The story of the "Uncrackable" Lockbox, and Why Hackers Need to Work Alongside Developers

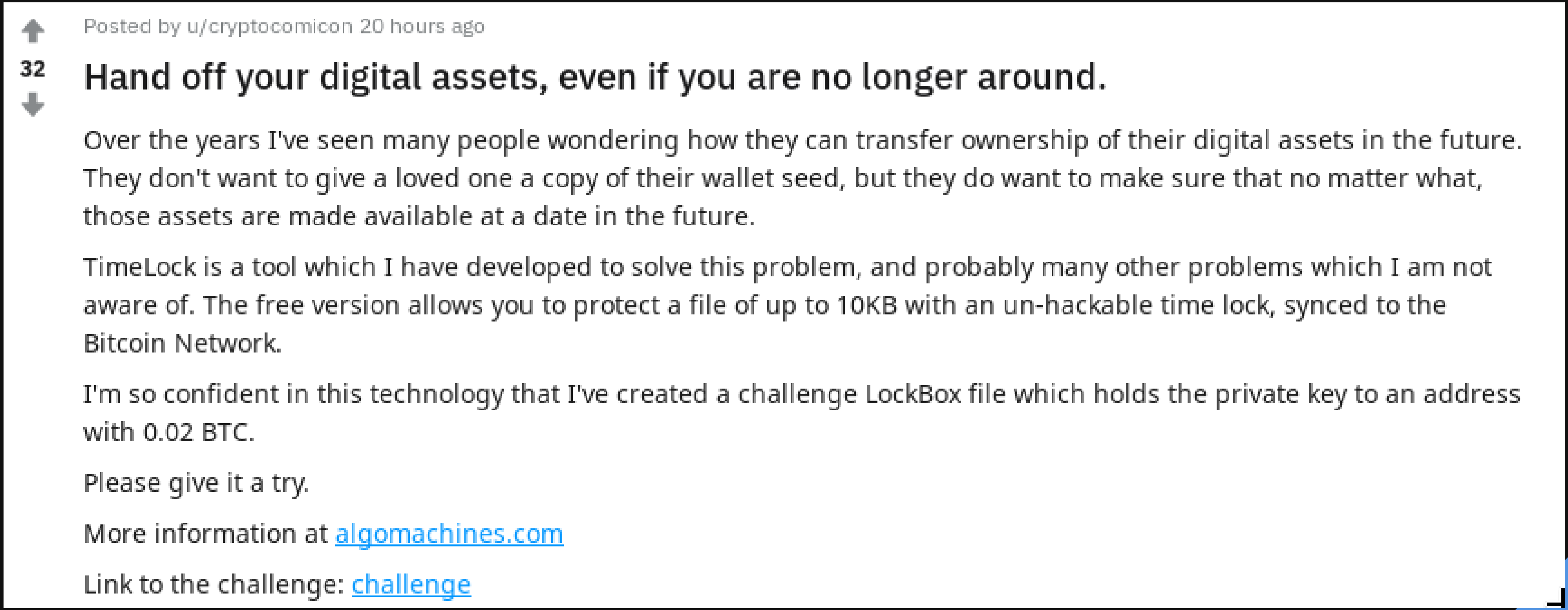
Matthew Ruffell

Kawaiicon 2019

What is TimeLock?

- Homemade encryption program.
  - Made by u/cryptocomicon, of algomachines.com
- Implements a time-sensitive lock.
- In order to test it’s security, challenges were posted to Reddit
  - “Lockboxes” contain a 0.02 BTC private key.
- We will cover 5 simple vulnerabilities.

Challenge #1



Posted by u/cryptocomicon 20 hours ago

32

Hand off your digital assets, even if you are no longer around.

Over the years I've seen many people wondering how they can transfer ownership of their digital assets in the future. They don't want to give a loved one a copy of their wallet seed, but they do want to make sure that no matter what, those assets are made available at a date in the future.

TimeLock is a tool which I have developed to solve this problem, and probably many other problems which I am not aware of. The free version allows you to protect a file of up to 10KB with an un-hackable time lock, synced to the Bitcoin Network.

I'm so confident in this technology that I've created a challenge LockBox file which holds the private key to an address with 0.02 BTC.

Please give it a try.

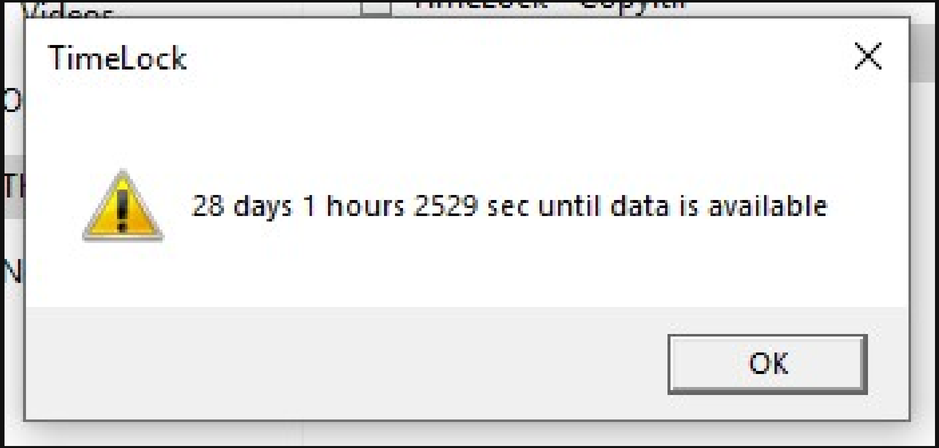
More information at algomachines.com

Link to the challenge: challenge

Information and Scope

- We are given:
  - Password - “TimeLock”.
  - Answers to questions - “0.02”.
  - Time range – Start and end, both UTC.
- This limits scope to time lock mechanism only.

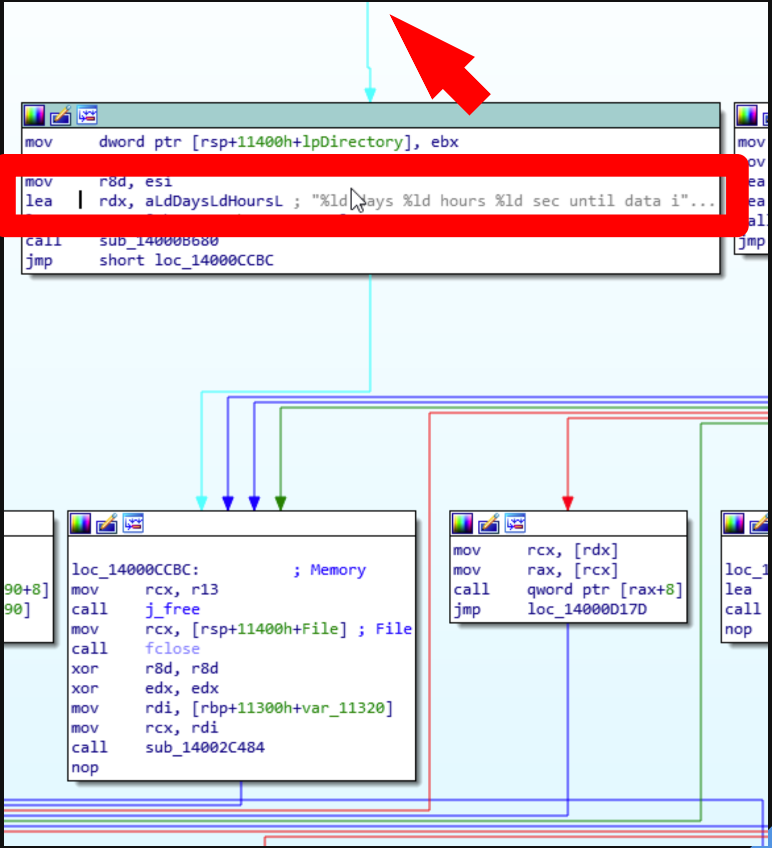
Xref Strings – Hackers Best Friend



TimeLock

28 days 1 hours 2529 sec until data is available

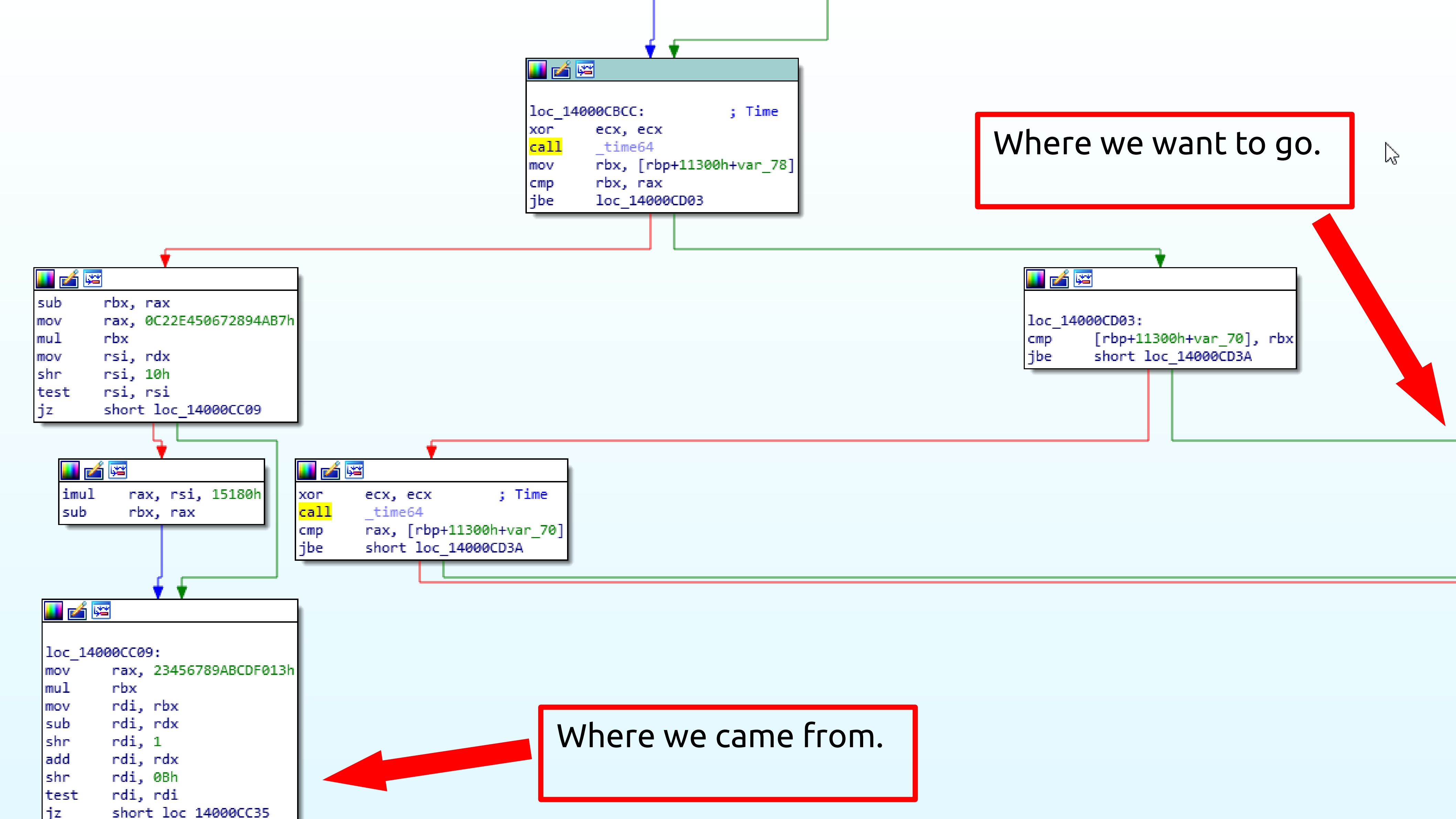
- “%ld days %ld hours %ld sec until data is available”
- “Select folder where %s will be created”



```
mov     dword ptr [rsp+11400h+lpDirectory], ebx
mov     r8d, esi
lea     rdx, aLdDaysLdHoursL ; "%ld days %ld hours %ld sec until data i"...
call    sub_14000B680
jmp     short loc_14000CCBC
```

```
loc_14000CCBC:          ; Memory
mov     rcx, r13
call    j_free
mov     rcx, [rsp+11400h+File] ; File
call    fclose
xor     r8d, r8d
xor     edx, edx
mov     rdi, [rbp+11300h+var_11320]
mov     rcx, rdi
call    sub_14002C484
nop
```

```
mov     rcx, [rdx]
mov     rax, [rcx]
call    qword ptr [rax+8]
jmp     loc_14000D17D
```



```
loc_14000CBCC:              ; Time
xor     ecx, ecx
call    _time64
mov     rbx, [rbp+11300h+var_78]
cmp     rbx, rax
jbe     loc_14000CD03
```

```
sub     rbx, rax
mov     rax, 0C22E450672894AB7h
mul     rbx
mov     rsi, rdx
shr     rsi, 10h
test    rsi, rsi
jz      short loc_14000CC09
```

```
loc_14000CD03:
cmp     [rbp+11300h+var_70], rbx
jbe     short loc_14000CD3A
```

```
imul    rax, rsi, 15180h
sub     rbx, rax
```

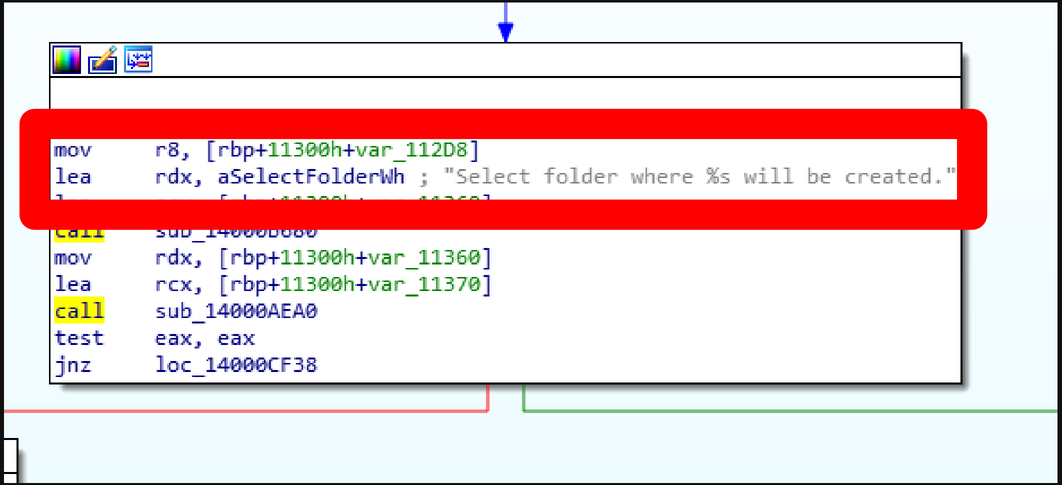
```
xor     ecx, ecx            ; Time
call    _time64
cmp     rax, [rbp+11300h+var_70]
jbe     short loc_14000CD3A
```

```
loc_14000CC09:
mov     rax, 23456789ABCDF013h
mul     rbx
mov     rdi, rbx
sub     rdi, rdx
shr     rdi, 1
add     rdi, rdx
shr     rdi, 0Bh
test    rdi, rdi
jz      short loc_14000CC35
```

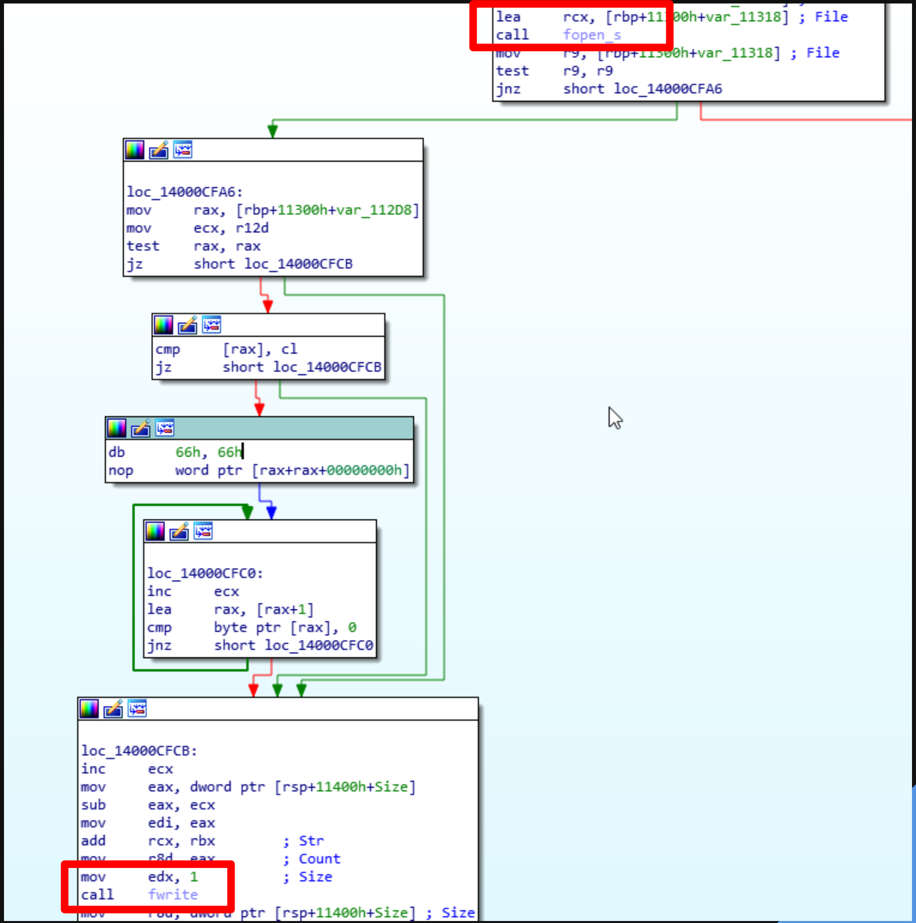
Where we want to go.

