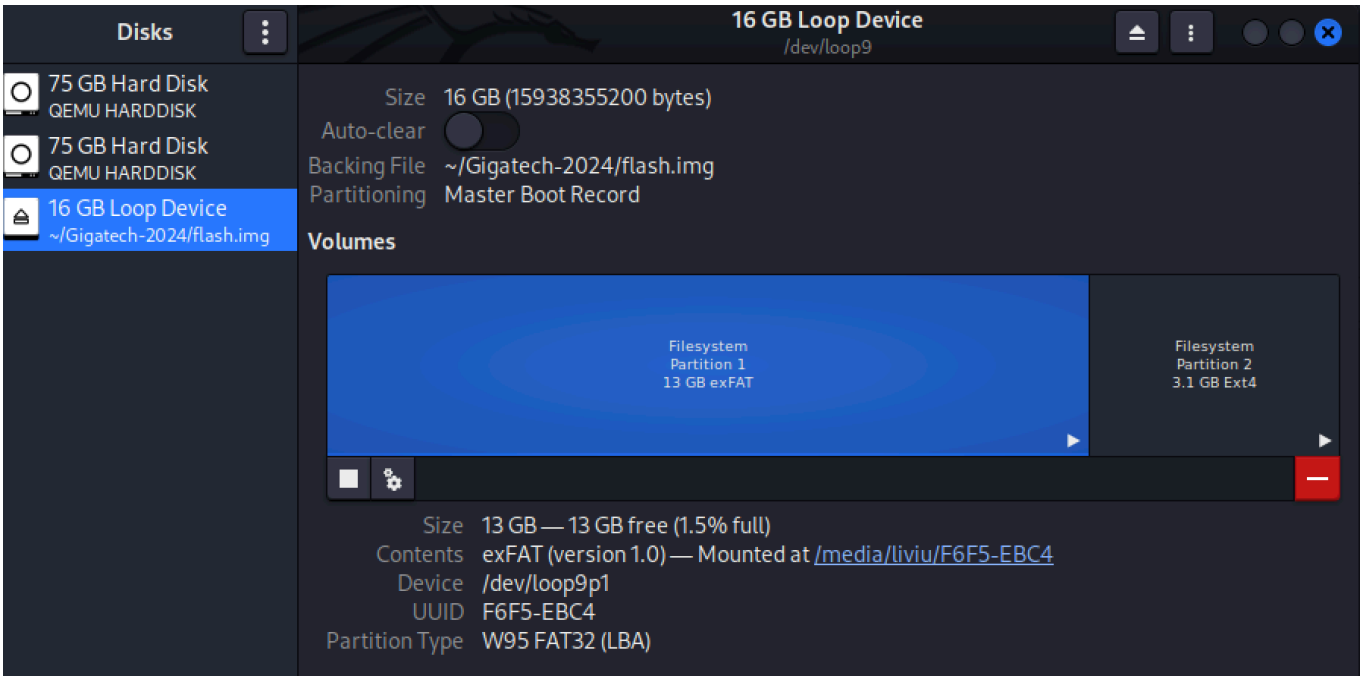
Mereacre Liviu
Mocrenco Artiom
Brinzila Calin
Nicu Iurie
Gidilica Nichita

For some context let's take a look at the challenge description:

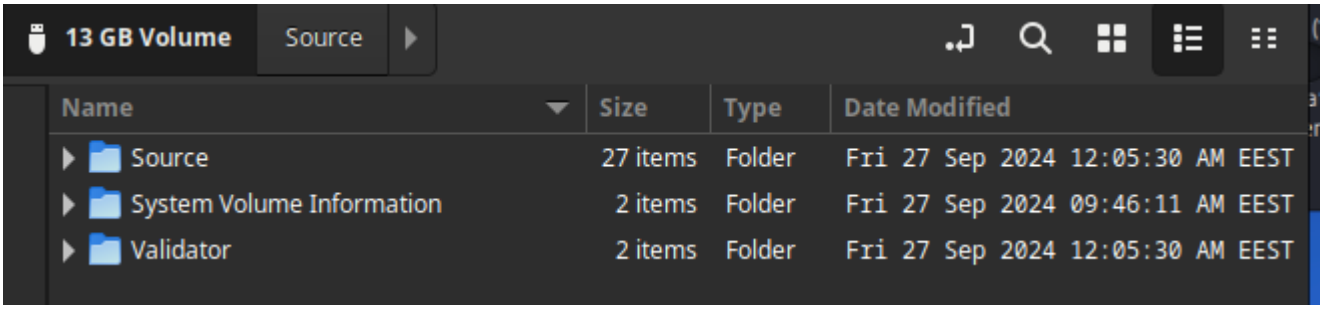
```
The year is 2042. You are a team of Interpol agents involved in the search
for stolen digital works of art.

During the investigation, you discovered a network of underground crypto cat
traders, but all attempts to physically catch at least one of the network
participants were unsuccessful.

Recently, one of your agents reported that there was an offer for the sale
of 2 vintage NFTs, the exact value of which has yet to be determined.

He reported that he had come into possession of a rather old information
storage device that belonged to the leader of a gang of illegal traders
under the pseudonym Byron.

Unfortunately, communication with the agent was interrupted, but a package
was delivered to the division office, the only content of which was this
ancient data storage device.

Using a quantum replicator, we created perfect copies of the device, which
we invite you to study.

For a better immersion into the world of ancient digital artefacts, you were
sent to 2024, where, under the guise of hackathon participants, you will
have to complete the task assigned to you.
```

```
Task: extract maximum useful information from the analysis of the provided
device. You are allowed to use any utilities, operating systems and
artificial intelligence assistance.
```

The "ancient storage device" turned out to be a simple USB Flash Drive that had 2 distinct partitions:

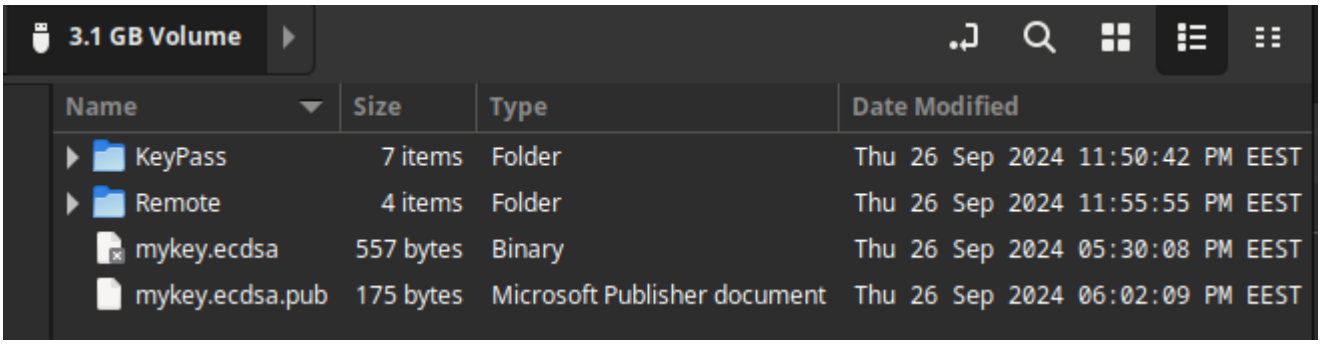


1st partition:



- the Source folder has a bunch of photos
- and the Validator folder has a binary that if executed loops "Gotcha you are dead"

2nd partition:



- 2 folders with duplicate images from the Source folder
- a pub and priv key

Reverse Engineering the found binary

After obtaining the source code we noticed that it is stuck in a infinite loop that spams text to the screen so we just edit the function out.

```
// Validator.Program

using System;

using System.IO;

using System.Security.Cryptography;



internal class Program

{

private static void Main(string[] args)

{

if (1 > args.Length)

{

Console.WriteLine("You forgot something!");
```

```
Environment.Exit(42);

}

string pwd = EBG13(Environment.GetEnvironmentVariable(EBG13("NQN")));

//if (!string.IsNullOrEmpty(pwd) && EBG13(EBG13(pwd)) == "Ybirynpr")

//{

byte[] tmp = File.ReadAllBytes(args[0]);

using (SHA256 sha = SHA256.Create())

{

if (BitConverter.ToString(sha.ComputeHash(tmp)).Replace("-", "").ToLower()
== Path.GetFileNameWithoutExtension(args[0])!.ToLower())

{

Console.WriteLine("Valid");

}

else

{

Console.WriteLine("Invalid");

}

}

Environment.Exit(0);

return;

//}
```

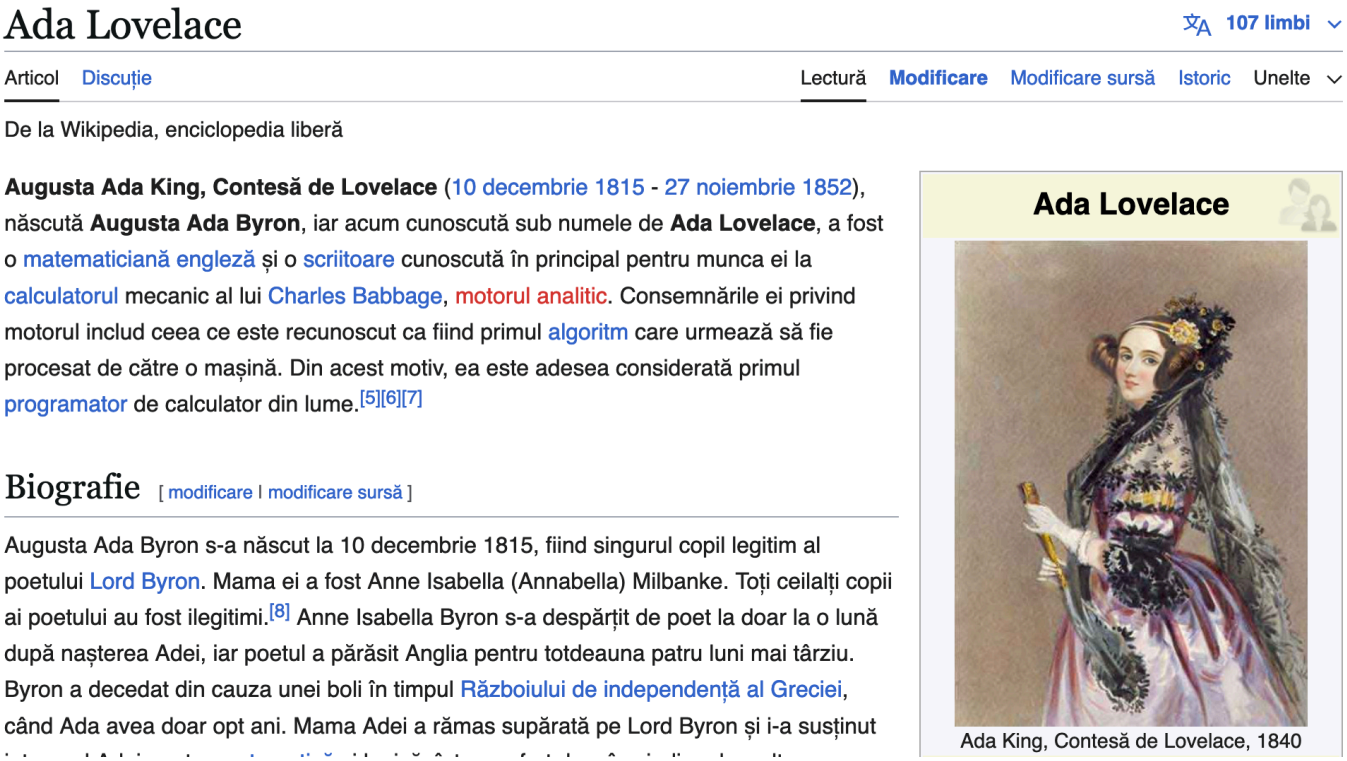
```
//while (true)

//{

// Console.Write("Gotcha! You are dead!");

//}

}



private static string EBG13(string input)

{

if (string.IsNullOrEmpty(input))

{

return null;

}

char[] buffer = new char[input.Length];

for (int i = 0; i < input.Length; i++)

{

char c = input[i];

if (c >= 'a' && c <= 'z')

{

int k = c + 13;

if (k > 122)
```

```
{
k -= 26;
}
buffer[i] = (char)k;
}
else if (c >= 'A' && c <= 'Z')
{
int j = c + 13;
if (j > 90)
{
j -= 26;
}
buffer[i] = (char)j;
}
else
{
buffer[i] = c;
}
}
return new string(buffer);
```

```
}

}
```

The next interesting thing we noticed is a function that performs ROT13 and another that checks a certain env variable(NQN=Ybirynpr), if we reverse the effect of ROT13 on this strings we get that the binary checks if the variable ADA is equal to Lovelace.

This is an obvious hint to this notable figure in CS.



Ada Lovelace

107 limbi

Articol Discuție Lectură **Modificare** Modificare sursă Istoric Unelte

De la Wikipedia, enciclopedia liberă

Augusta Ada King, Contesă de Lovelace (10 decembrie 1815 - 27 noiembrie 1852), născută **Augusta Ada Byron**, iar acum cunoscută sub numele de **Ada Lovelace**, a fost o matematiciană engleză și o scriitoare cunoscută în principal pentru munca ei la calculatorul mecanic al lui Charles Babbage, motorul analitic. Consemnările ei privind motorul includ ceea ce este recunoscut ca fiind primul algoritm care urmează să fie procesat de către o mașină. Din acest motiv, ea este adesea considerată primul programator de calculator din lume.[5][6][7]

Biografie [modificare | modificare sursă]

Augusta Ada Byron s-a născut la 10 decembrie 1815, fiind singurul copil legitim al poetului Lord Byron. Mama ei a fost Anne Isabella (Annabella) Milbanke. Toți ceilalți copii ai poetului au fost ilegitimi.[8] Anne Isabella Byron s-a despărțit de poet la doar la o lună după nașterea Adei, iar poetul a părăsit Anglia pentru totdeauna patru luni mai târziu. Byron a decedat din cauza unei boli în timpul Războiului de independență al Greciei, când Ada avea doar opt ani. Mama Adei a rămas supărată pe Lord Byron și i-a susținut