Where we came from.

“True” Path Leads to File Writing



```
mov     r8, [rbp+11300h+var_112D8]
lea     rdx, aSelectFolderWh ; "Select folder where %s will be created."
call    sub_14000B680
mov     rdx, [rbp+11300h+var_11360]
lea     rcx, [rbp+11300h+var_11370]
call    sub_14000AEA0
test    eax, eax
jnz     loc_14000CF38
```



```
lea     rcx, [rbp+11300h+var_11318] ; File
call    fopen_s
mov     r9, [rbp+11300h+var_11318] ; File
test    r9, r9
jnz     short loc_14000CFA6
```

```
loc_14000CFA6:
mov     rax, [rbp+11300h+var_112D8]
mov     ecx, r12d
test    rax, rax
jz      short loc_14000CFCB
```

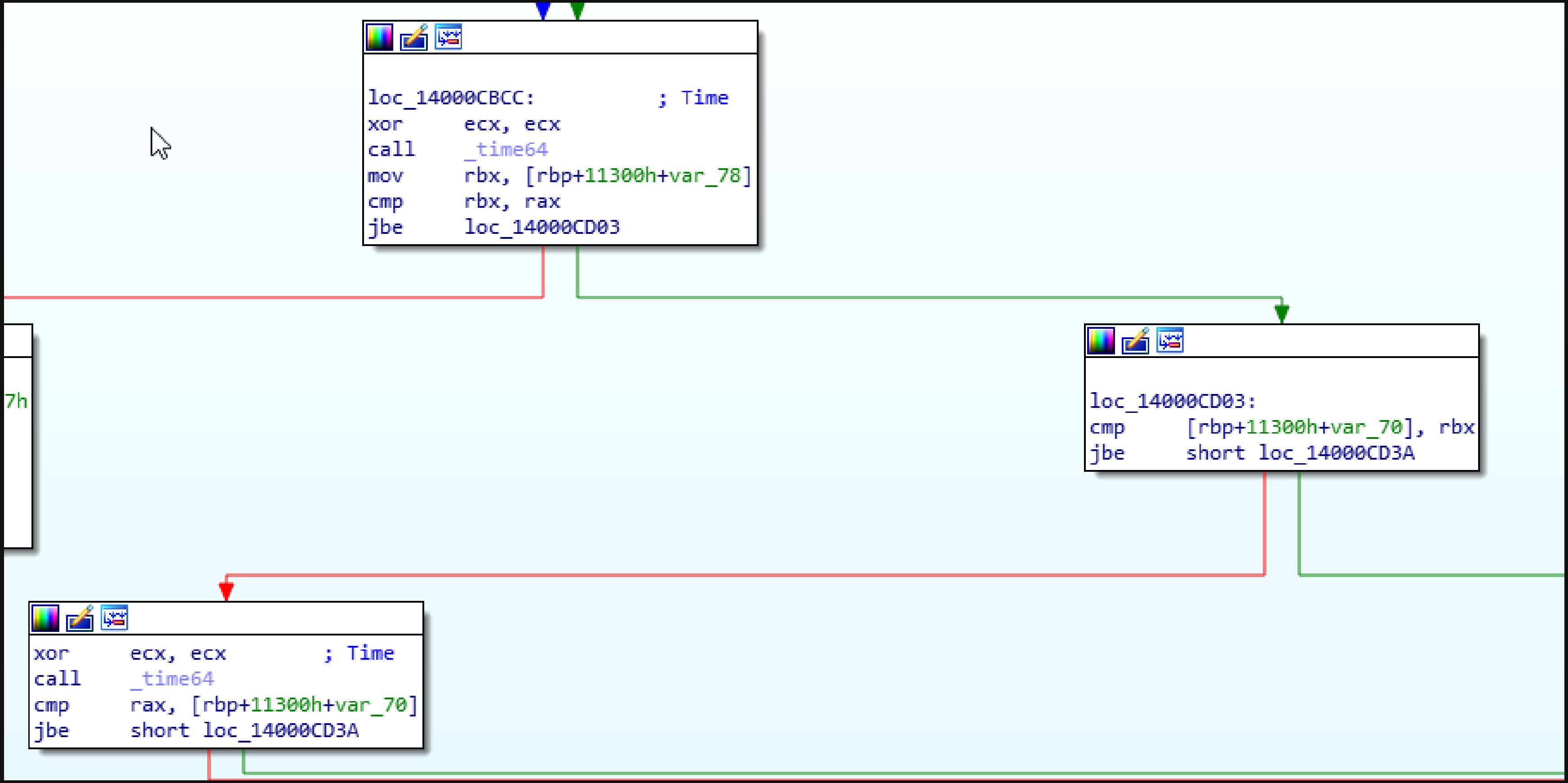
```
cmp     [rax], cl
jz      short loc_14000CFCB
```

```
db      66h, 66h
nop     word ptr [rax+rax+00000000h]
```

```
loc_14000CFC0:
inc     ecx
lea     rax, [rax+1]
cmp     byte ptr [rax], 0
jnz     short loc_14000CFC0
```

```
loc_14000CFCB:
inc     ecx
mov     eax, dword ptr [rsp+11400h+Size]
sub     eax, ecx
mov     edi, eax
add     rcx, rbx        ; Str
mov     r8d, eax        ; Count
mov     edx, 1          ; Size
call    fwrite
mov     r8d, dword ptr [rsp+11400h+Size] ; Size
```

Time Mechanism == If Statements



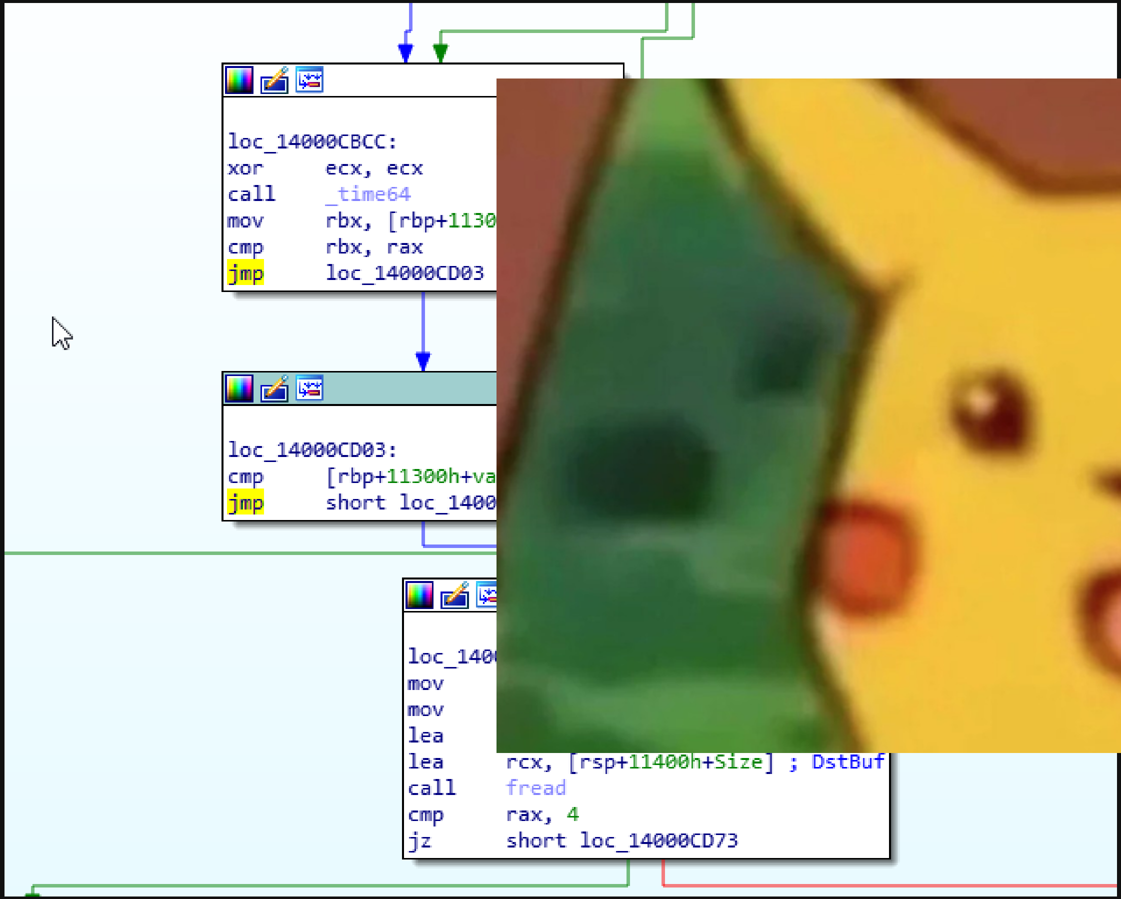
```
loc_14000CBCC:              ; Time
xor     ecx, ecx
call    _time64
mov     rbx, [rbp+11300h+var_78]
cmp     rbx, rax
jbe     loc_14000CD03
```

```
7h
```

```
loc_14000CD03:
cmp     [rbp+11300h+var_70], rbx
jbe     short loc_14000CD3A
```

```
xor     ecx, ecx            ; Time
call    _time64
cmp     rax, [rbp+11300h+var_70]
jbe     short loc_14000CD3A
```

Patched Logic

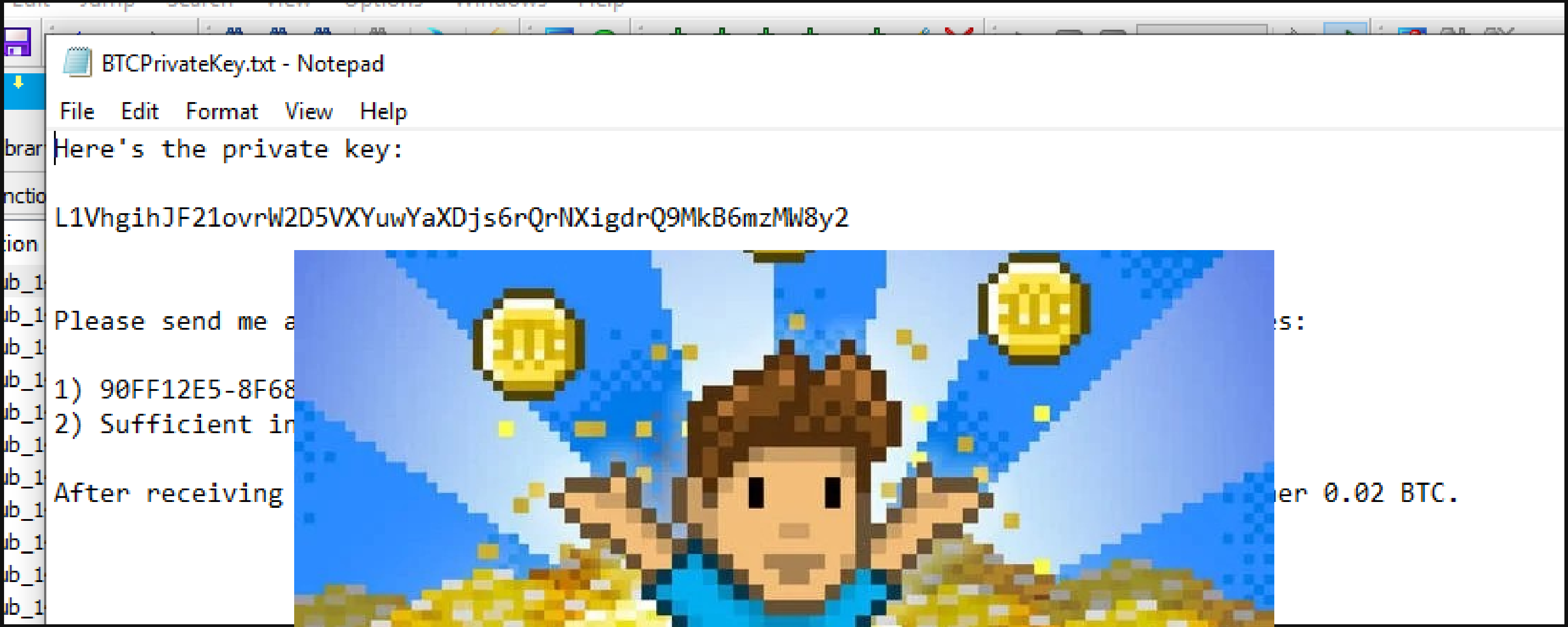


```
loc_14000CBCC:
xor     ecx, ecx
call    _time64
mov     rbx, [rbp+1130
cmp     rbx, rax
jmp     loc_14000CD03
```

```
loc_14000CD03:
cmp     [rbp+11300h+va
jmp     short loc_1400
```

```
loc_140
mov
mov
lea
lea     rcx, [rsp+11400h+Size] ; DstBuf
call    fread
cmp     rax, 4
jz      short loc_14000CD73
```

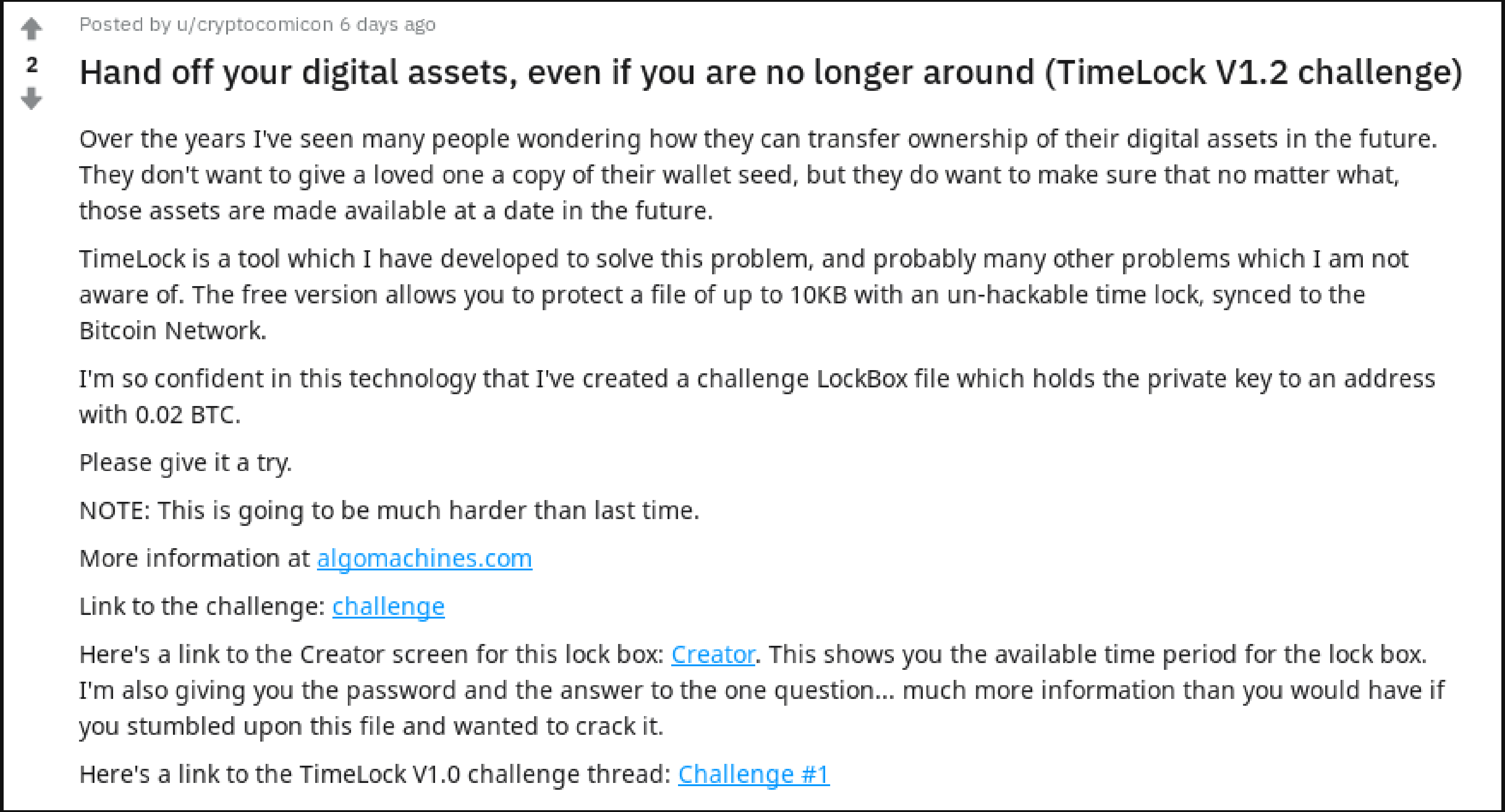
Loot #1



BTCPrivateKey.txt - Notepad

```
Here's the private key:

L1VhgihJF21ovrW2D5VXYuwYaXDjs6rQrNXigdrQ9MkB6mzMW8y2


Please send me a                                          s:

1) 90FF12E5-8F68
2) Sufficient in

After receiving                                           er 0.02 BTC.
```

Challenge #2



Posted by u/cryptocomicon 6 days ago

2

Hand off your digital assets, even if you are no longer around (TimeLock V1.2 challenge)

Over the years I've seen many people wondering how they can transfer ownership of their digital assets in the future. They don't want to give a loved one a copy of their wallet seed, but they do want to make sure that no matter what, those assets are made available at a date in the future.