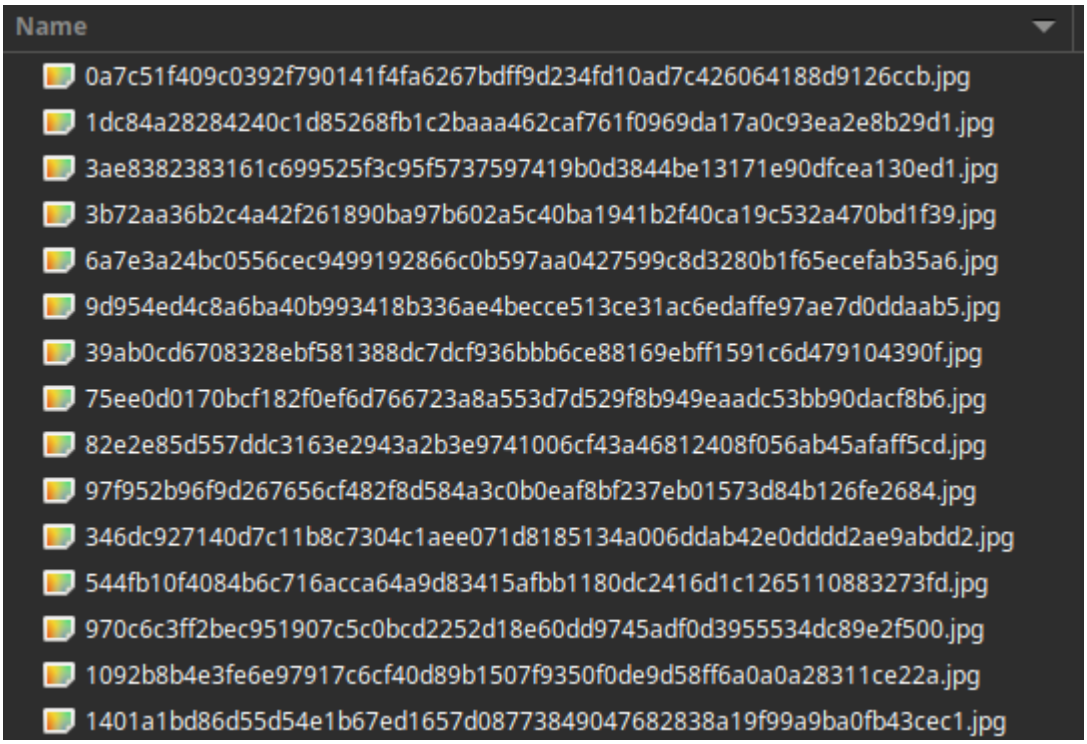
Ada Lovelace

Ada King, Contesă de Lovelace, 1840

If we pass this check we can add files as arguments and it tells us "Valid" or "Invalid". While checking each photo we see that all photos in the Source folder are valid and those from the other partition are all invalid.

Investigating the images

All of the images has a very specific name, a certain size and values:



After some trial and error we noticed that their name is the sha256sum of the file:

```
┌──(liviu㉿kali)-[/media/liviu/F6F5-EBC4/Source]
└─$ sha256sum 0a7c51f409c0392f790141f4fa6267bdff9d234fd10ad7c426064188d9126ccb.jpg
0a7c51f409c0392f790141f4fa6267bdff9d234fd10ad7c426064188d9126ccb  0a7c51f409c0392f790141f4fa6267bdff9d234fd10ad7c426064188d9126ccb.jpg
```

Now we know that the files in the second partition don't pass the Validator check because their names are different from their hash value.

Next thing we did is an excel sheet to help us visualize the differences:

	A	B	C	D	E	F	G
1	Partition	Directory	Image ID	Hash	Filename	Filename matches Hash	Size
2	First	Source	Mountain B	0a7c51f409c0392f790141f4fa6267bdff9d234fd10ad7c426064188d9126ccb	0a7c51f409c0392f790141f4fa6267bdff9d234fd10ad7c426064188d9126ccb.jpg	Yes	21819546
3	First	Source	Space E	1092b8b4e3fe6e97917c6cf40d89b1507f9350f0de9d58ff6a0a0a28311ce22a	1092b8b4e3fe6e97917c6cf40d89b1507f9350f0de9d58ff6a0a0a28311ce22a.jpg	Yes	4870588
4	First	Source	Space C	1401a1bd86d55d54e1b67ed1657d087738490476828 38a19f99a9ba0fb43cec1	1401a1bd86d55d54e1b67ed1657d087738490476828 38a19f99a9ba0fb43cec1.jpg	Yes	6045007
5	First	Source	Beach C	1dc84a28284240c1d85268fb1c2baaa462caf761f0969da17a0c93ea2e8b29d1	1dc84a28284240c1d85268fb1c2baaa462caf761f0969da17a0c93ea2e8b29d1.jpg	Yes	8048954
6	First	Source	Field A	346dc927140d7c11b8c7304c1aee071d8185134a006ddab42e0dddd2ae9abdd2	346dc927140d7c11b8c7304c1aee071d8185134a006ddab42e0dddd2ae9abdd2.jpg	Yes	1921813
7	First	Source	Road A	397996988beed0a27e1d48ff176054dd23005292093bb1c8e649740088 55b9c2	397996988beed0a27e1d48ff176054dd23005292093bb1c8e649740088 55b9c2.jpg	Yes	8110483
8	First	Source	Lake A	39ab0cd6708328ebf581388dc7dcf936bbb6ce88169ebff1591c6d479104390f	39ab0cd6708328ebf581388dc7dcf936bbb6ce88169ebff1591c6d479104390f.jpg	Yes	4732060
9	First	Source	Mountain A	3ae8382383161c699525f3c95f5737597419b0d3844be13171e90dfcea130ed1	3ae8382383161c699525f3c95f5737597419b0d3844be13171e90dfcea130ed1.jpg	Yes	2717389
10	First	Source	Space A	3b72aa36b2c4a42f261890ba97b602a5c40ba1941b2f40ca19c532a470bd1f39	3b72aa36b2c4a42f261890ba97b602a5c40ba1941b2f40ca19c532a470bd1f39.jpg	Yes	3271594
11	First	Source	Lake B	544fb10f4084b6c716acca64a9d83415afbb1180dc2416d1c1265110883273fd	544fb10f4084b6c716acca64a9d83415afbb1180dc2416d1c1265110883273fd.jpg	Yes	4380557
12	First	Source	Beach B	5876887a860d2634b48a0a766128261cc69f63cb3d00f5793e399e3b2d2111fb	5876887a860d2634b48a0a766128261cc69f63cb3d00f5793e399e3b2d2111fb.jpg	Yes	290138
13	First	Source	Space D	6a7e3a24bc0556cec9499192866c0b597aa0427599c8d3280b1f65ecefab35a6	6a7e3a24bc0556cec9499192866c0b597aa0427599c8d3280b1f65ecefab35a6.jpg	Yes	7982047
14	First	Source	Field D	75ee0d0170bcf182f0ef6d766723a8a553d7d529f8b949eaadc53bb90dacf8b6	75ee0d0170bcf182f0ef6d766723a8a553d7d529f8b949eaadc53bb90dacf8b6.jpg	Yes	12566660
15	First	Source	Waterfall B	82e2e85d557ddc3163e2943a2b3e9741006cf43a46812408f056ab45afaff5cd	82e2e85d557ddc3163e2943a2b3e9741006cf43a46812408f056ab45afaff5cd.jpg	Yes	8447436
16	First	Source	Tree B	970c6c3ff2bec951907c5c0bcd2252d18e60dd9745adf0d3955534dc89e2f500	970c6c3ff2bec951907c5c0bcd2252d18e60dd9745adf0d3955534dc89e2f500.jpg	Yes	3655537
17	First	Source	Field C	97f952b96f9d267656cf482f8d584a3c0b0eaf8bf237eb01573d84b126fe2684	97f952b96f9d267656cf482f8d584a3c0b0eaf8bf237eb01573d84b126fe2684.jpg	Yes	1689092
18	First	Source	City A	9d954ed4c8a6ba40b993418b336ae4becce513ce31ac6edaffe97ae7d0ddaab5	9d954ed4c8a6ba40b993418b336ae4becce513ce31ac6edaffe97ae7d0ddaab5.jpg	Yes	2158884
19	First	Source	Beach D	b76688b88fae5879e52ffb6ac74b08d38e973e1a2f7fb2e467c8e77836ad22a1	b76688b88fae5879e52ffb6ac74b08d38e973e1a2f7fb2e467c8e77836ad22a1.jpg	Yes	4058373
20	First	Source	Space F	bb0236e303f2ed69eb49466bbd961d178948234114b68a6ca84c569fa5ffb219	bb0236e303f2ed69eb49466bbd961d178948234114b68a6ca84c569fa5ffb219.jpg	Yes	4190674
21	First	Source	Space G	c67b777c47ef1fbc69a6ea47a1dc9095742f8f3c8d771040e301799bb2fb4ecb	c67b777c47ef1fbc69a6ea47a1dc9095742f8f3c8d771040e301799bb2fb4ecb.jpg	Yes	12830525
22	First	Source	Turtle A	ce5d0ed4f3b8641b8fc7e60d1c02de4241c63a119b7990477a6a85784451355f	ce5d0ed4f3b8641b8fc7e60d1c02de4241c63a119b7990477a6a85784451355f.jpg	Yes	7444941
23	First	Source	Space B	cfa686e6fb78330092b69ca8cc15df29bdb702c84e3dca2b40e3ff007f235a2d	cfa686e6fb78330092b69ca8cc15df29bdb702c84e3dca2b40e3ff007f235a2d.jpg	Yes	4232448
24	First	Source	Field B	d6b1ef3dfd2223b73b87f3b7c2a9d7bc270136440236915554 3d6f43fdd51431	d6b1ef3dfd2223b73b87f3b7c2a9d7bc270136440236915554 3d6f43fdd51431.jpg	Yes	4067765
25	First	Source	Beach A	e8c0801cc699e6b6582c4dc115fd045738820e6b21e916bd927f0d03fab533fd	e8c0801cc699e6b6582c4dc115fd045738820e6b21e916bd927f0d03fab533fd.jpg	Yes	6327159
26	First	Source	Tree A	eda921415a263025ff0456b582fd8710965639fc84f63d68c23349e780fcb4ec	eda921415a263025ff0456b582fd8710965639fc84f63d68c23349e780fcb4ec.jpg	Yes	5916835
27	First	Source	Tree C	f22cc5805b9834280d2465ec0784964e07cb39dff426c0257f067299943000 71	f22cc5805b9834280d2465ec0784964e07cb39dff426c0257f067299943000 71.jpg	Yes	14630633
28	First	Source	Waterfall A	f90fa2d93b4cd61b8321bff7e9d880f898379244fa3f90bddfe0c85b28bcdccb	f90fa2d93b4cd61b8321bff7e9d880f898379244fa3f90bddfe0c85b28bcdccb.jpg	Yes	20299747
29	Second	Remote	Space E	1092b8b4e3fe6e97917c6cf40d89b1507f9350f0de9d58ff6a0a0a28311ce22a	007db8b4e3fe6e97917c6cf40d89b1507f9350f0de9d58ff6a0a0a28311ce22a.jpg	No	4870588
30	Second	Remote	Beach C	1dc84a28284240c1d85268fb1c2baaa462caf761f0969da17a0c93ea2e8b29d1	01fb4a28284240c1d85268fb1c2baaa462caf761f0969da17a0c93ea2e8b29d1.jpg	No	8048954
31	Second	Remote	Tree A	eda921415a263025ff0456b582fd8710965639fc84f63d68c23349e780fcb4ec	02b421415a263025ff0456b582fd8710965639fc84f63d68c23349e780fcb4ec.jpg	No	5916835
32	Second	Remote	Tree C	f22cc5805b9834280d2465ec0784964e07cb39dff426c0257f067299943000 71	03c2c5805b9834280d2465ec0784964e07cb39dff426c0257f067299943000 71.jpg	No	14630633
33	Second	KeyPass	Beach B	5876887a860d2634b48a0a766128261cc69f63cb3d00f5793e399e3b2d2111fb	4376887a860d2634b48a0a766128261cc69f63cb3d00f5793e399e3b2d2111fb.jpg	No	290138
34	Second	KeyPass	Space D	6a7e3a24bc0556cec9499192866c0b597aa0427599c8d3280b1f65ecefab35a6	6a613a24bc0556cec9499192866c0b597aa0427599c8d3280b1f65ecefab35a6.jpg	No	7982047
35	Second	KeyPass	Field D	75ee0d0170bcf182f0ef6d766723a8a553d7d529f8b949eaadc53bb90dacf8b6	75ee720170bcf182f0ef6d766723a8a553d7d529f8b949eaadc53bb90dacf8b6.jpg	No	12566660
36	Second	KeyPass	Waterfall B	82e2e85d557ddc3163e2943a2b3e9741006cf43a46812408f056ab45afaff5cd	82e2e864557ddc3163e2943a2b3e9741006cf43a46812408f056ab45afaff5cd.jpg	No	8447436
37	Second	KeyPass	Tree B	970c6c3ff2bec951907c5c0bcd2252d18e60dd9745adf0d3955534dc89e2f500	970c6c3f61bec951907c5c0bcd2252d18e60dd9745adf0d3955534dc89e2f500.jpg	No	3655537
38	Second	KeyPass	Field C	97f952b96f9d267656cf482f8d584a3c0b0eaf8bf237eb01573d84b126fe2684	97f952b96f6e267656cf482f8d584a3c0b0eaf8bf237eb01573d84b126fe2684.jpg	No	1689092
39	Second	KeyPass	City A	9d954ed4c8a6ba40b993418b336ae4becce513ce31ac6edaffe97ae7d0ddaab5	9d954ed4c8a66f40b993418b336ae4becce513ce31ac6edaffe97ae7d0ddaab5.jpg	No	2158884
40							

After trying a bunch of encodings hex->ASCII gave us a promising result, the differences from the Keepass folder are very easily converted like so:

- 43 = C

- 61 = a
- 72 = r
- 64 = d
- 61 = a
- 6e = n
- 6f = o

We noticed a pattern, the values from the Remote folder were ascending (00, 01, 02 and 03) and we guessed that the remaining 2 values are also hex:

Each two hex digits can be converted into a decimal number:

- 00 = 0
- 7d = 125
- 01 = 1
- fb = 251
- 02 = 2
- b4 = 180
- 03 = 3
- c2 = 194

This looks exactly like an IP but when we try it it doesn't work so we try to reverse it:

-instead of: 125.251.180.194
-we try: 194.180.251.125

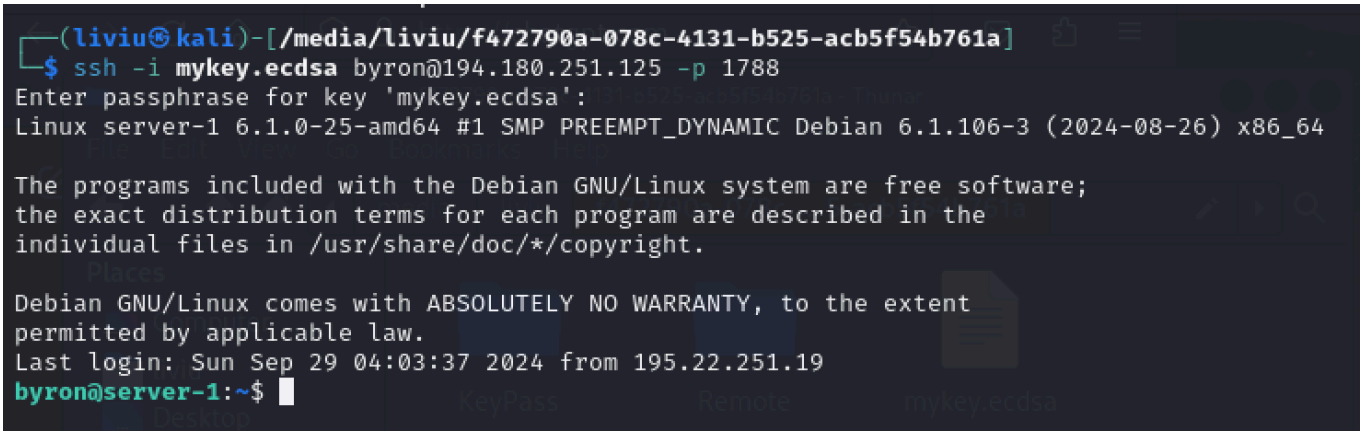
```
role:           Sergiu IANCIUC
address:        Miron Costin 3/1
address:        MD-2068
address:        Chisinau
address:        MOLDOVA, REPUBLIC OF
phone:          +37332777777
nic-hdl:        SI4154-RIPE
mnt-by:         mnt-md-itns-net-mnt16-1
created:        2019-11-22T14:09:39Z
last-modified:  2020-05-30T15:55:59Z
source:         RIPE # Filtered
```

We see that this Ip works and also it's from Moldova!