TimeLock is a tool which I have developed to solve this problem, and probably many other problems which I am not aware of. The free version allows you to protect a file of up to 10KB with an un-hackable time lock, synced to the Bitcoin Network.

I'm so confident in this technology that I've created a challenge LockBox file which holds the private key to an address with 0.02 BTC.

Please give it a try.

NOTE: This is going to be much harder than last time.

More information at algomachines.com

Link to the challenge: challenge

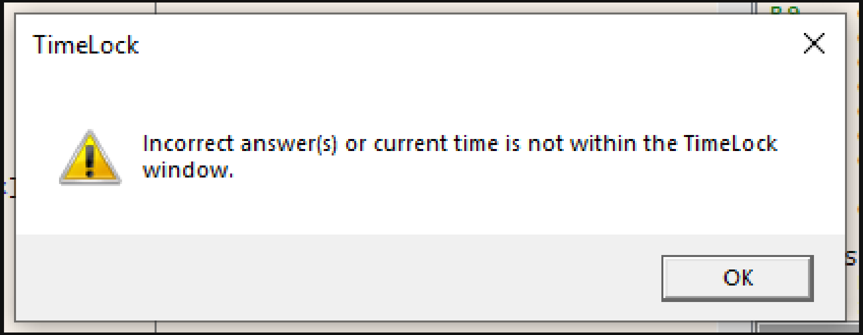
Here's a link to the Creator screen for this lock box: Creator. This shows you the available time period for the lock box. I'm also giving you the password and the answer to the one question... much more information than you would have if you stumbled upon this file and wanted to crack it.

Here's a link to the TimeLock V1.0 challenge thread: Challenge #1

Plan of Attack

- Locate where the time is passed into decryption function, set it to future.
- We know what the times are. Keep an eye out for:
  - 22/02/2019 00:00 UTC becomes **1550793600**.
    Hex: **0x5C6F3B80**
  - 23/02/2019 00:00 UTC becomes **1550880000**.
    Hex: **0x5C708D00**

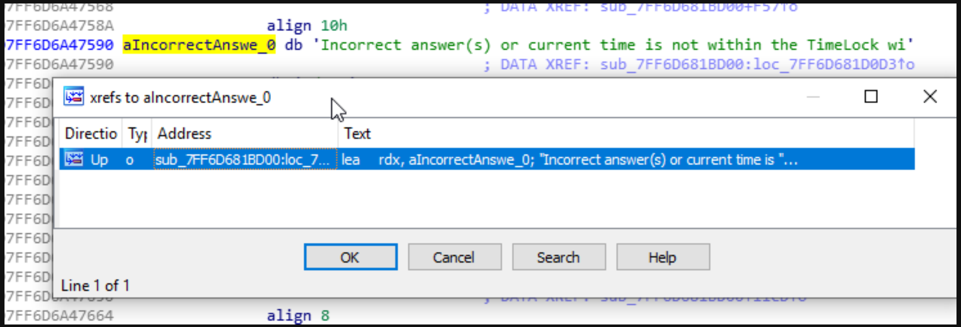
Jumping to String



TimeLock

Incorrect answer(s) or current time is not within the TimeLock window.

OK



```
7FF6D6A4758A                 align 10h
7FF6D6A47590 aIncorrectAnswe_0 db 'Incorrect answer(s) or current time is not within the TimeLock wi'
7FF6D6A47590                                         ; DATA XREF: sub_7FF6D681BD00:loc_7FF6D681D0D3↑o
```

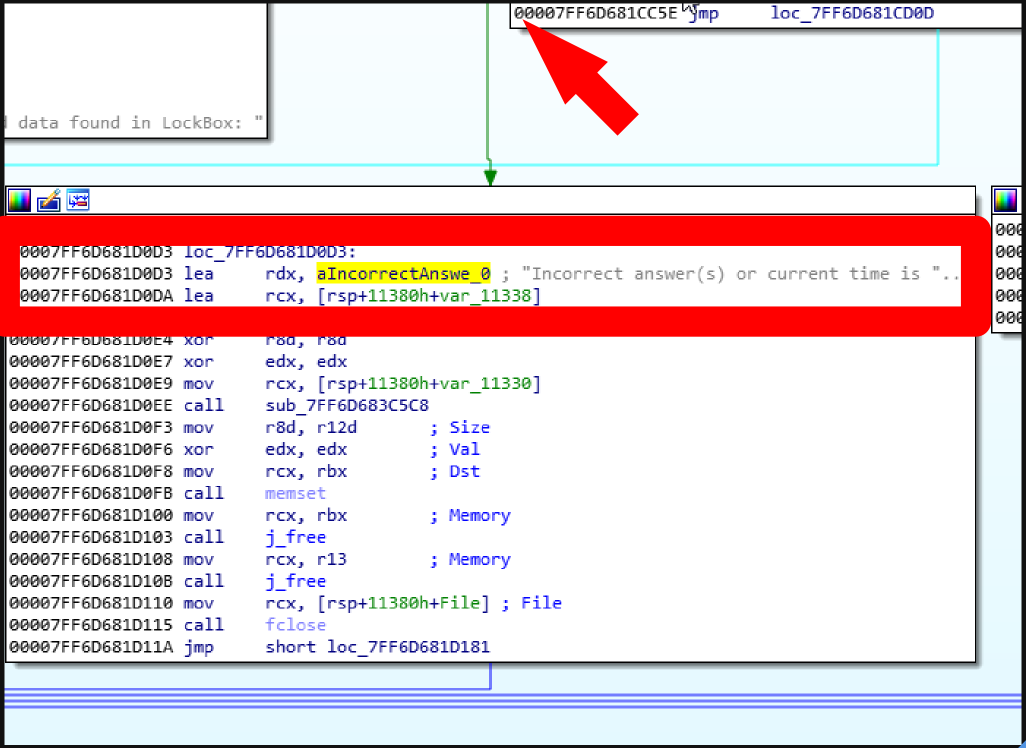
xrefs to aIncorrectAnswe_0

Directio	Typ	Address	Text
Up	o	sub_7FF6D681BD00:loc_7...	lea rdx, aIncorrectAnswe_0; "Incorrect answer(s) or current time is "...

OK Cancel Search Help

Line 1 of 1

```
7FF6D6A47664                 align 8
```

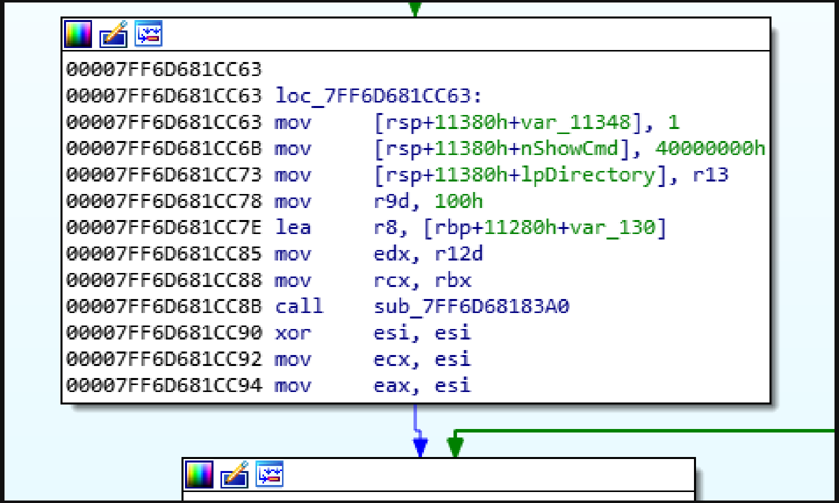


```
00007FF6D681CC5E jmp     loc_7FF6D681CD0D
```

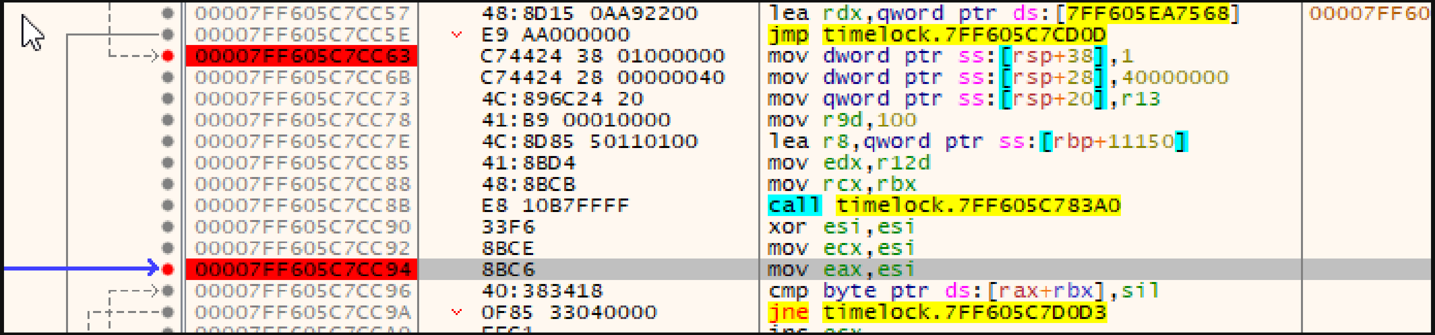
```
 data found in LockBox: "
```

```
0007FF6D681D0D3 loc_7FF6D681D0D3:
0007FF6D681D0D3 lea     rdx, aIncorrectAnswe_0 ; "Incorrect answer(s) or current time is "..
0007FF6D681D0DA lea     rcx, [rsp+11380h+var_11338]
00007FF6D681D0E7 xor     edx, edx
00007FF6D681D0E9 mov     rcx, [rsp+11380h+var_11330]
00007FF6D681D0EE call    sub_7FF6D683C5C8
00007FF6D681D0F3 mov     r8d, r12d       ; Size
00007FF6D681D0F6 xor     edx, edx        ; Val
00007FF6D681D0F8 mov     rcx, rbx        ; Dst
00007FF6D681D0FB call    memset
00007FF6D681D100 mov     rcx, rbx        ; Memory
00007FF6D681D103 call    j_free
00007FF6D681D108 mov     rcx, r13        ; Memory
00007FF6D681D10B call    j_free
00007FF6D681D110 mov     rcx, [rsp+11380h+File] ; File
00007FF6D681D115 call    fclose
00007FF6D681D11A jmp     short loc_7FF6D681D181
```

Setting Up Breakpoints

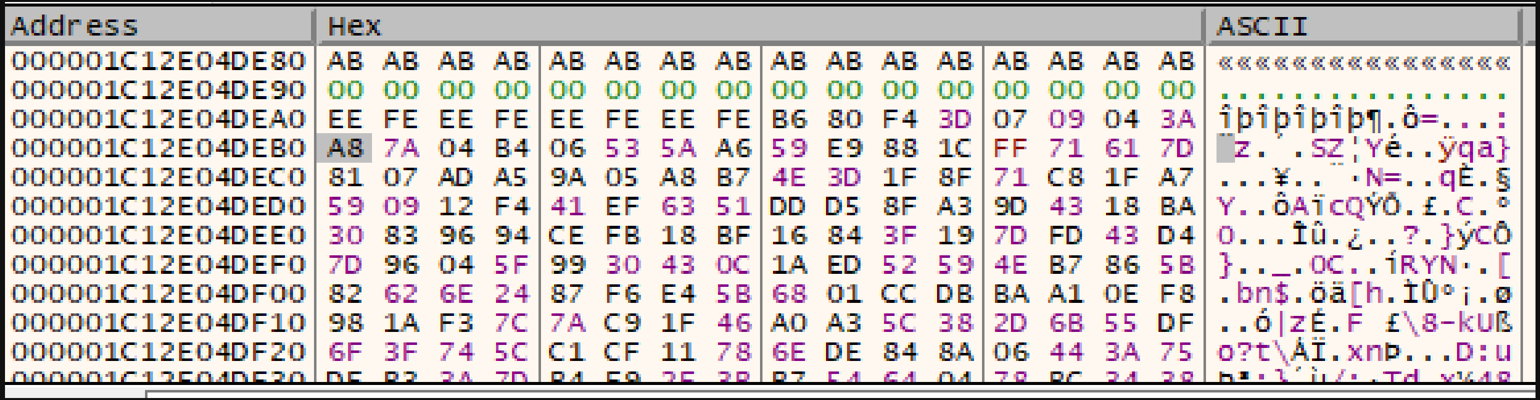


```
00007FF6D681CC63
00007FF6D681CC63 loc_7FF6D681CC63:
00007FF6D681CC63 mov     [rsp+11380h+var_11348], 1
00007FF6D681CC6B mov     [rsp+11380h+nShowCmd], 40000000h
00007FF6D681CC73 mov     [rsp+11380h+lpDirectory], r13
00007FF6D681CC78 mov     r9d, 100h
00007FF6D681CC7E lea     r8, [rbp+11280h+var_130]
00007FF6D681CC85 mov     edx, r12d
00007FF6D681CC88 mov     rcx, rbx
00007FF6D681CC8B call    sub_7FF6D68183A0
00007FF6D681CC90 xor     esi, esi
00007FF6D681CC92 mov     ecx, esi
00007FF6D681CC94 mov     eax, esi
```

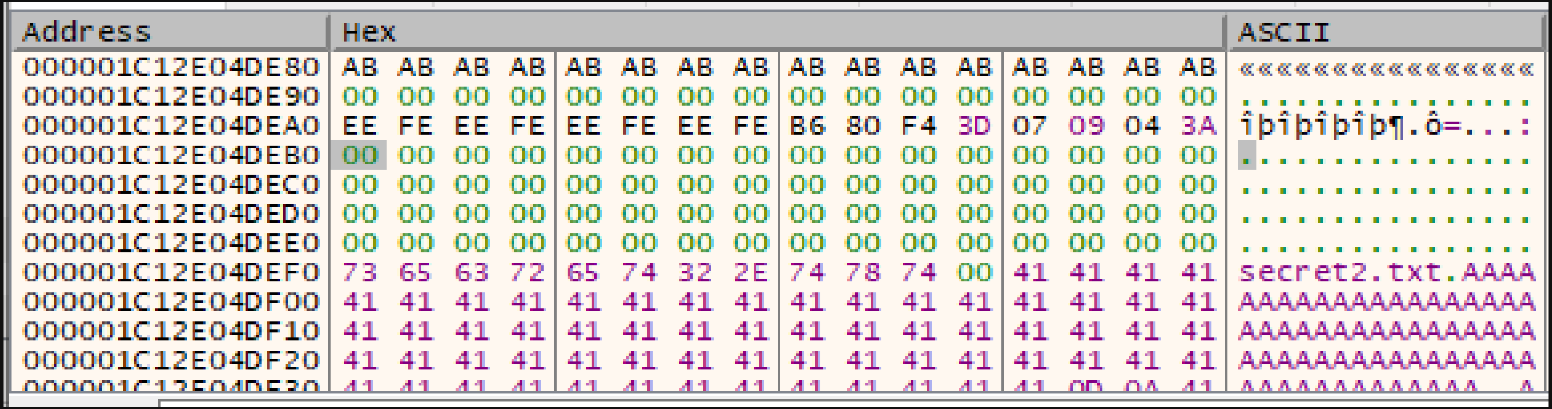


```
00007FF605C7CC57    48:8D15 0AA92200     lea rdx,qword ptr ds:[7FF605EA7568]    00007FF60
00007FF605C7CC5E    E9 AA000000          jmp timelock.7FF605C7CD0D
00007FF605C7CC63    C74424 38 01000000   mov dword ptr ss:[rsp+38],1
00007FF605C7CC6B    C74424 28 00000040   mov dword ptr ss:[rsp+28],40000000
00007FF605C7CC73    4C:896C24 20         mov qword ptr ss:[rsp+20],r13
00007FF605C7CC78    41:B9 00010000       mov r9d,100
00007FF605C7CC7E    4C:8D85 50110100     lea r8,qword ptr ss:[rbp+11150]
00007FF605C7CC85    41:8BD4              mov edx,r12d
00007FF605C7CC88    48:8BCB              mov rcx,rbx
00007FF605C7CC8B    E8 10B7FFFF          call timelock.7FF605C783A0
00007FF605C7CC90    33F6                 xor esi,esi
00007FF605C7CC92    8BCE                 mov ecx,esi
00007FF605C7CC94    8BC6                 mov eax,esi
00007FF605C7CC96    40:383418            cmp byte ptr ds:[rax+rbx],sil
00007FF605C7CC9A    0F85 33040000        jne timelock.7FF605C7D0D3
```

Decryption Function Found

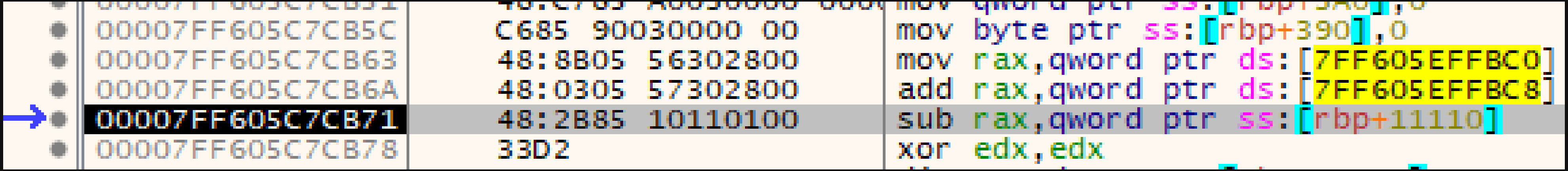


```
Address           Hex                                                ASCII
000001C12E04DE80  AB AB AB AB  AB AB AB AB  AB AB AB AB  AB AB AB AB  ««««««««««««««««
000001C12E04DE90  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12E04DEA0  EE FE EE FE  EE FE EE FE  B6 80 F4 3D  07 09 04 3A  îþîþîþîþ¶.ô=...:
000001C12E04DEB0  A8 7A 04 B4  06 53 5A A6  59 E9 88 1C  FF 71 61 7D  ¨z.´.SZ¦Yé..ÿqa}
000001C12E04DEC0  81 07 AD A5  9A 05 A8 B7  4E 3D 1F 8F  71 C8 1F A7  ...¥..¨·N=..qÈ.§
000001C12E04DED0  59 09 12 F4  41 EF 63 51  DD D5 8F A3  9D 43 18 BA  Y..ôAïcQÝÕ.£.C.º
000001C12E04DEE0  30 83 96 94  CE FB 18 BF  16 84 3F 19  7D FD 43 D4  0...Îû.¿..?.}ýCÔ
000001C12E04DEF0  7D 96 04 5F  99 30 43 0C  1A ED 52 59  4E B7 86 5B  }.._.0C..íRYN·.[
000001C12E04DF00  82 62 6E 24  87 F6 E4 5B  68 01 CC DB  BA A1 0E F8  .bn$.öä[h.ÌÛº¡.ø
000001C12E04DF10  98 1A F3 7C  7A C9 1F 46  A0 A3 5C 38  2D 6B 55 DF  ..ó|zÉ.F £\8-kUß
000001C12E04DF20  6F 3F 74 5C  C1 CF 11 78  6E DE 84 8A  06 44 3A 75  o?t\ÁÏ.xnÞ...D:u
```



```
Address           Hex                                                ASCII
000001C12E04DE80  AB AB AB AB  AB AB AB AB  AB AB AB AB  AB AB AB AB  ««««««««««««««««
000001C12E04DE90  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12E04DEA0  EE FE EE FE  EE FE EE FE  B6 80 F4 3D  07 09 04 3A  îþîþîþîþ¶.ô=...:
000001C12E04DEB0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12E04DEC0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12E04DED0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12E04DEE0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12E04DEF0  73 65 63 72  65 74 32 2E  74 78 74 00  41 41 41 41  secret2.txt.AAAA
000001C12E04DF00  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  AAAAAAAAAAAAAAAA
000001C12E04DF10  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  AAAAAAAAAAAAAAAA
000001C12E04DF20  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  AAAAAAAAAAAAAAAA
```

Breakthrough Found

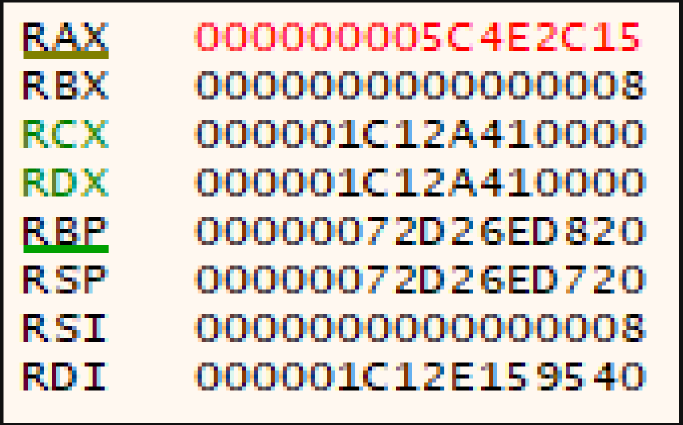


```
● 00007FF605C7CB5C    C685 90030000 00     mov byte ptr ss:[rbp+390],0
● 00007FF605C7CB63    48:8B05 56302800     mov rax,qword ptr ds:[7FF605EFFBC0]
● 00007FF605C7CB6A    48:0305 57302800     add rax,qword ptr ds:[7FF605EFFBC8]
→● 00007FF605C7CB71   48:2B85 10110100     sub rax,qword ptr ss:[rbp+11110]
● 00007FF605C7CB78    33D2                 xor edx,edx
```

0x5C4E2C15 looks familiar

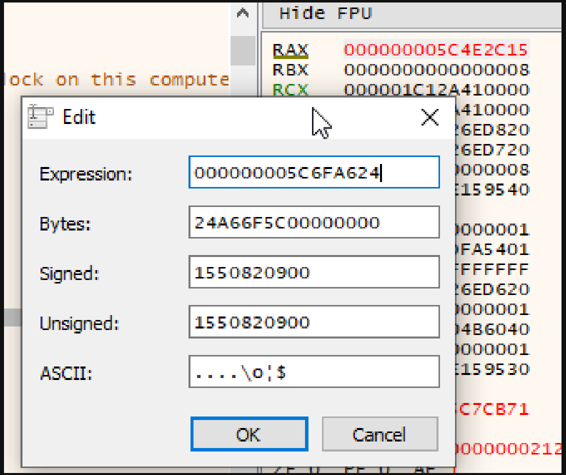
Converting to decimal: **1548626965**

This is a Unix timestamp!
28/01/19 11:09:25



```
RAX    000000005C4E2C15
RBX    0000000000000008
RCX    000001C12A410000
RDX    000001C12A410000
RBP    00000072D26ED820
RSP    00000072D26ED720
RSI    0000000000000008
RDI    000001C12E159540
```

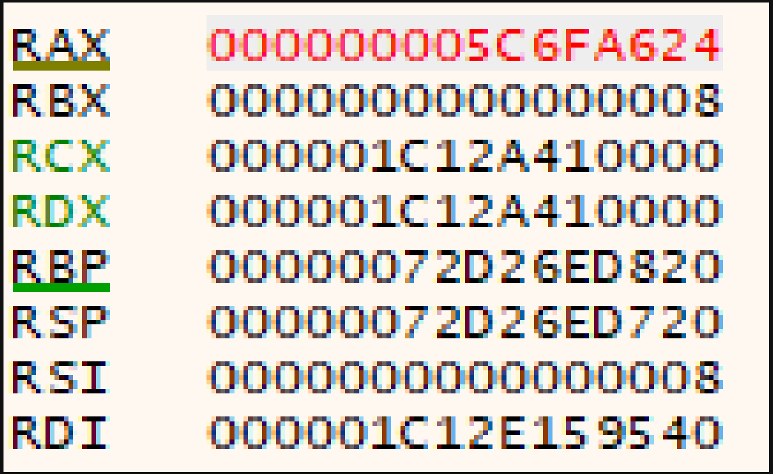
Modifying Timestamp



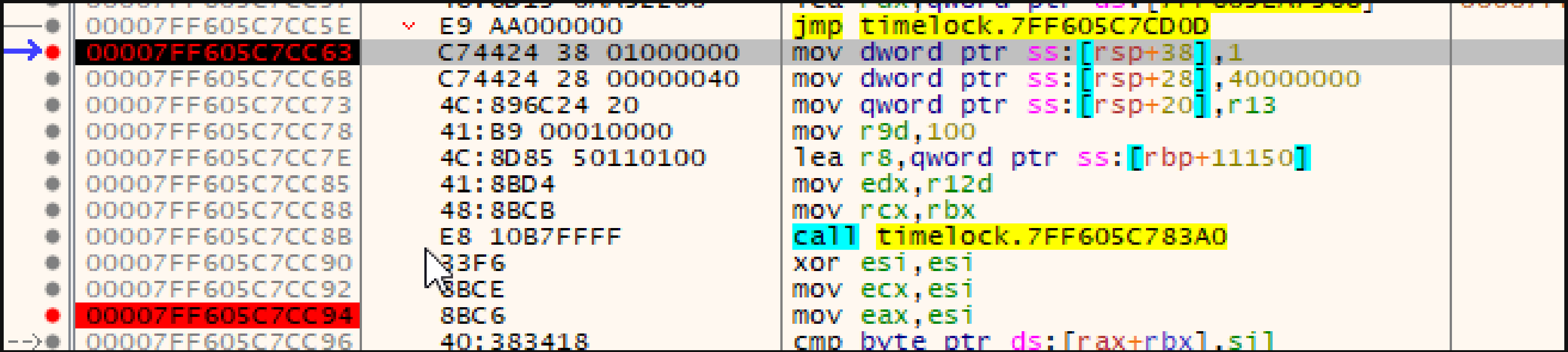
```
Hide FPU
RAX    000000005C4E2C15
RBX    0000000000000008
RCX    000001C12A410000
lock on this compute
```

Edit

Expression:	000000005C6FA624
Bytes:	24A66F5C00000000
Signed:	1550820900
Unsigned:	1550820900
ASCII:	....\o¦$

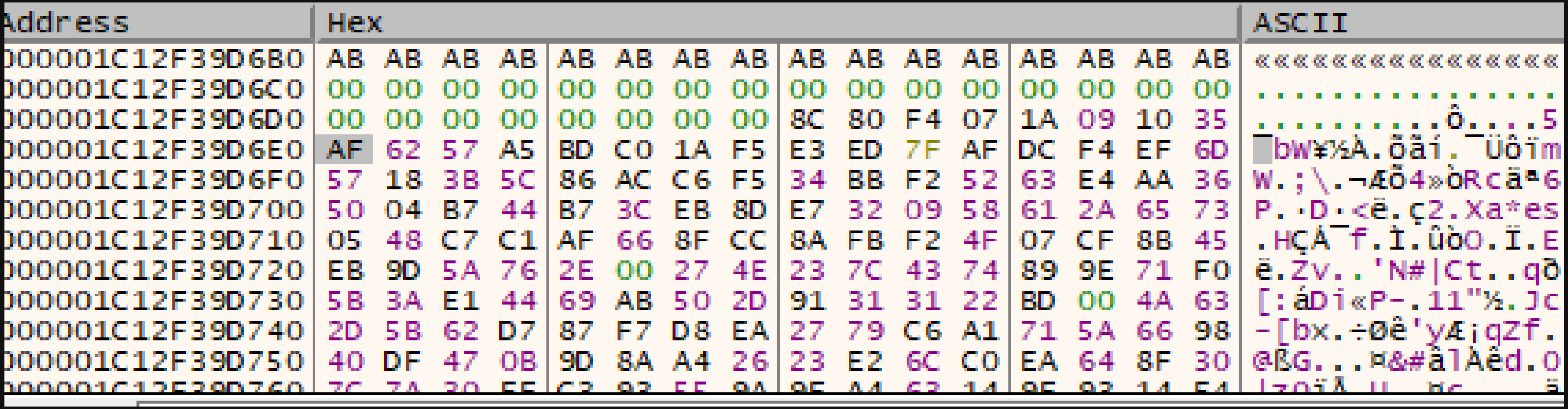


```
RAX    000000005C6FA624
RBX    0000000000000008
RCX    000001C12A410000
RDX    000001C12A410000
RBP    00000072D26ED820
RSP    00000072D26ED720
RSI    0000000000000008
RDI    000001C12E159540
```

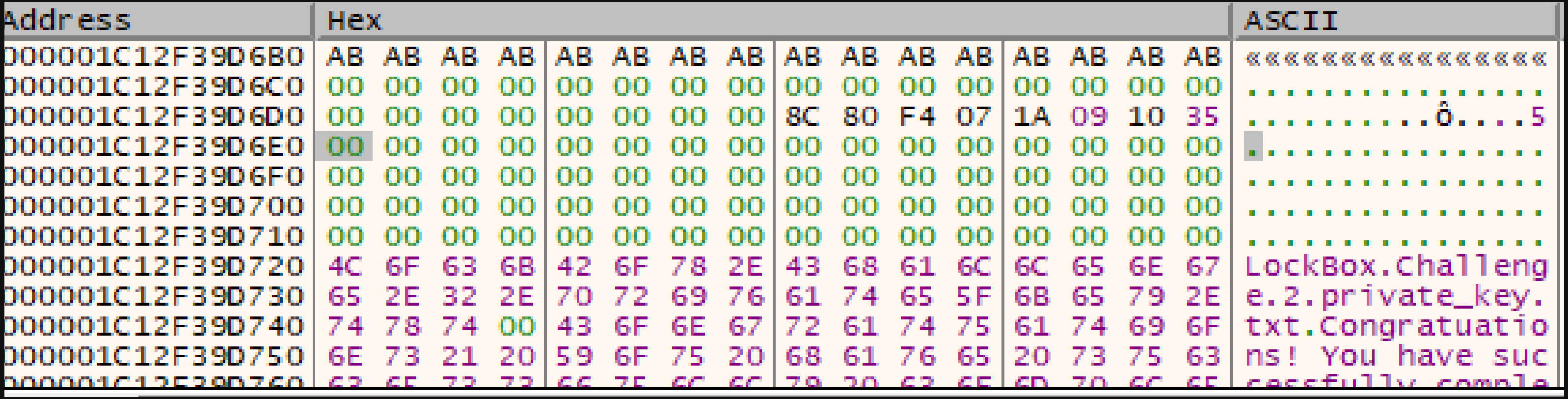


```
00007FF605C7CC5E    E9 AA000000          jmp timelock.7FF605C7CD0D
00007FF605C7CC63    C74424 38 01000000   mov dword ptr ss:[rsp+38],1
00007FF605C7CC6B    C74424 28 00000040   mov dword ptr ss:[rsp+28],40000000
00007FF605C7CC73    4C:896C24 20         mov qword ptr ss:[rsp+20],r13
00007FF605C7CC78    41:B9 00010000       mov r9d,100
00007FF605C7CC7E    4C:8D85 50110100     lea r8,qword ptr ss:[rbp+11150]
00007FF605C7CC85    41:8BD4              mov edx,r12d
00007FF605C7CC88    48:8BCB              mov rcx,rbx
00007FF605C7CC8B    E8 10B7FFFF          call timelock.7FF605C783A0
00007FF605C7CC90    33F6                 xor esi,esi
00007FF605C7CC92    8BCE                 mov ecx,esi
00007FF605C7CC94    8BC6                 mov eax,esi
00007FF605C7CC96    40:383418            cmp byte ptr ds:[rax+rbx],sil
```

Stepping Over Decryption

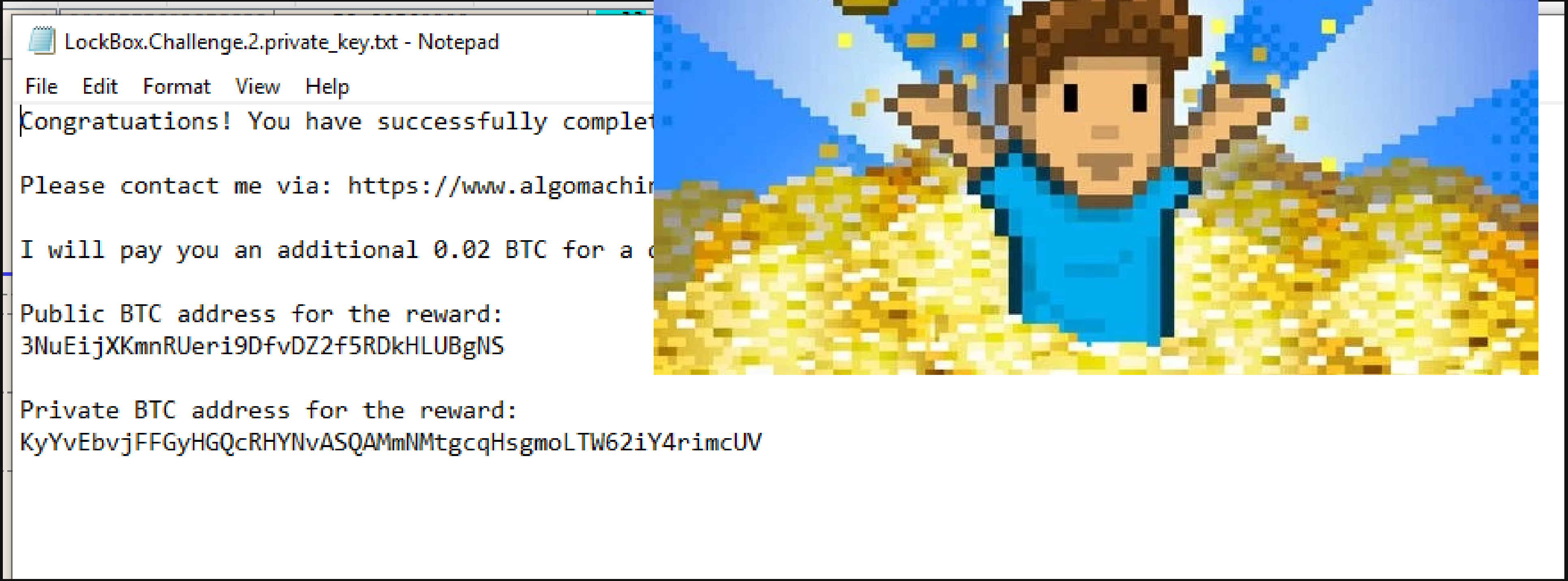


```
Address            Hex                                                ASCII
000001C12F39D6B0   AB AB AB AB  AB AB AB AB  AB AB AB AB  AB AB AB AB  ««««««««««««««««
000001C12F39D6C0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12F39D6D0   00 00 00 00  00 00 00 00  8C 80 F4 07  1A 09 10 35  ..........ô....5
000001C12F39D6E0   AF 62 57 A5  BD C0 1A F5  E3 ED 7F AF  DC F4 EF 6D  ¯bW¥½À.õãí.¯Üôïm
000001C12F39D6F0   57 18 3B 5C  86 AC C6 F5  34 BB F2 52  63 E4 AA 36  W.;\.¬Æõ4»òRcäª6
000001C12F39D700   50 04 B7 44  B7 3C EB 8D  E7 32 09 58  61 2A 65 73  P.·D·<ë.ç2.Xa*es
000001C12F39D710   05 48 C7 C1  AF 66 8F CC  8A FB F2 4F  07 CF 8B 45  .HÇÁ¯f.Ì.ûòO.Ï.E
000001C12F39D720   EB 9D 5A 76  2E 00 27 4E  23 7C 43 74  89 9E 71 F0  ë.Zv..'N#|Ct..qð
000001C12F39D730   5B 3A E1 44  69 AB 50 2D  91 31 31 22  BD 00 4A 63  [:áDi«P-.11"½.Jc
000001C12F39D740   2D 5B 62 D7  87 F7 D8 EA  27 79 C6 A1  71 5A 66 98  -[b×.÷Øê'yÆ¡qZf.
000001C12F39D750   40 DF 47 0B  9D 8A A4 26  23 E2 6C C0  EA 64 8F 30  @ßG...¤&#âlÀêd.0
```



```
Address            Hex                                                ASCII
000001C12F39D6B0   AB AB AB AB  AB AB AB AB  AB AB AB AB  AB AB AB AB  ««««««««««««««««
000001C12F39D6C0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12F39D6D0   00 00 00 00  00 00 00 00  8C 80 F4 07  1A 09 10 35  ..........ô....5
000001C12F39D6E0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12F39D6F0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12F39D700   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12F39D710   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001C12F39D720   4C 6F 63 6B  42 6F 78 2E  43 68 61 6C  6C 65 6E 67  LockBox.Challeng
000001C12F39D730   65 2E 32 2E  70 72 69 76  61 74 65 5F  6B 65 79 2E  e.2.private_key.
000001C12F39D740   74 78 74 00  43 6F 6E 67  72 61 74 75  61 74 69 6F  txt.Congratulatio
000001C12F39D750   6E 73 21 20  59 6F 75 20  68 61 76 65  20 73 75 63  ns! You have suc
```