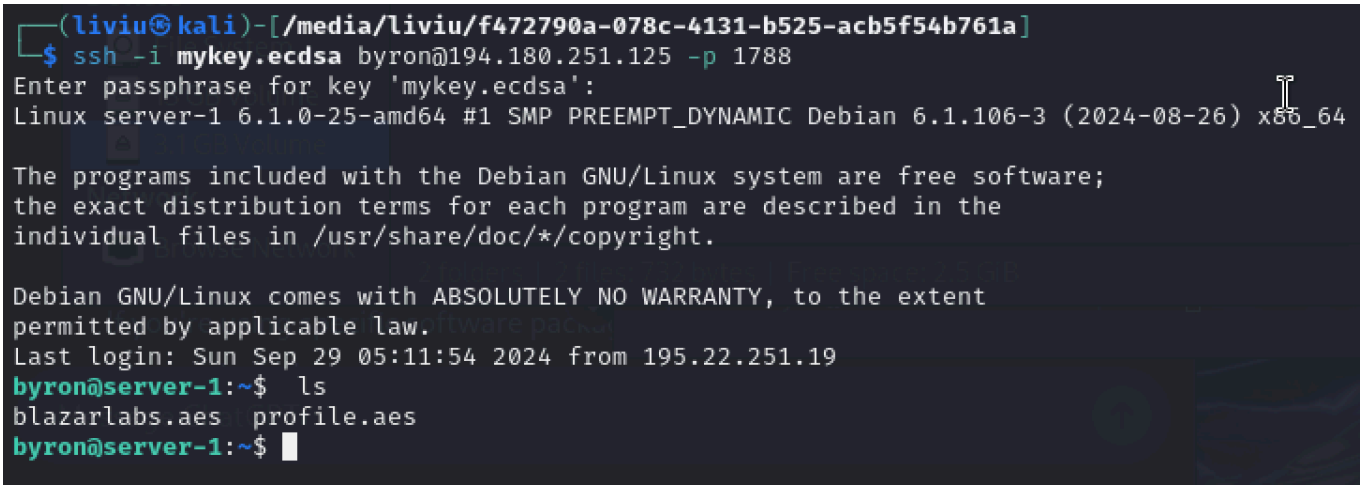
Gaining Access

After a nmap scan we see that port 1788 is open and supports ssh.

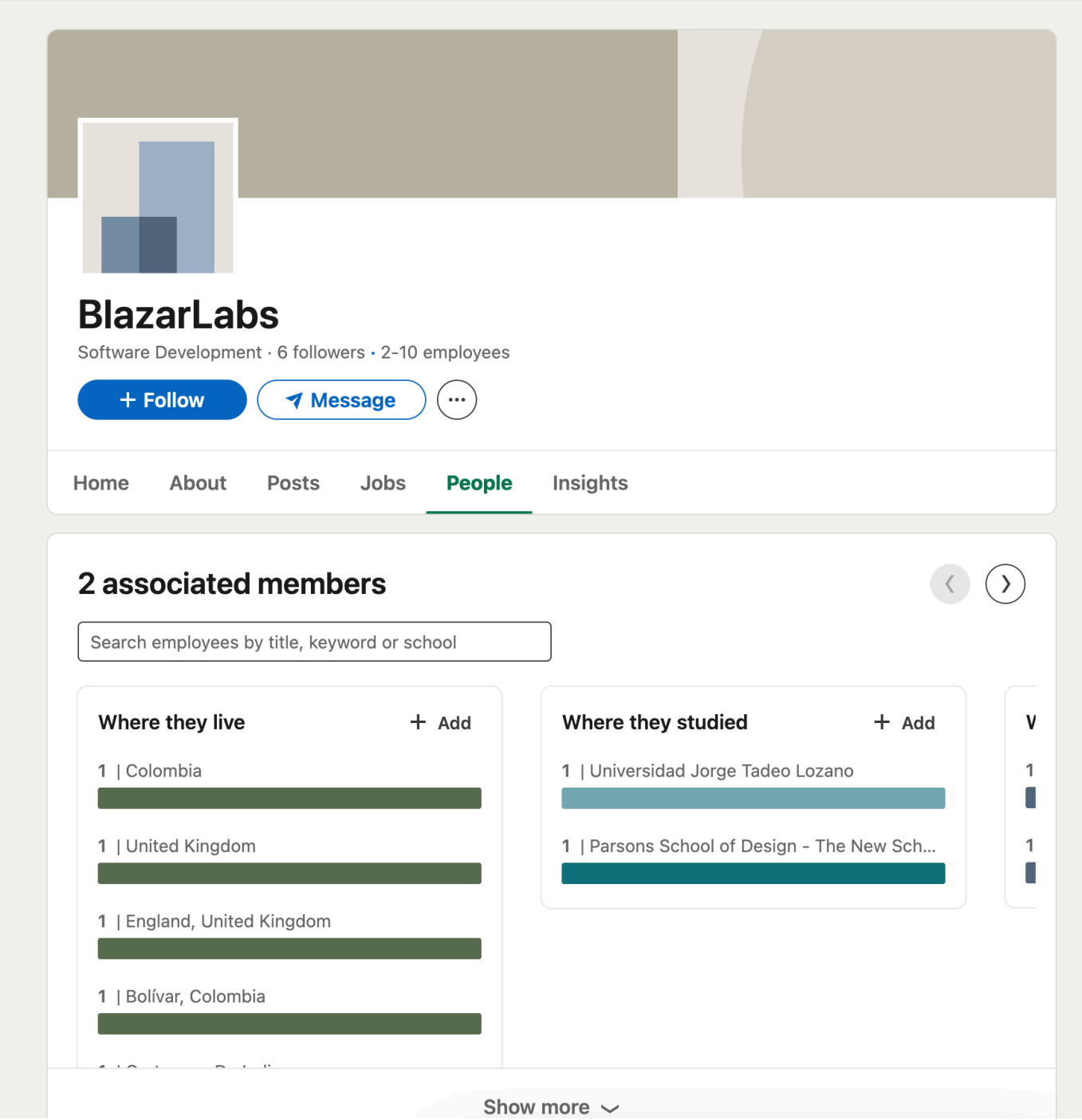
Next we try to connect to it via ssh, with the sshkeys from the usb drive using the crime leaders name "byron" and using the password "Cardano".