Loot #2

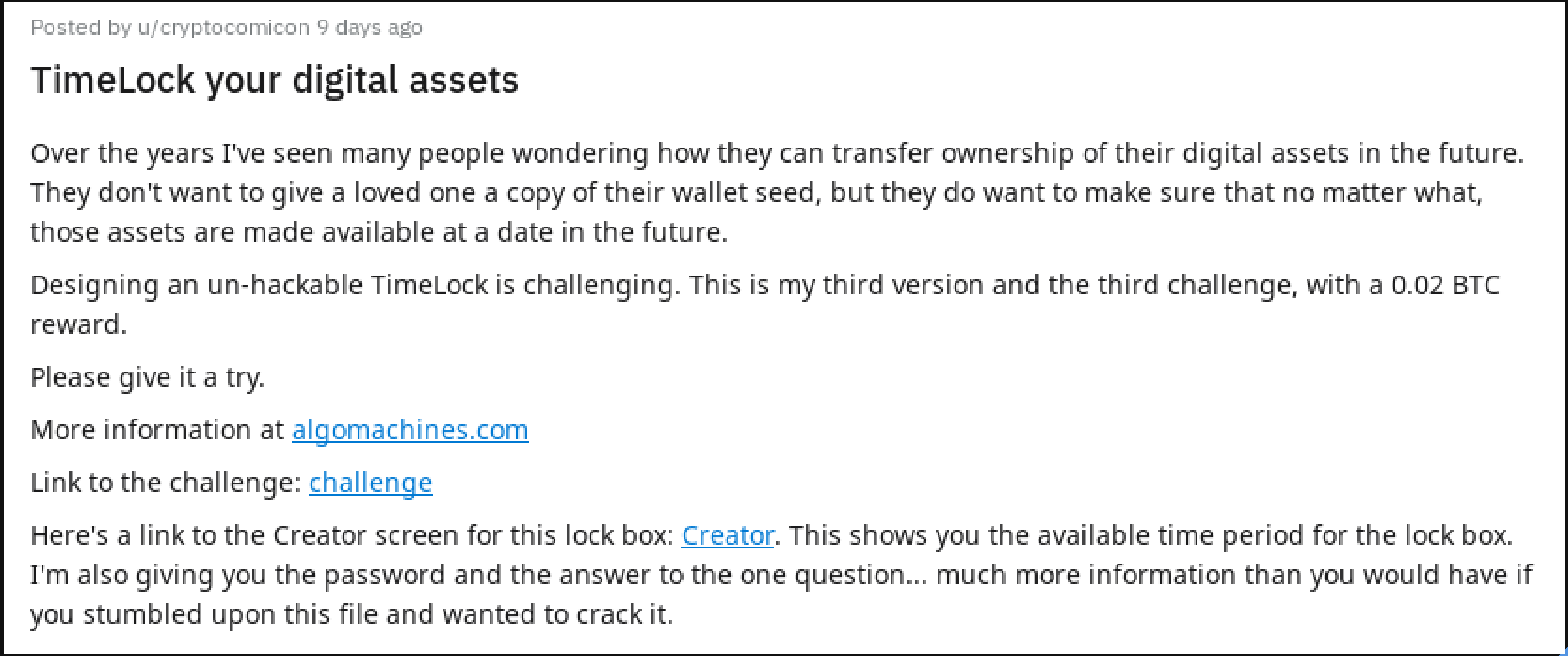


LockBox.Challenge.2.private_key.txt - Notepad

File Edit Format View Help

```
Congratuations! You have successfully complet

Please contact me via: https://www.algomachi

I will pay you an additional 0.02 BTC for a 

Public BTC address for the reward:
3NuEijXKmnRUeri9DfvDZ2f5RDkHLUBgNS

Private BTC address for the reward:
KyYvEbvjFFGyHGQcRHYNvASQAMmNMtgcqHsgmoLTW62iY4rimcUV
```

Challenge #3



Posted by u/cryptocomicon 9 days ago

TimeLock your digital assets

Over the years I've seen many people wondering how they can transfer ownership of their digital assets in the future. They don't want to give a loved one a copy of their wallet seed, but they do want to make sure that no matter what, those assets are made available at a date in the future.

Designing an un-hackable TimeLock is challenging. This is my third version and the third challenge, with a 0.02 BTC reward.

Please give it a try.

More information at algomachines.com

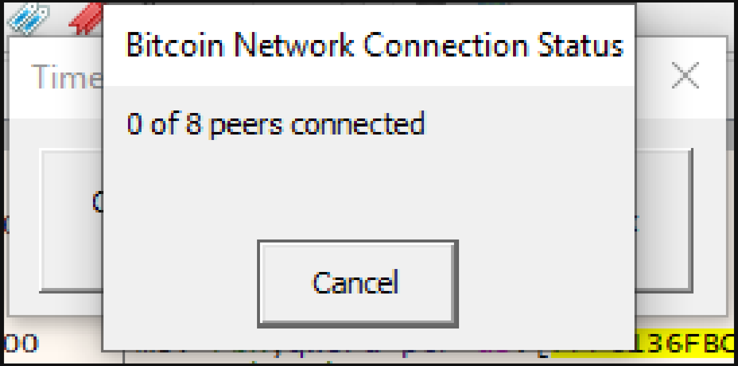
Link to the challenge: challenge

Here's a link to the Creator screen for this lock box: Creator. This shows you the available time period for the lock box. I'm also giving you the password and the answer to the one question... much more information than you would have if you stumbled upon this file and wanted to crack it.

Plan of Attack

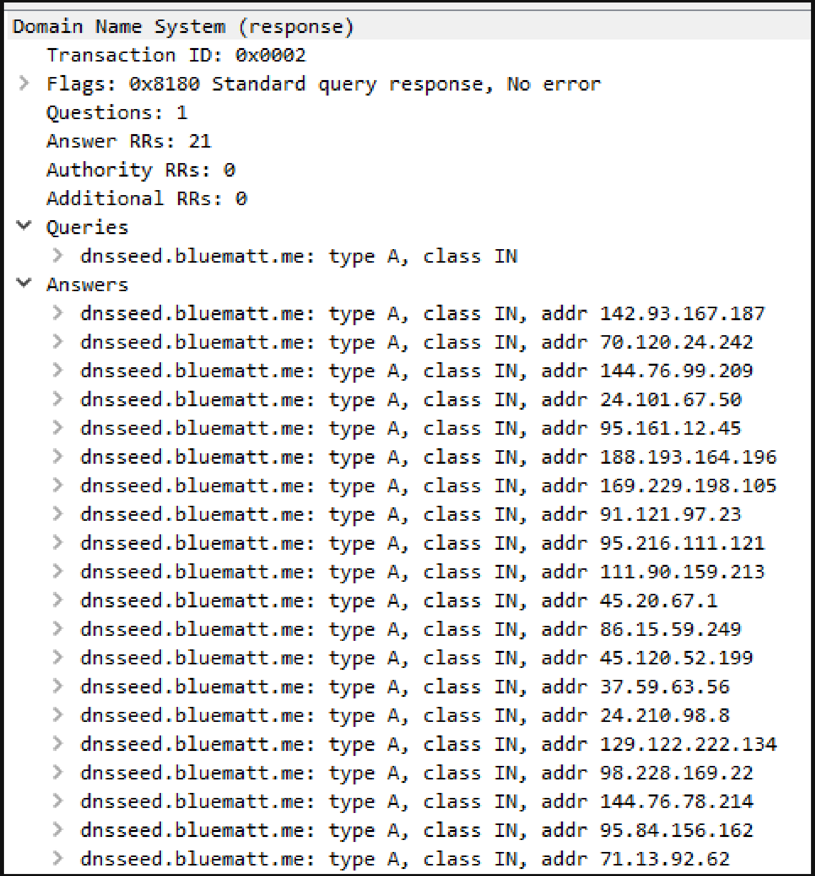
- Launch a “Sybil” Attack
  - Introduce malicious nodes as the network.
  - Behave exactly like legitimate nodes.
  - Have time set to the future.
  - Disable internet access and force local nodes to connect.

TimeLock Uses DNS Seed Nodes

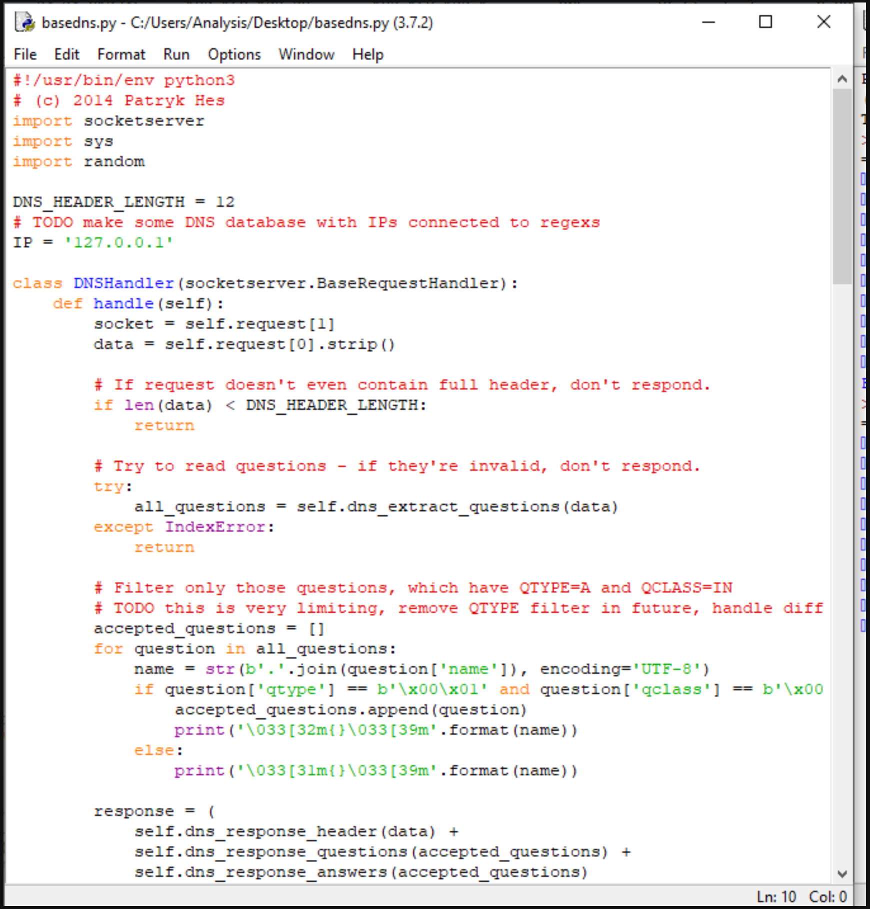

Bitcoin Network Connection Status

0 of 8 peers connected

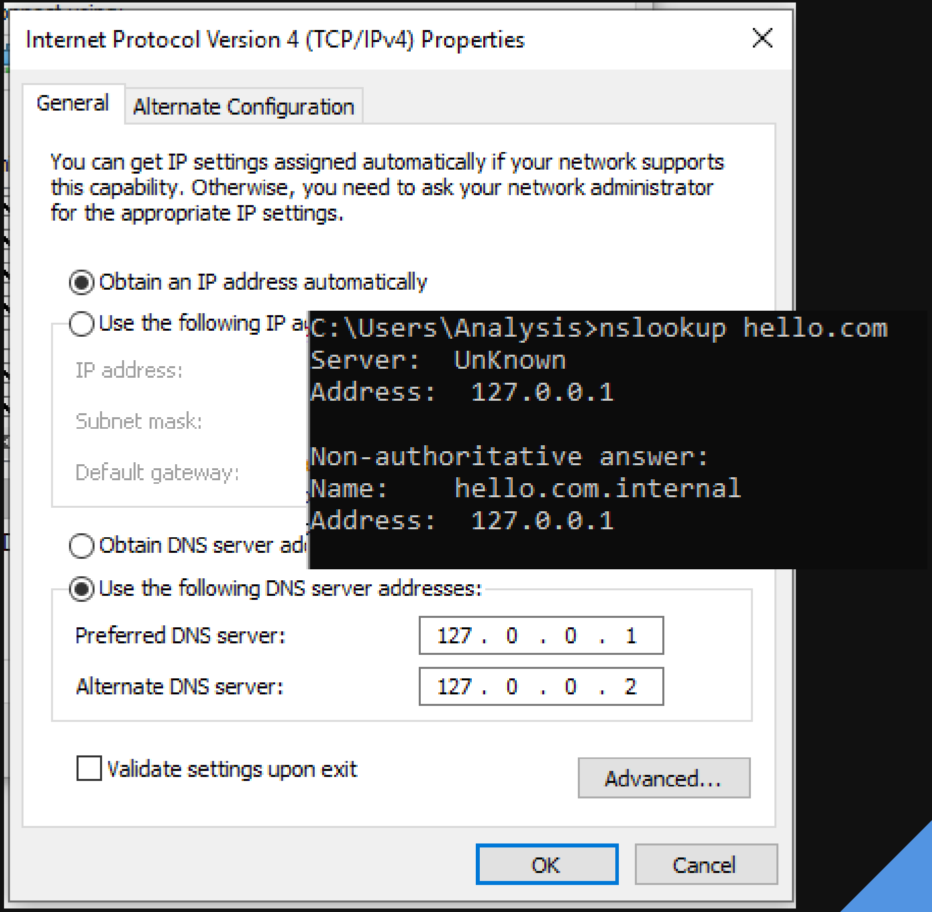
- seed.bitcoin.spia.be
- bitseed.xf2.org
- dnsseed.bitcoin.dashjr.org
- dnsseed.bluematt.org
- missionctrl.info


```
Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 21
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > dnsseed.bluematt.me: type A, class IN
  v Answers
    > dnsseed.bluematt.me: type A, class IN, addr 142.93.167.187
    > dnsseed.bluematt.me: type A, class IN, addr 70.120.24.242
    > dnsseed.bluematt.me: type A, class IN, addr 144.76.99.209
    > dnsseed.bluematt.me: type A, class IN, addr 24.101.67.50
    > dnsseed.bluematt.me: type A, class IN, addr 95.161.12.45
    > dnsseed.bluematt.me: type A, class IN, addr 188.193.164.196
    > dnsseed.bluematt.me: type A, class IN, addr 169.229.198.105
    > dnsseed.bluematt.me: type A, class IN, addr 91.121.97.23
    > dnsseed.bluematt.me: type A, class IN, addr 95.216.111.121
    > dnsseed.bluematt.me: type A, class IN, addr 111.90.159.213
    > dnsseed.bluematt.me: type A, class IN, addr 45.20.67.1
    > dnsseed.bluematt.me: type A, class IN, addr 86.15.59.249
    > dnsseed.bluematt.me: type A, class IN, addr 45.120.52.199
    > dnsseed.bluematt.me: type A, class IN, addr 37.59.63.56
    > dnsseed.bluematt.me: type A, class IN, addr 24.210.98.8
    > dnsseed.bluematt.me: type A, class IN, addr 129.122.222.134
    > dnsseed.bluematt.me: type A, class IN, addr 98.228.169.22
    > dnsseed.bluematt.me: type A, class IN, addr 144.76.78.214
    > dnsseed.bluematt.me: type A, class IN, addr 95.84.156.162
    > dnsseed.bluematt.me: type A, class IN, addr 71.13.92.62
```