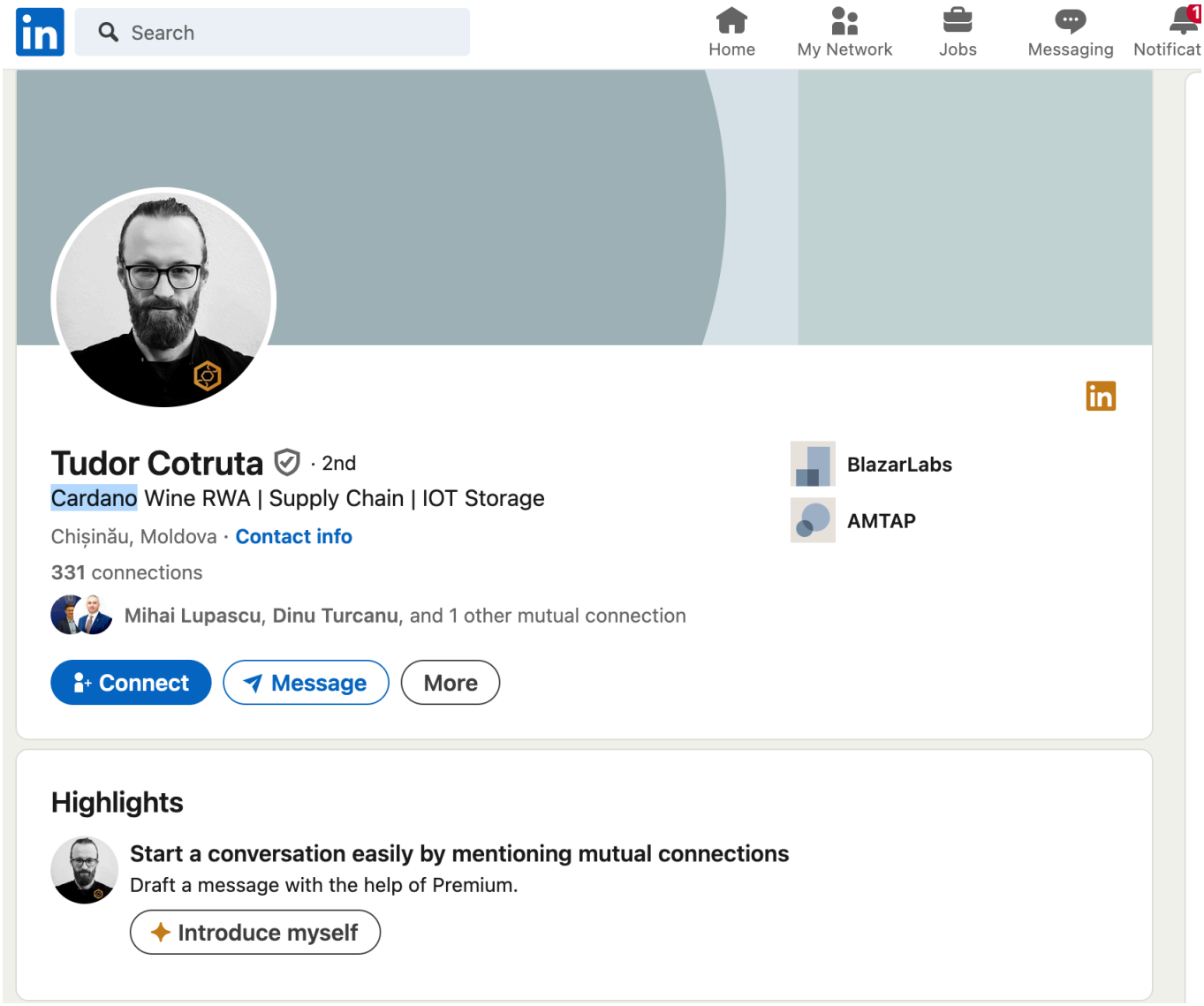
Inside we see 2 very interesting files, and these are the wallet key and the second is probably used to show us how it was made:



The first file seems common but the first has a very distinct name so we do a little google-fu, first we find a company with the same name that develops WEB3 tech:

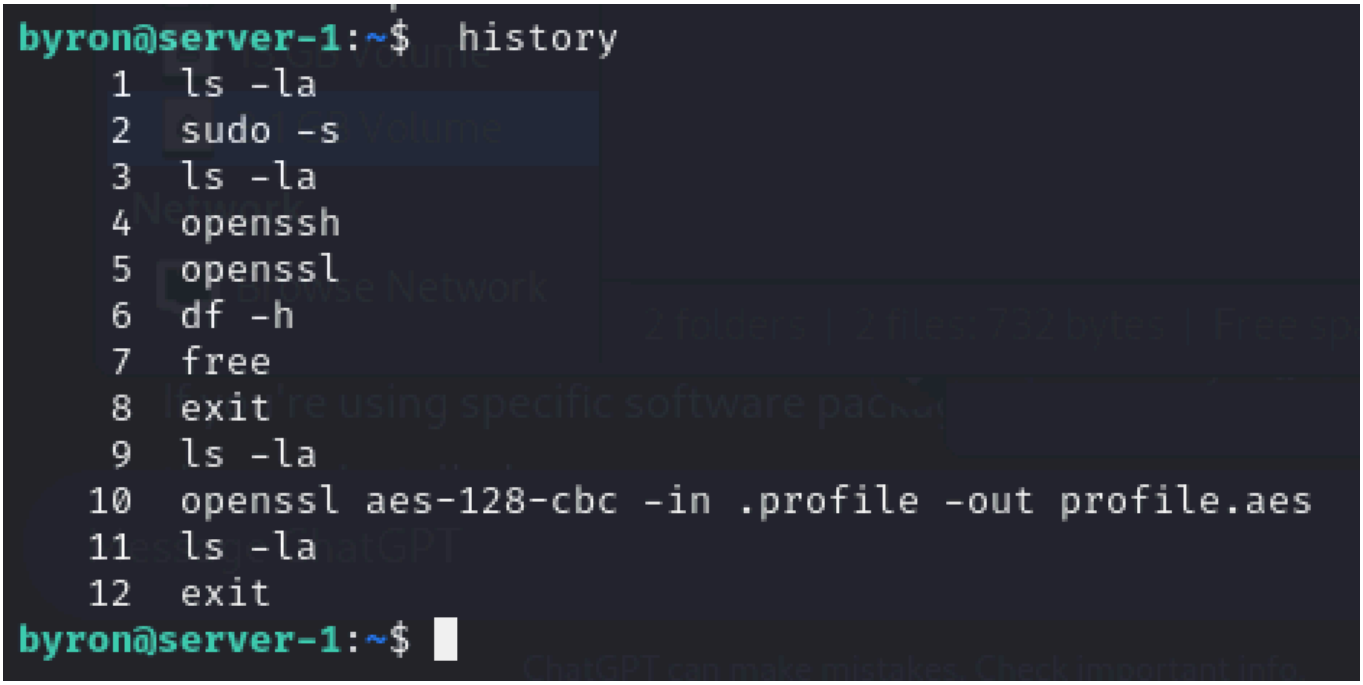


They have employees from Moldova so it seems like we are the right track:


Search
Home
My Network
Jobs
Messaging
Notificat
Tudor Cotruta · 2nd
Cardano Wine RWA | Supply Chain | IOT Storage
Chișinău, Moldova · Contact info
331 connections
Mihai Lupascu, Dinu Turcanu, and 1 other mutual connection
Connect
Message
More
BlazarLabs
AMTAP
Highlights
Start a conversation easily by mentioning mutual connections
Draft a message with the help of Premium.
Introduce myself

Decryption

Here we can see how another file was encrypted:



This knowledge enables us to perform a Known-plaintext attack and retrieve the password of profile.aes which is "Lovelace".

Using the same password we decrypt the blazarlabs.aes and we get a screenshot of the wallet app name and the seed phrase. Obviously the next thing we did is login into this wallet and transfer all the contents into out wallet.

New Transaction

1 Cardano Address

addr1q925x9kmpfjup44684lvcfg8c68w7dvlpqr3ag0w2q9a9vxqx63
l2kvf8d6pazrm4st0zjud40wk0rfqnne933mhw5cq7ey8p9

2 Tokens

198.64666 Ada

3 Collectibles

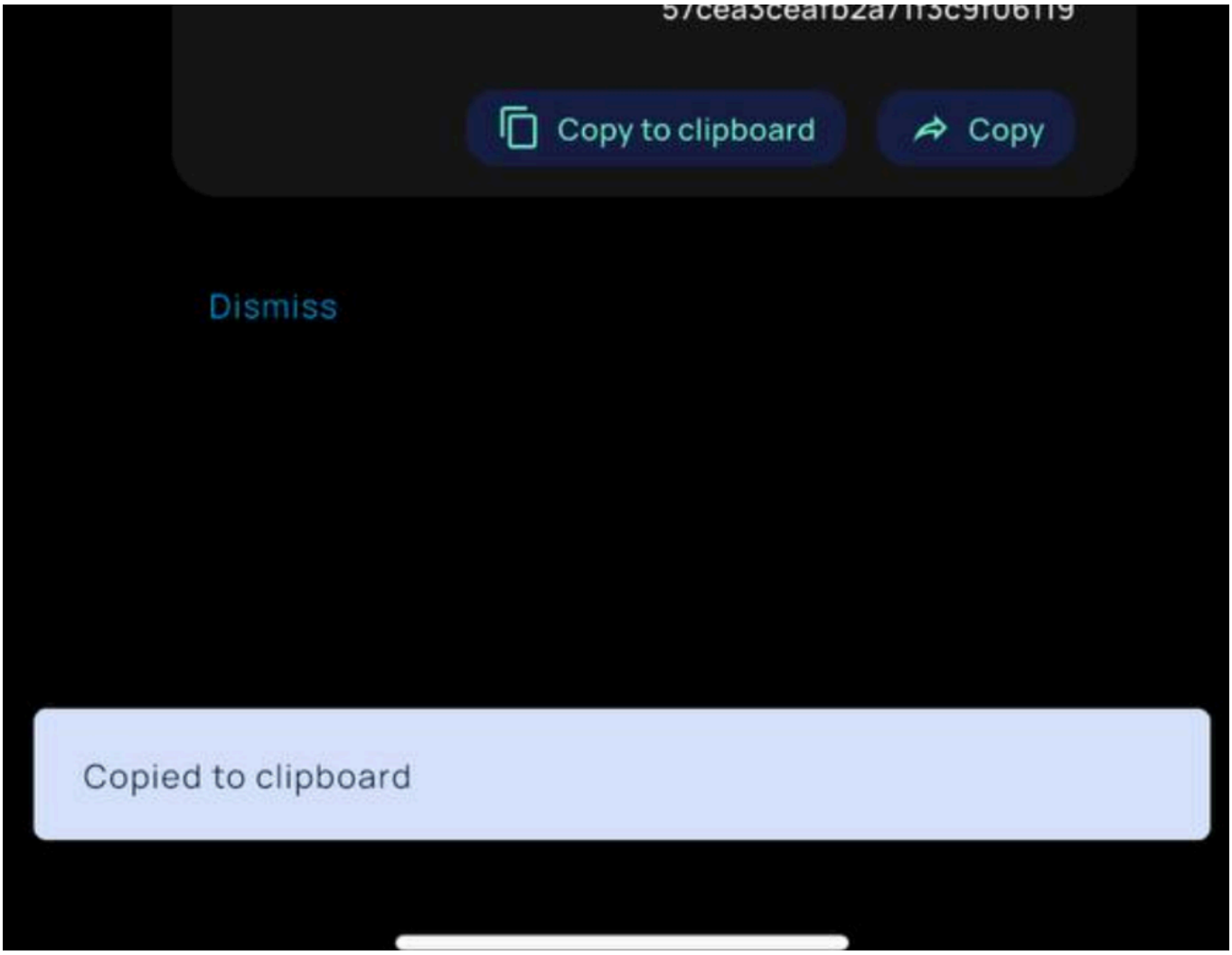
Wisdom#0257
Easelle#0127

4 Fees Overview

Total fees: 0.172233₳

5 ✓ Transaction Submitted

Tx Hash 6b359b1b5ac0b34b5b0d8a811fcae2329d3dce2


57cea3cea1b2a7113c9f06119
Copy to clipboard
Copy
Dismiss
Copied to clipboard

14:29 4G 46

HEX team

$78.22