Rolling Our Own DNS


basedns.py - C:/Users/Analysis/Desktop/basedns.py (3.7.2)
File Edit Format Run Options Window Help
Ln: 10 Col: 0

```python
#!/usr/bin/env python3
# (c) 2014 Patryk Hes
import socketserver
import sys
import random

DNS_HEADER_LENGTH = 12
# TODO make some DNS database with IPs connected to regexs
IP = '127.0.0.1'

class DNSHandler(socketserver.BaseRequestHandler):
    def handle(self):
        socket = self.request[1]
        data = self.request[0].strip()

        # If request doesn't even contain full header, don't respond.
        if len(data) < DNS_HEADER_LENGTH:
            return

        # Try to read questions - if they're invalid, don't respond.
        try:
            all_questions = self.dns_extract_questions(data)
        except IndexError:
            return

        # Filter only those questions, which have QTYPE=A and QCLASS=IN
        # TODO this is very limiting, remove QTYPE filter in future, handle diff
        accepted_questions = []
        for question in all_questions:
            name = str(b'.'.join(question['name']), encoding='UTF-8')
            if question['qtype'] == b'\x00\x01' and question['qclass'] == b'\x00
                accepted_questions.append(question)
                print('\033[32m{}\033[39m'.format(name))
            else:
                print('\033[31m{}\033[39m'.format(name))

        response = (
            self.dns_response_header(data) +
            self.dns_response_questions(accepted_questions) +
            self.dns_response_answers(accepted_questions)
```



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

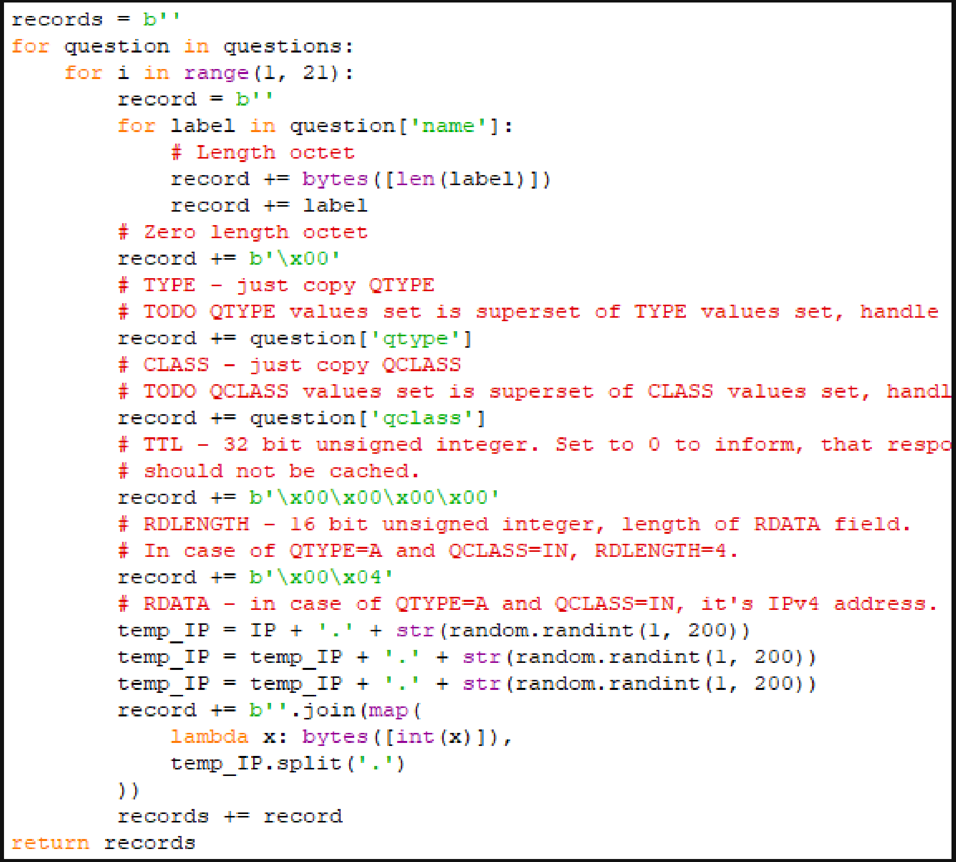
[✓ Obtain an IP address automatically]
Use the following IP a
IP address:
Subnet mask:
Default gateway:

Obtain DNS server ad
[✓ Use the following DNS server addresses:]
Preferred DNS server: 127 . 0 . 0 . 1
Alternate DNS server: 127 . 0 . 0 . 2

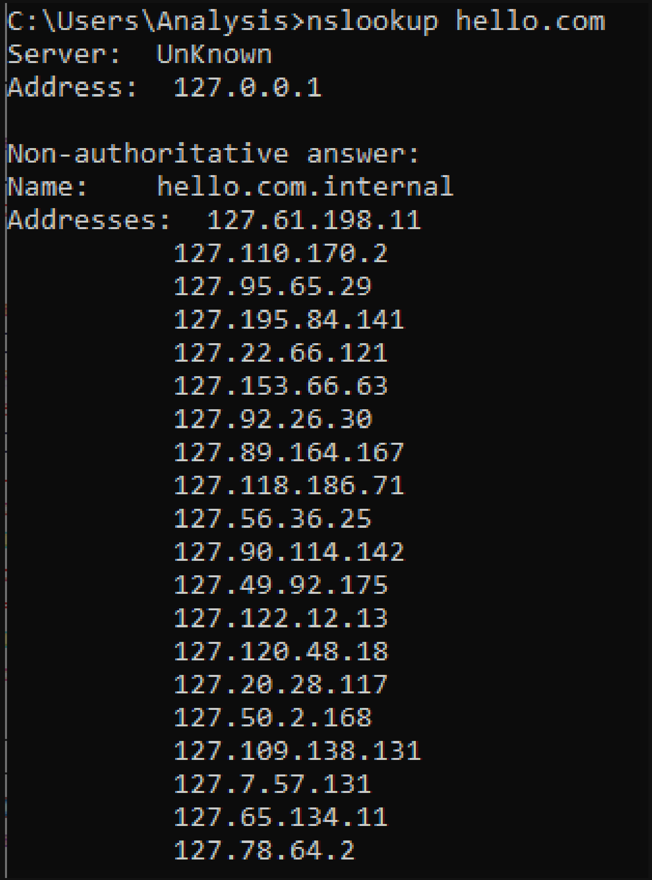
☐ Validate settings upon exit

```
C:\Users\Analysis>nslookup hello.com
Server:   UnKnown
Address:  127.0.0.1

Non-authoritative answer:
Name:    hello.com.internal
Address:  127.0.0.1
```

Generating DNS Records Randomly

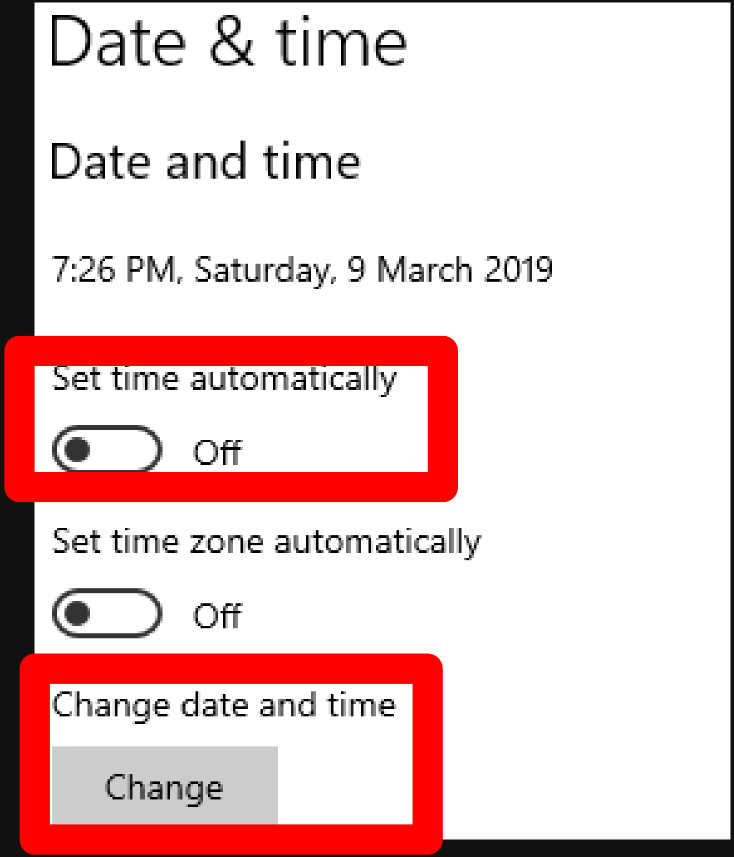


```
records = b''
for question in questions:
    for i in range(1, 21):
        record = b''
        for label in question['name']:
            # Length octet
            record += bytes([len(label)])
            record += label
        # Zero length octet
        record += b'\x00'
        # TYPE - just copy QTYPE
        # TODO QTYPE values set is superset of TYPE values set, handle
        record += question['qtype']
        # CLASS - just copy QCLASS
        # TODO QCLASS values set is superset of CLASS values set, handl
        record += question['qclass']
        # TTL - 32 bit unsigned integer. Set to 0 to inform, that respo
        # should not be cached.
        record += b'\x00\x00\x00\x00'
        # RDLENGTH - 16 bit unsigned integer, length of RDATA field.
        # In case of QTYPE=A and QCLASS=IN, RDLENGTH=4.
        record += b'\x00\x04'
        # RDATA - in case of QTYPE=A and QCLASS=IN, it's IPv4 address.
        temp_IP = IP + '.' + str(random.randint(1, 200))
        temp_IP = temp_IP + '.' + str(random.randint(1, 200))
        temp_IP = temp_IP + '.' + str(random.randint(1, 200))
        record += b''.join(map(
            lambda x: bytes([int(x)]),
            temp_IP.split('.')
        ))
        records += record
return records
```



```
C:\Users\Analysis>nslookup hello.com
Server:  UnKnown
Address:  127.0.0.1

Non-authoritative answer:
Name:    hello.com.internal
Addresses:  127.61.198.11
          127.110.170.2
          127.95.65.29
          127.195.84.141
          127.22.66.121
          127.153.66.63
          127.92.26.30
          127.89.164.167
          127.118.186.71
          127.56.36.25
          127.90.114.142
          127.49.92.175
          127.122.12.13
          127.120.48.18
          127.20.28.117
          127.50.2.168
          127.109.138.131
          127.7.57.131
          127.65.134.11
          127.78.64.2
```

Starting Our Bitcoin Node


Date & time

Date and time

7:26 PM, Saturday, 9 March 2019

Set time automatically

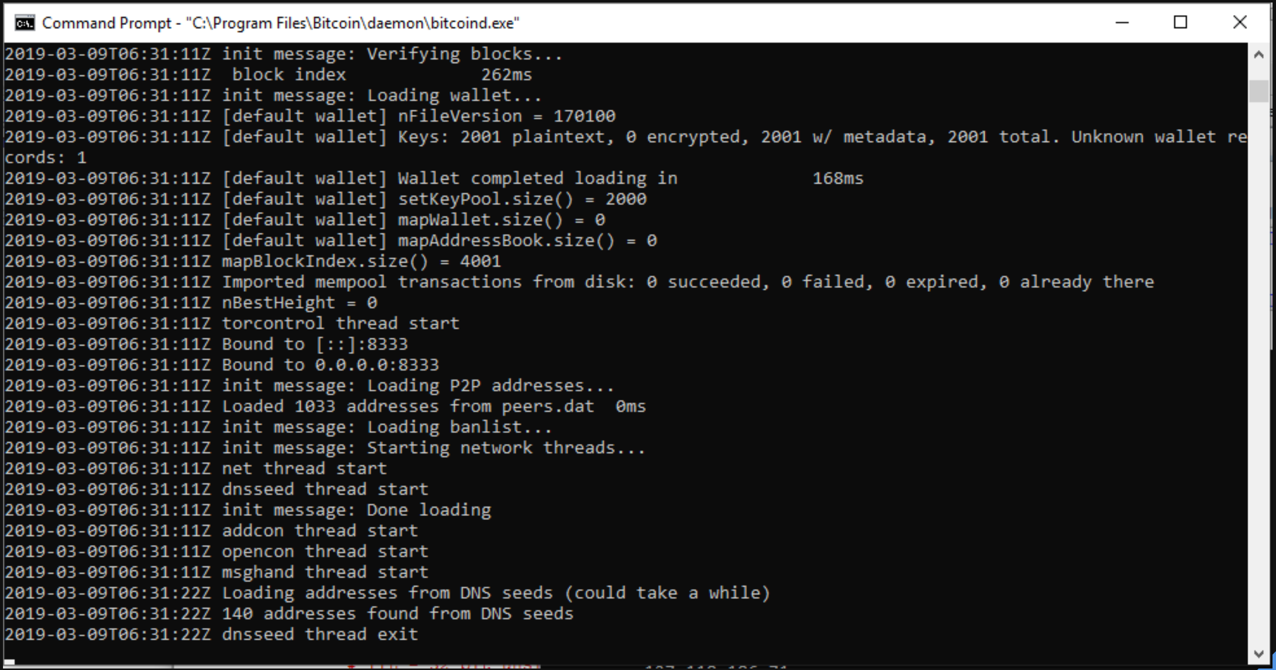
Off

Set time zone automatically

Off

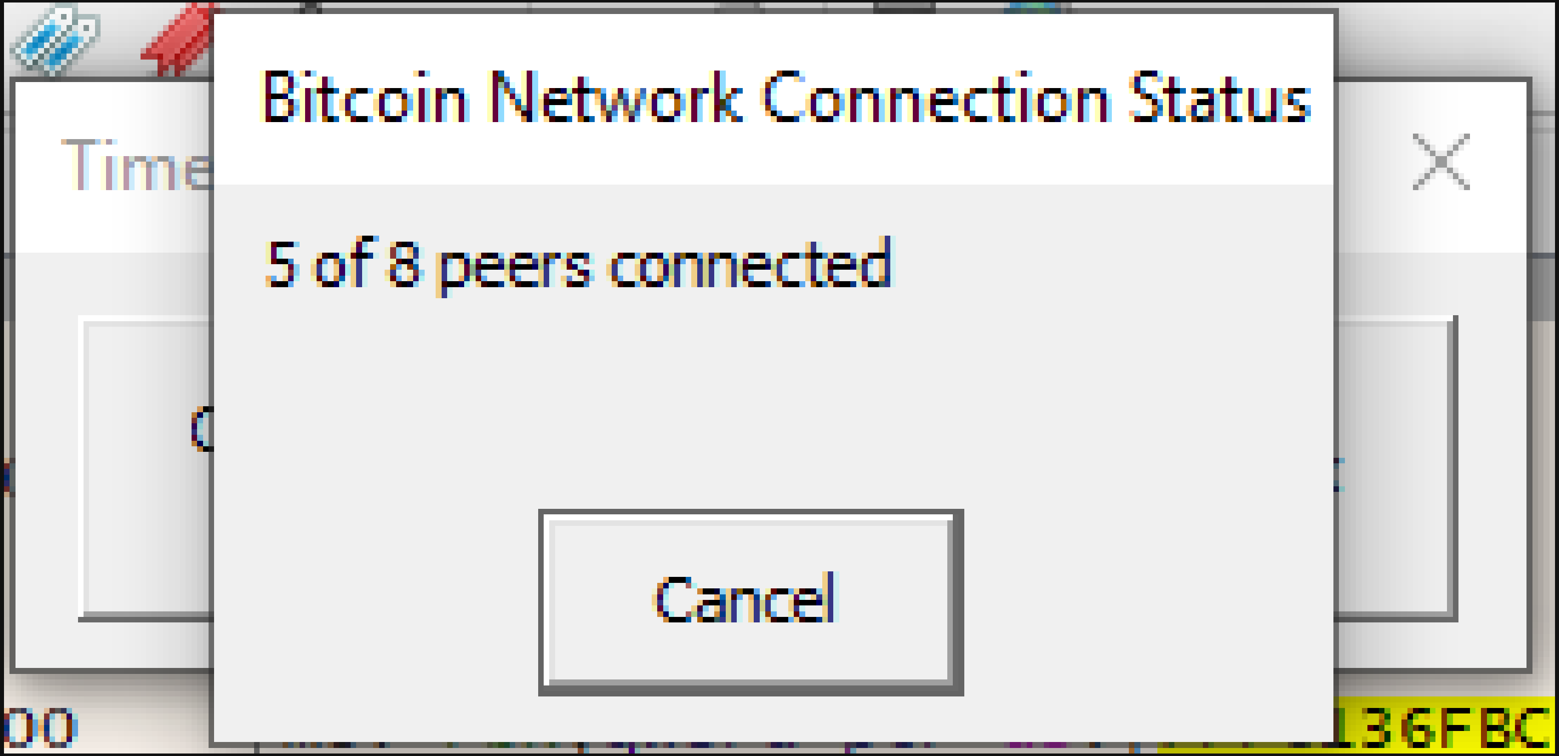
Change date and time

Change


Command Prompt - "C:\Program Files\Bitcoin\daemon\bitcoind.exe"

```
2019-03-09T06:31:11Z init message: Verifying blocks...
2019-03-09T06:31:11Z  block index              262ms
2019-03-09T06:31:11Z init message: Loading wallet...
2019-03-09T06:31:11Z [default wallet] nFileVersion = 170100
2019-03-09T06:31:11Z [default wallet] Keys: 2001 plaintext, 0 encrypted, 2001 w/ metadata, 2001 total. Unknown wallet re
cords: 1
2019-03-09T06:31:11Z [default wallet] Wallet completed loading in              168ms
2019-03-09T06:31:11Z [default wallet] setKeyPool.size() = 2000
2019-03-09T06:31:11Z [default wallet] mapWallet.size() = 0
2019-03-09T06:31:11Z [default wallet] mapAddressBook.size() = 0
2019-03-09T06:31:11Z mapBlockIndex.size() = 4001
2019-03-09T06:31:11Z Imported mempool transactions from disk: 0 succeeded, 0 failed, 0 expired, 0 already there
2019-03-09T06:31:11Z nBestHeight = 0
2019-03-09T06:31:11Z torcontrol thread start
2019-03-09T06:31:11Z Bound to [::]:8333
2019-03-09T06:31:11Z Bound to 0.0.0.0:8333
2019-03-09T06:31:11Z init message: Loading P2P addresses...
2019-03-09T06:31:11Z Loaded 1033 addresses from peers.dat  0ms
2019-03-09T06:31:11Z init message: Loading banlist...
2019-03-09T06:31:11Z init message: Starting network threads...
2019-03-09T06:31:11Z net thread start
2019-03-09T06:31:11Z dnsseed thread start
2019-03-09T06:31:11Z init message: Done loading
2019-03-09T06:31:11Z addcon thread start
2019-03-09T06:31:11Z opencon thread start
2019-03-09T06:31:11Z msghand thread start
2019-03-09T06:31:22Z Loading addresses from DNS seeds (could take a while)
2019-03-09T06:31:22Z 140 addresses found from DNS seeds
2019-03-09T06:31:22Z dnsseed thread exit
```

Did We Hack The Thing Yet?