+ Buy ADA

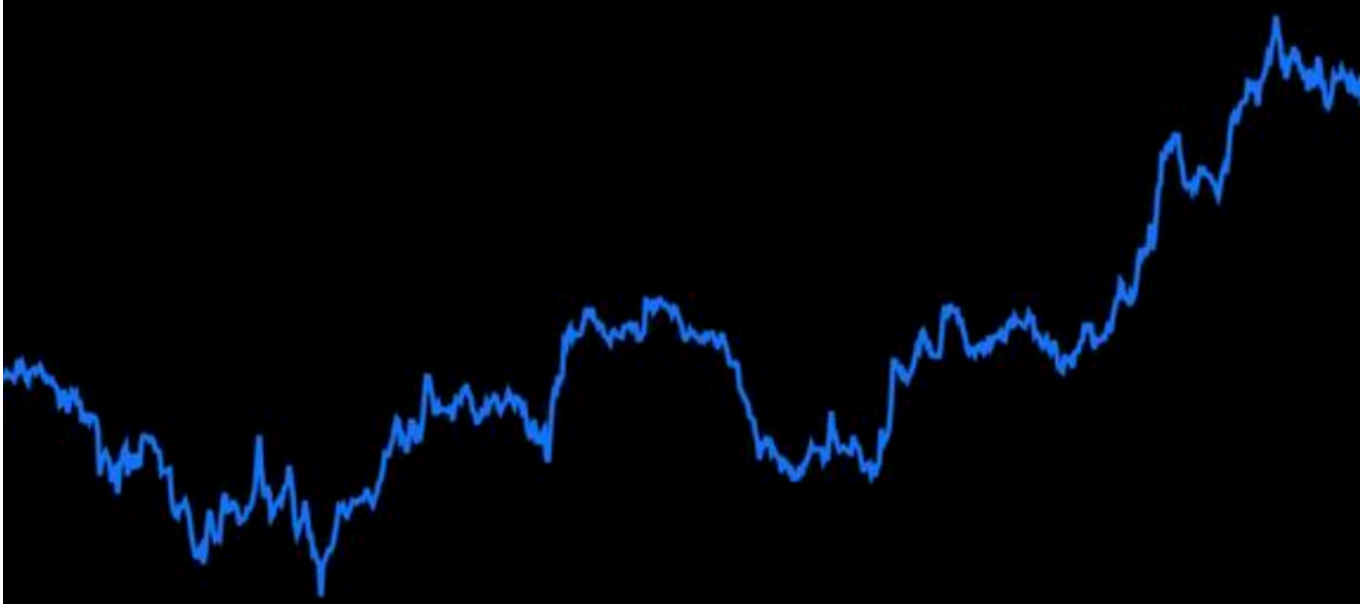
Portfolio Balance

Cardano

198.65 ADA

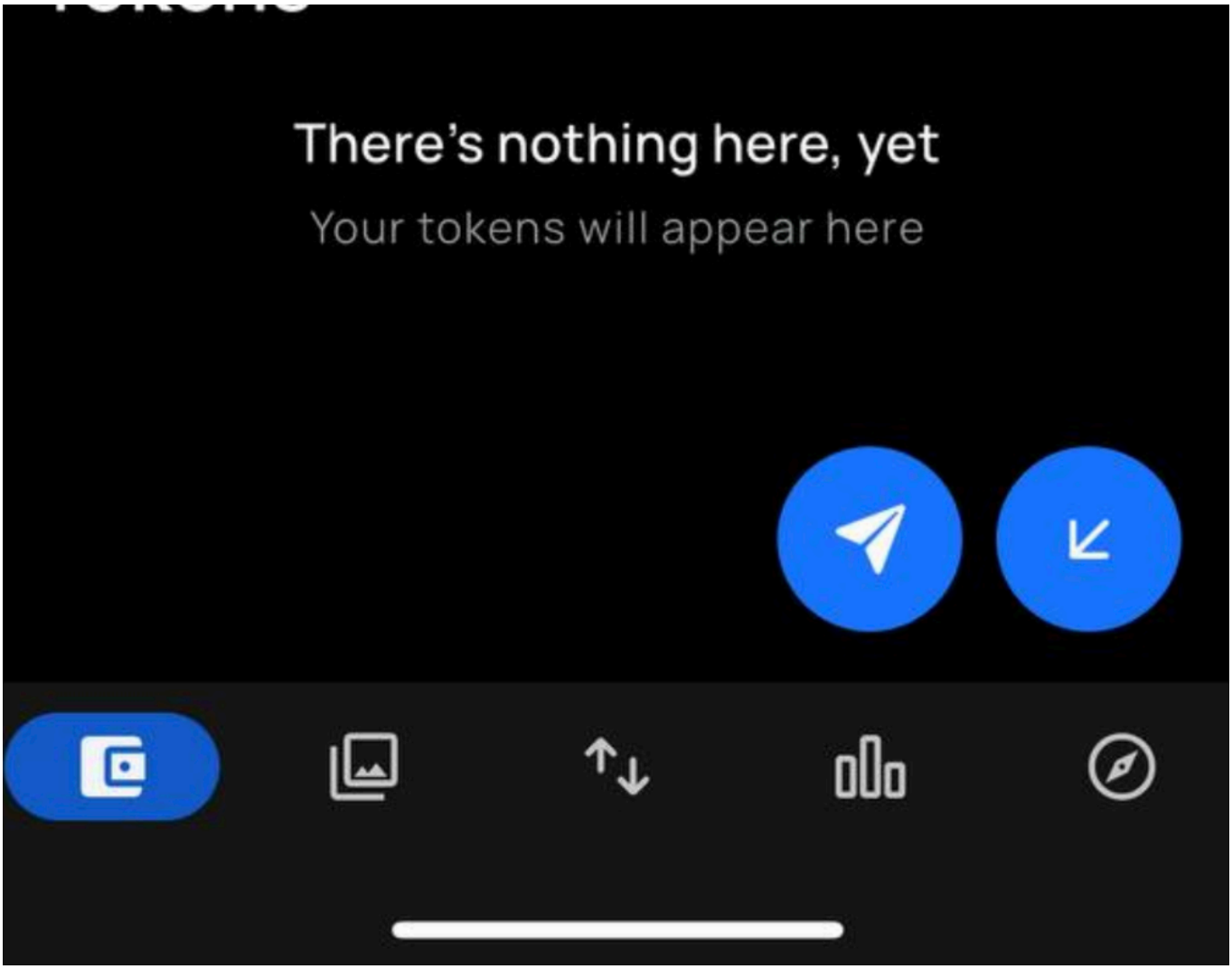
$0.39 +12.25%

$78.22



1 Y 3 M 1 M 1 W 24 H

Tokens


There’s nothing here, yet
Your tokens will appear here

14:29 4G 46

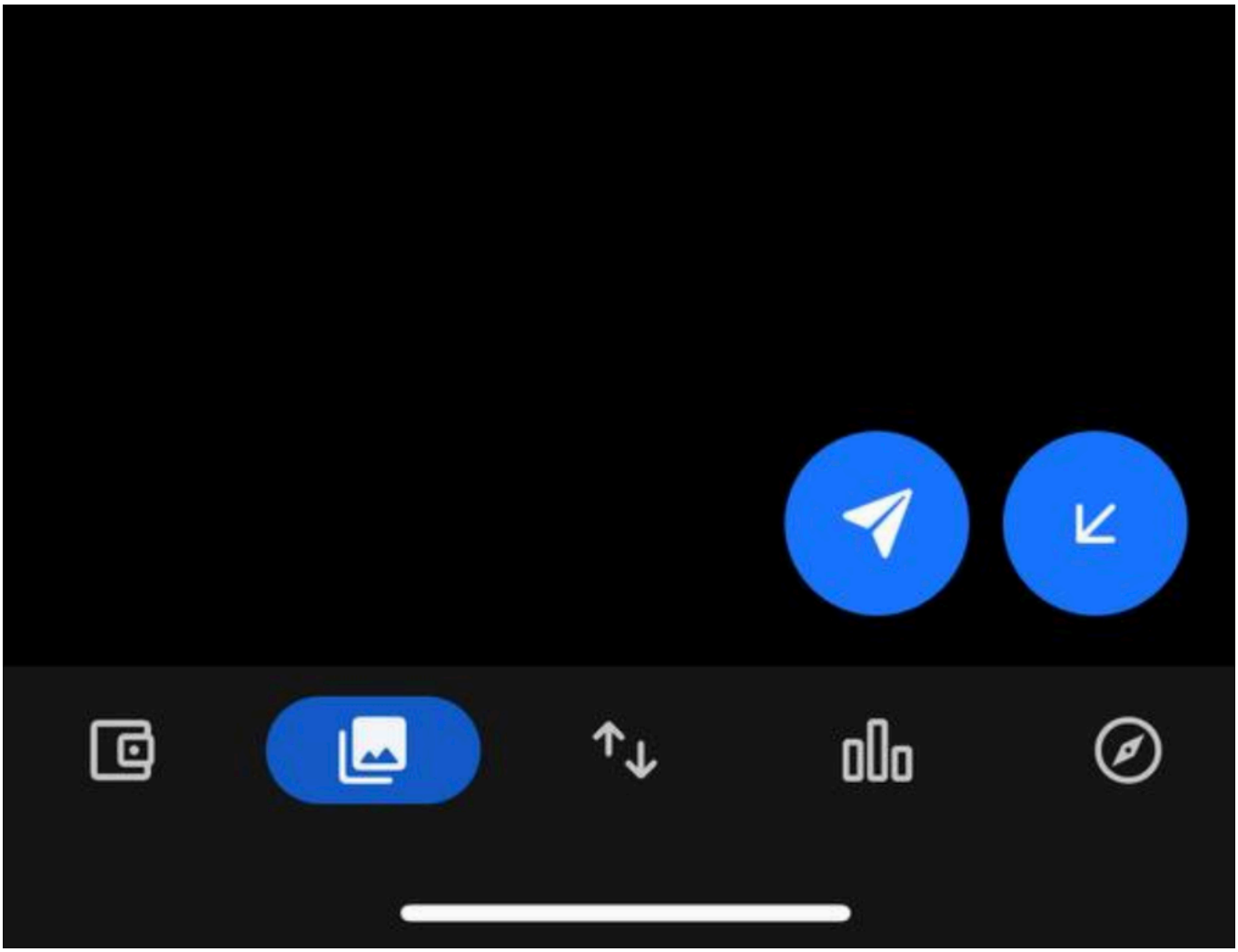
Collectibles

For Sale

Search collectibles

Wisdom Proxies
Floor price: 44 ADA
1 NFTs >

CardanoProxies
Floor price: 32 ADA
1 NFTs >



This is how we completed the challenge.

-HEX team