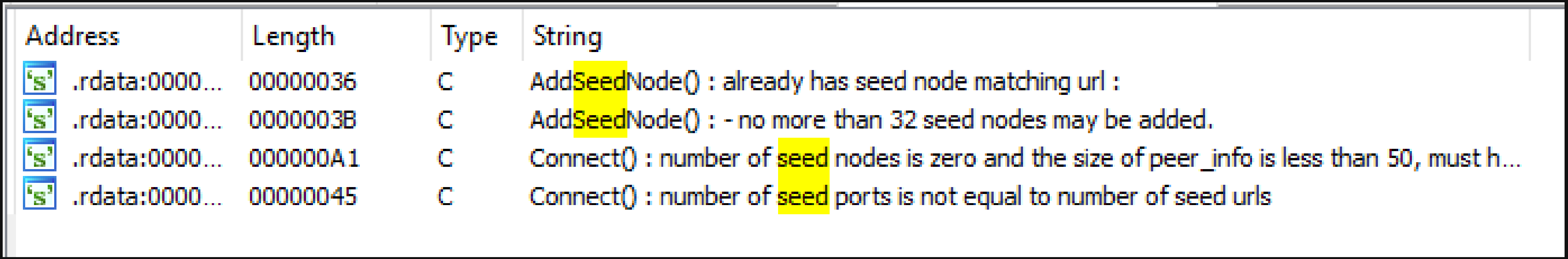


Time

Bitcoin Network Connection Status

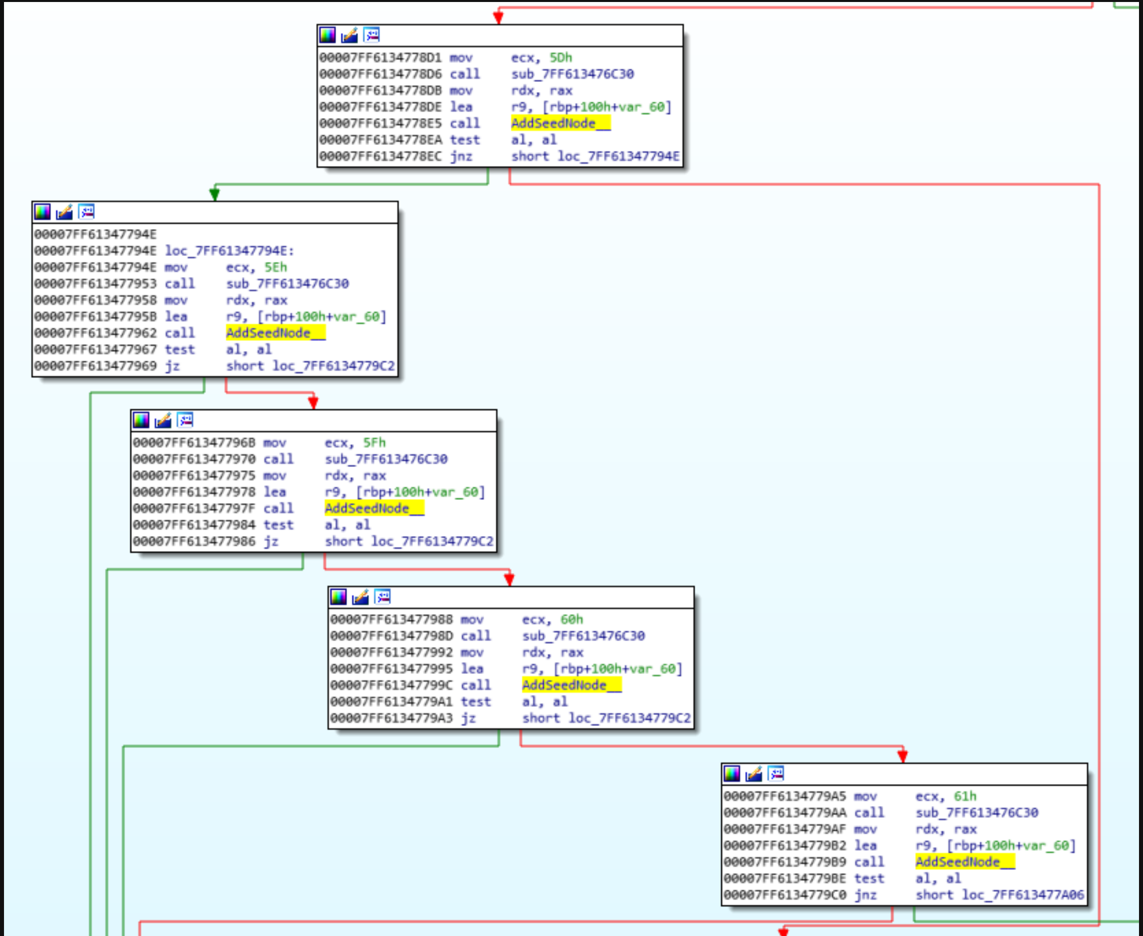
5 of 8 peers connected

When Stuck – Search Strings



Address	Length	Type	String
.rdata:0000...	00000036	C	AddSeedNode() : already has seed node matching url :
.rdata:0000...	0000003B	C	AddSeedNode() : - no more than 32 seed nodes may be added.
.rdata:0000...	000000A1	C	Connect() : number of seed nodes is zero and the size of peer_info is less than 50, must h...
.rdata:0000...	00000045	C	Connect() : number of seed ports is not equal to number of seed urls

Five Calls to AddSeedNode()



```
00007FF6134778D1 mov     ecx, 5Dh
00007FF6134778D6 call    sub_7FF613476C30
00007FF6134778DB mov     rdx, rax
00007FF6134778DE lea     r9, [rbp+100h+var_60]
00007FF6134778E5 call    AddSeedNode__
00007FF6134778EA test    al, al
00007FF6134778EC jnz     short loc_7FF61347794E
```

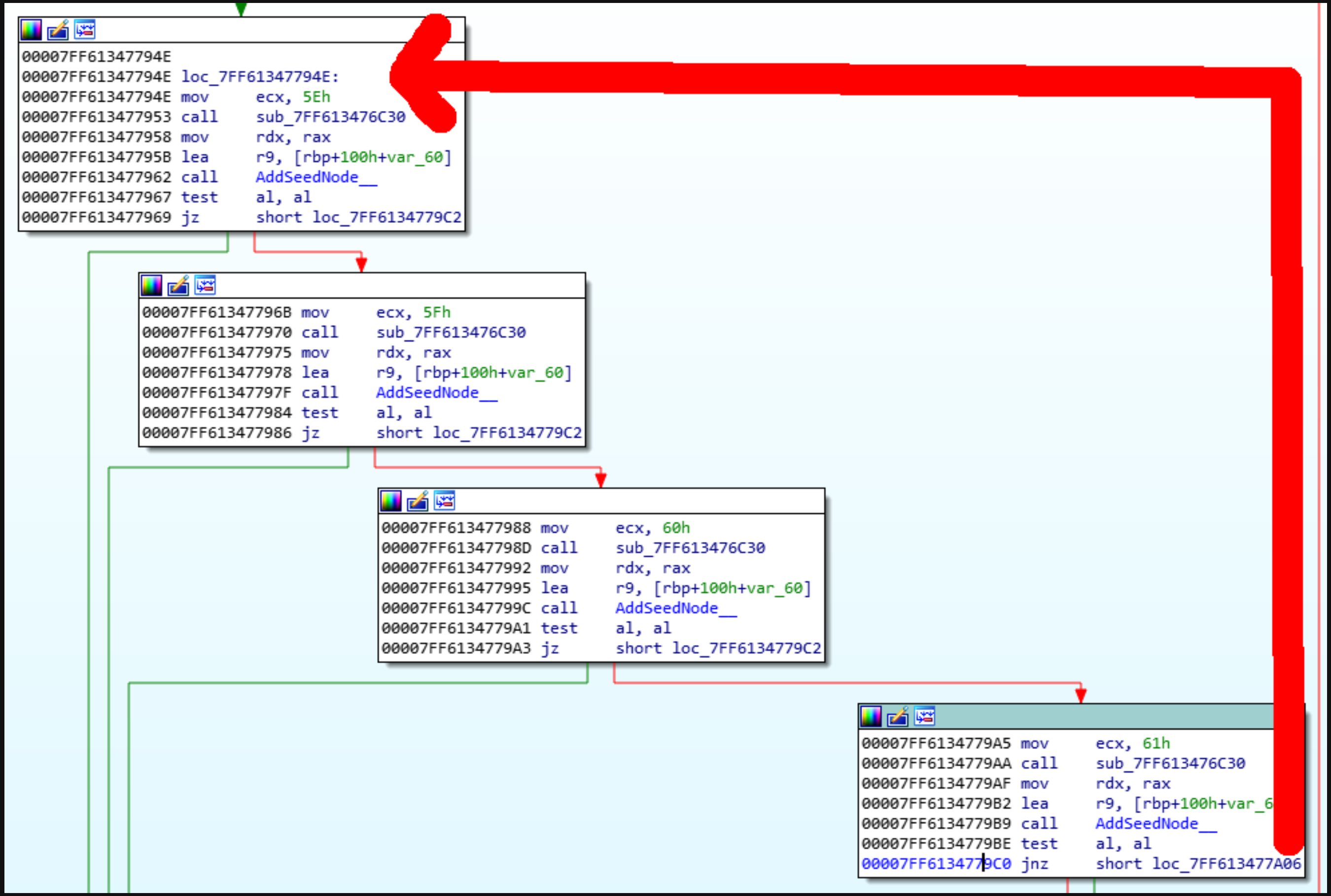
```
00007FF61347794E
00007FF61347794E loc_7FF61347794E:
00007FF61347794E mov     ecx, 5Eh
00007FF613477953 call    sub_7FF613476C30
00007FF613477958 mov     rdx, rax
00007FF61347795B lea     r9, [rbp+100h+var_60]
00007FF613477962 call    AddSeedNode__
00007FF613477967 test    al, al
00007FF613477969 jz      short loc_7FF6134779C2
```

```
00007FF61347796B mov     ecx, 5Fh
00007FF613477970 call    sub_7FF613476C30
00007FF613477975 mov     rdx, rax
00007FF613477978 lea     r9, [rbp+100h+var_60]
00007FF61347797F call    AddSeedNode__
00007FF613477984 test    al, al
00007FF613477986 jz      short loc_7FF6134779C2
```

```
00007FF613477988 mov     ecx, 60h
00007FF61347798D call    sub_7FF613476C30
00007FF613477992 mov     rdx, rax
00007FF613477995 lea     r9, [rbp+100h+var_60]
00007FF61347799C call    AddSeedNode__
00007FF6134779A1 test    al, al
00007FF6134779A3 jz      short loc_7FF6134779C2
```

```
00007FF6134779A5 mov     ecx, 61h
00007FF6134779AA call    sub_7FF613476C30
00007FF6134779AF mov     rdx, rax
00007FF6134779B2 lea     r9, [rbp+100h+var_60]
00007FF6134779B9 call    AddSeedNode__
00007FF6134779BE test    al, al
00007FF6134779C0 jnz     short loc_7FF613477A06
```

What Happens If We Do It Again?



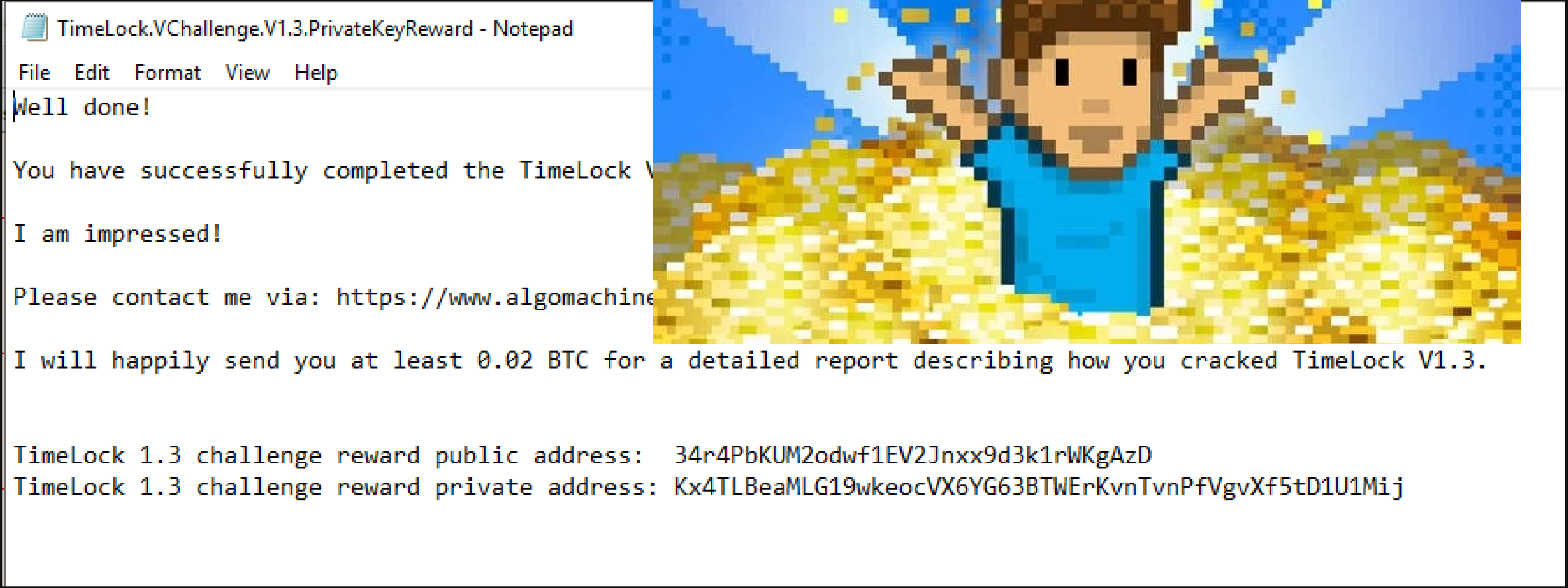
```
00007FF61347794E
00007FF61347794E loc_7FF61347794E:
00007FF61347794E mov     ecx, 5Eh
00007FF613477953 call    sub_7FF613476C30
00007FF613477958 mov     rdx, rax
00007FF61347795B lea     r9, [rbp+100h+var_60]
00007FF613477962 call    AddSeedNode__
00007FF613477967 test    al, al
00007FF613477969 jz      short loc_7FF6134779C2
```

```
00007FF61347796B mov     ecx, 5Fh
00007FF613477970 call    sub_7FF613476C30
00007FF613477975 mov     rdx, rax
00007FF613477978 lea     r9, [rbp+100h+var_60]
00007FF61347797F call    AddSeedNode__
00007FF613477984 test    al, al
00007FF613477986 jz      short loc_7FF6134779C2
```

```
00007FF613477988 mov     ecx, 60h
00007FF61347798D call    sub_7FF613476C30
00007FF613477992 mov     rdx, rax
00007FF613477995 lea     r9, [rbp+100h+var_60]
00007FF61347799C call    AddSeedNode__
00007FF6134779A1 test    al, al
00007FF6134779A3 jz      short loc_7FF6134779C2
```

```
00007FF6134779A5 mov     ecx, 61h
00007FF6134779AA call    sub_7FF613476C30
00007FF6134779AF mov     rdx, rax
00007FF6134779B2 lea     r9, [rbp+100h+var_6
00007FF6134779B9 call    AddSeedNode__
00007FF6134779BE test    al, al
00007FF6134779C0 jnz     short loc_7FF613477A06
```

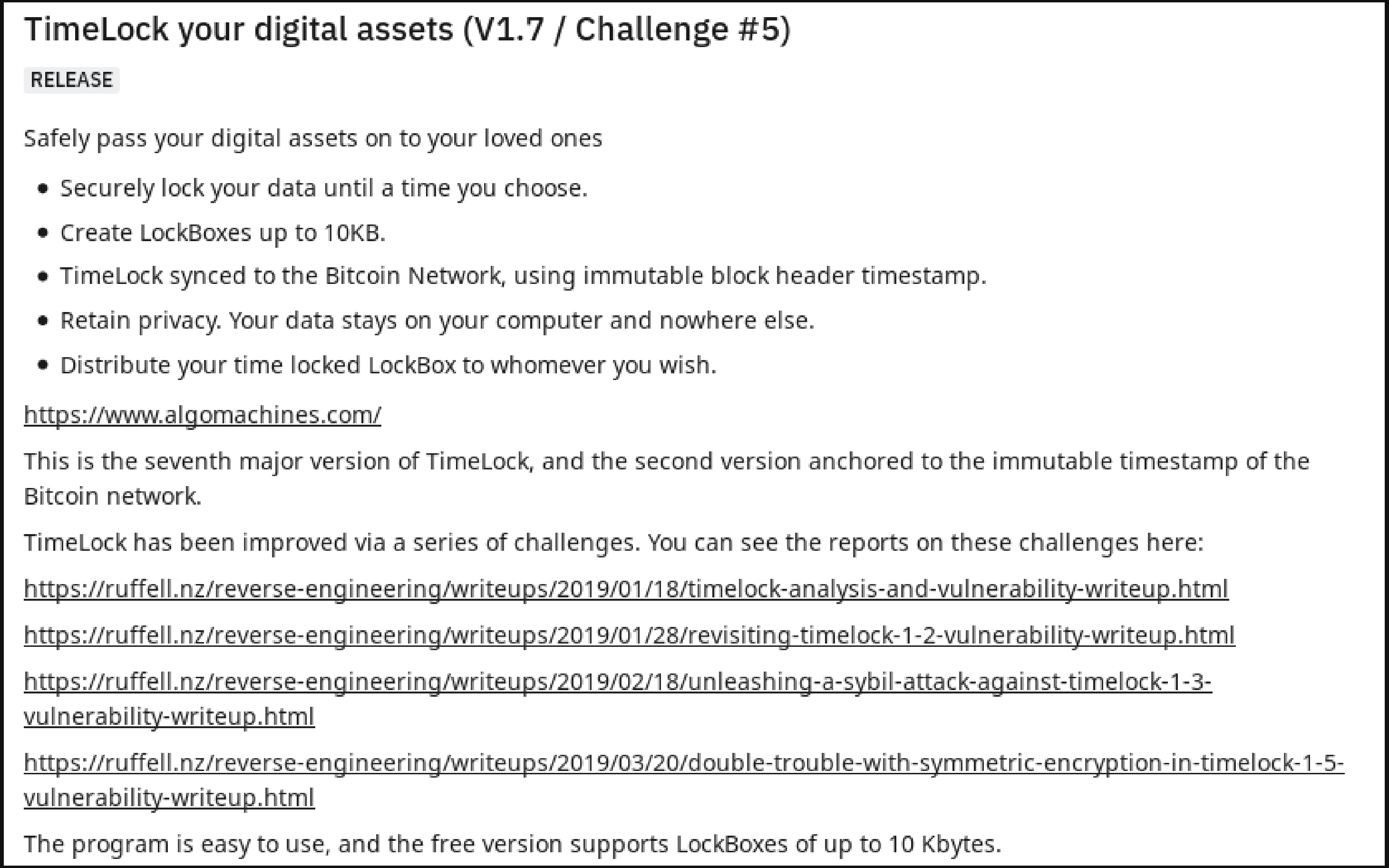
Loot #3



TimeLock.VChallenge.V1.3.PrivateKeyReward - Notepad

```
Well done!

You have successfully completed the TimeLock V

I am impressed!

Please contact me via: https://www.algomachine

I will happily send you at least 0.02 BTC for a detailed report describing how you cracked TimeLock V1.3.


TimeLock 1.3 challenge reward public address:  34r4PbKUM2odwf1EV2Jnxx9d3k1rWKgAzD
TimeLock 1.3 challenge reward private address: Kx4TLBeaMLG19wkeocVX6YG63BTWErKvnTvnPfVgvXf5tD1U1Mij
```

Challenge #4 and #5



TimeLock your digital assets (V1.7 / Challenge #5)

RELEASE

Safely pass your digital assets on to your loved ones

- Securely lock your data until a time you choose.
- Create LockBoxes up to 10KB.
- TimeLock synced to the Bitcoin Network, using immutable block header timestamp.
- Retain privacy. Your data stays on your computer and nowhere else.
- Distribute your time locked LockBox to whomever you wish.

https://www.algomachines.com/

This is the seventh major version of TimeLock, and the second version anchored to the immutable timestamp of the Bitcoin network.

TimeLock has been improved via a series of challenges. You can see the reports on these challenges here:

https://ruffell.nz/reverse-engineering/writeups/2019/01/18/timelock-analysis-and-vulnerability-writeup.html

https://ruffell.nz/reverse-engineering/writeups/2019/01/28/revisiting-timelock-1-2-vulnerability-writeup.html

https://ruffell.nz/reverse-engineering/writeups/2019/02/18/unleashing-a-sybil-attack-against-timelock-1-3-vulnerability-writeup.html

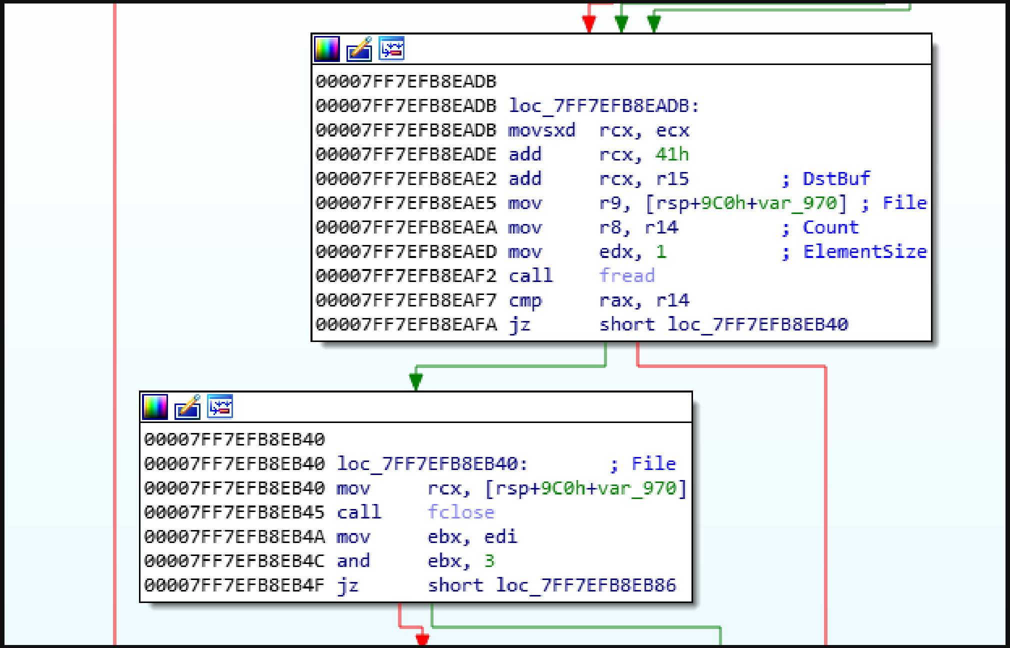
https://ruffell.nz/reverse-engineering/writeups/2019/03/20/double-trouble-with-symmetric-encryption-in-timelock-1-5-vulnerability-writeup.html

The program is easy to use, and the free version supports LockBoxes of up to 10 Kbytes.

Plan of Attack

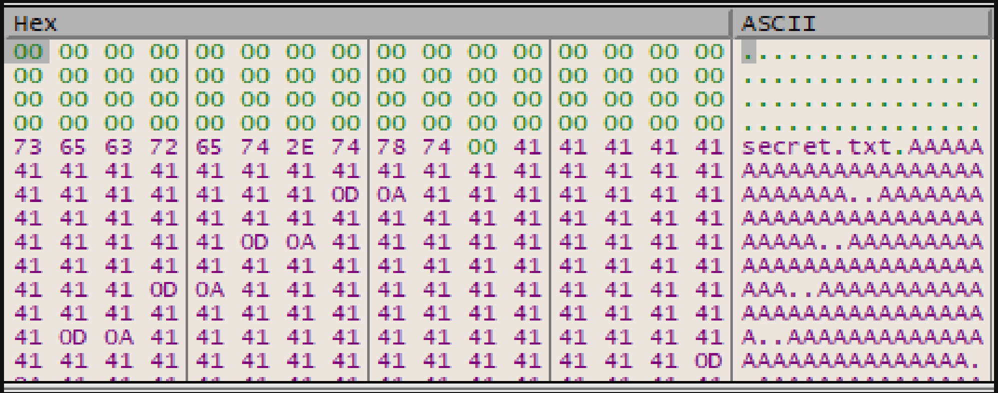
- Review encryption functions:
  - Look for bad modes of encryption.
  - Look for weak encryption schemes.
- *“Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break” - Bruce Schneier*

Locate Encryption Functions

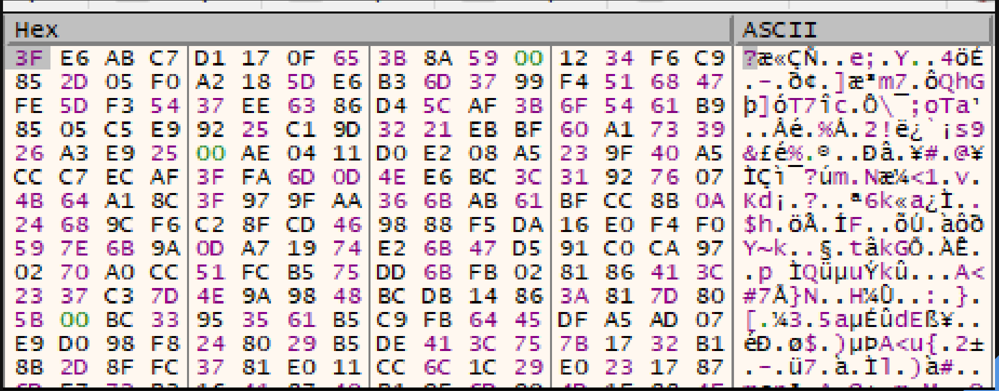


```
00007FF7EFB8EADB
00007FF7EFB8EADB loc_7FF7EFB8EADB:
00007FF7EFB8EADB movsxd  rcx, ecx
00007FF7EFB8EADE add     rcx, 41h
00007FF7EFB8EAE2 add     rcx, r15         ; DstBuf
00007FF7EFB8EAE5 mov     r9, [rsp+9C0h+var_970] ; File
00007FF7EFB8EAEA mov     r8, r14          ; Count
00007FF7EFB8EAED mov     edx, 1           ; ElementSize
00007FF7EFB8EAF2 call    fread
00007FF7EFB8EAF7 cmp     rax, r14
00007FF7EFB8EAFA jz      short loc_7FF7EFB8EB40
```

```
00007FF7EFB8EB40
00007FF7EFB8EB40 loc_7FF7EFB8EB40:         ; File
00007FF7EFB8EB40 mov     rcx, [rsp+9C0h+var_970]
00007FF7EFB8EB45 call    fclose
00007FF7EFB8EB4A mov     ebx, edi
00007FF7EFB8EB4C and     ebx, 3
00007FF7EFB8EB4F jz      short loc_7FF7EFB8EB86
```



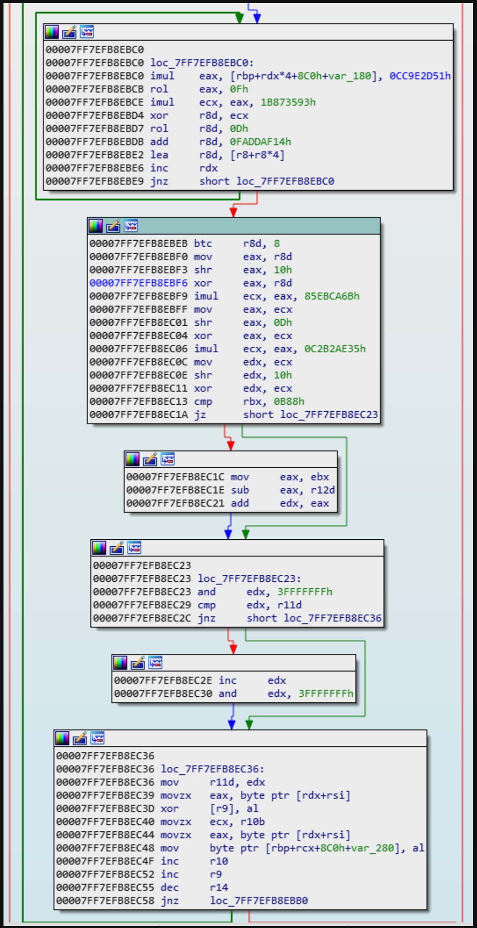
```
Hex                                                ASCII
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
73 65 63 72 65 74 2E 74 78 74 00 41 41 41 41 41   secret.txt.AAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 0D 0A 41 41 41 41 41 41 41   AAAAAAA..AAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
41 41 41 41 41 0D 0A 41 41 41 41 41 41 41 41 41   AAAAA..AAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
41 41 41 0D 0A 41 41 41 41 41 41 41 41 41 41 41   AAA..AAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
41 0D 0A 41 41 41 41 41 41 41 41 41 41 41 41 41   A..AAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 0D   AAAAAAAAAAAAAAA.
```



```
Hex                                                ASCII
3F E6 AB C7 D1 17 0F 65 3B 8A 59 00 12 34 F6 C9   ?æ«ÇÑ..e;.Y..4öÉ
85 2D 05 F0 A2 18 5D E6 B3 6D 37 99 F4 51 68 47   .-.ð¢.]æ³m7.ôQhG
FE 5D F3 54 37 EE 63 86 D4 5C AF 3B 6F 54 61 B9   þ]óT7îc.Ô\¯;oTa¹
85 05 C5 E9 92 25 C1 9D 32 21 EB BF 60 A1 73 39   ..Åé.%Á.2!ë¿`¡s9
26 A3 E9 25 00 AE 04 11 D0 E2 08 A5 23 9F 40 A5   &£é%.®..Ðâ.¥#.@¥
CC C7 EC AF 3F FA 6D 0D 4E E6 BC 3C 31 92 76 07   ÌÇì¯?úm.Næ¼<1.v.
4B 64 A1 8C 3F 97 9F AA 36 6B AB 61 BF CC 8B 0A   Kd¡.?..ª6k«a¿Ì..
24 68 9C F6 C2 8F CD 46 98 88 F5 DA 16 E0 F4 F0   $h.öÂ.ÍF..õÚ.àôð
59 7E 6B 9A 0D A7 19 74 E2 6B 47 D5 91 C0 CA 97   Y~k..§.tâkGÕ.ÀÊ.
02 70 A0 CC 51 FC B5 75 DD 6B FB 02 81 86 41 3C   .p ÌQüµuÝkû...A<
23 37 C3 7D 4E 9A 98 48 BC DB 14 86 3A 81 7D 80   #7Ã}N..H¼Û..:.}.
5B 00 BC 33 95 35 61 B5 C9 FB 64 45 DF A5 AD 07   [.¼3.5aµÉûdEß¥..
E9 D0 98 F8 24 80 29 B5 DE 41 3C 75 7B 17 32 B1   éÐ.ø$.)µÞA<u{.2±
8B 2D 8F FC 37 81 E0 11 CC 6C 1C 29 E0 23 17 87   .-.ü7.à.Ìl.)à#..
```

Encryption Round

Generates single byte keystream



```
00007FF7EFB8EBC0
00007FF7EFB8EBC0 loc_7FF7EFB8EBC0:
00007FF7EFB8EBC0 imul    eax, [rbp+rdx*4+8C0h+var_180], 0CC9E2D51h
00007FF7EFB8EBCB rol     eax, 0Fh
00007FF7EFB8EBCE imul    ecx, eax, 1B873593h
00007FF7EFB8EBD4 xor     r8d, ecx
00007FF7EFB8EBD7 rol     r8d, 0Dh
00007FF7EFB8EBDB add     r8d, 0FADDAF14h
00007FF7EFB8EBE2 lea     r8d, [r8+r8*4]
00007FF7EFB8EBE6 inc     rdx
00007FF7EFB8EBE9 jnz     short loc_7FF7EFB8EBC0
```

```
00007FF7EFB8EBEB btc     r8d, 8
00007FF7EFB8EBF0 mov     eax, r8d
00007FF7EFB8EBF3 shr     eax, 10h
00007FF7EFB8EBF6 xor     eax, r8d
00007FF7EFB8EBF9 imul    ecx, eax, 85EBCA6Bh
00007FF7EFB8EBFF mov     eax, ecx
00007FF7EFB8EC01 shr     eax, 0Dh
00007FF7EFB8EC04 xor     eax, ecx
00007FF7EFB8EC06 imul    ecx, eax, 0C2B2AE35h
00007FF7EFB8EC0C mov     edx, ecx
00007FF7EFB8EC0E shr     edx, 10h
00007FF7EFB8EC11 xor     edx, ecx
00007FF7EFB8EC13 cmp     rbx, 0B88h
00007FF7EFB8EC1A jz      short loc_7FF7EFB8EC23
```

```
00007FF7EFB8EC1C mov     eax, ebx
00007FF7EFB8EC1E sub     eax, r12d
00007FF7EFB8EC21 add     edx, eax
```

```
00007FF7EFB8EC23
00007FF7EFB8EC23 loc_7FF7EFB8EC23:
00007FF7EFB8EC23 and     edx, 3FFFFFFFh
00007FF7EFB8EC29 cmp     edx, r11d
00007FF7EFB8EC2C jnz     short loc_7FF7EFB8EC36
```

```
00007FF7EFB8EC2E inc     edx
00007FF7EFB8EC30 and     edx, 3FFFFFFFh
```

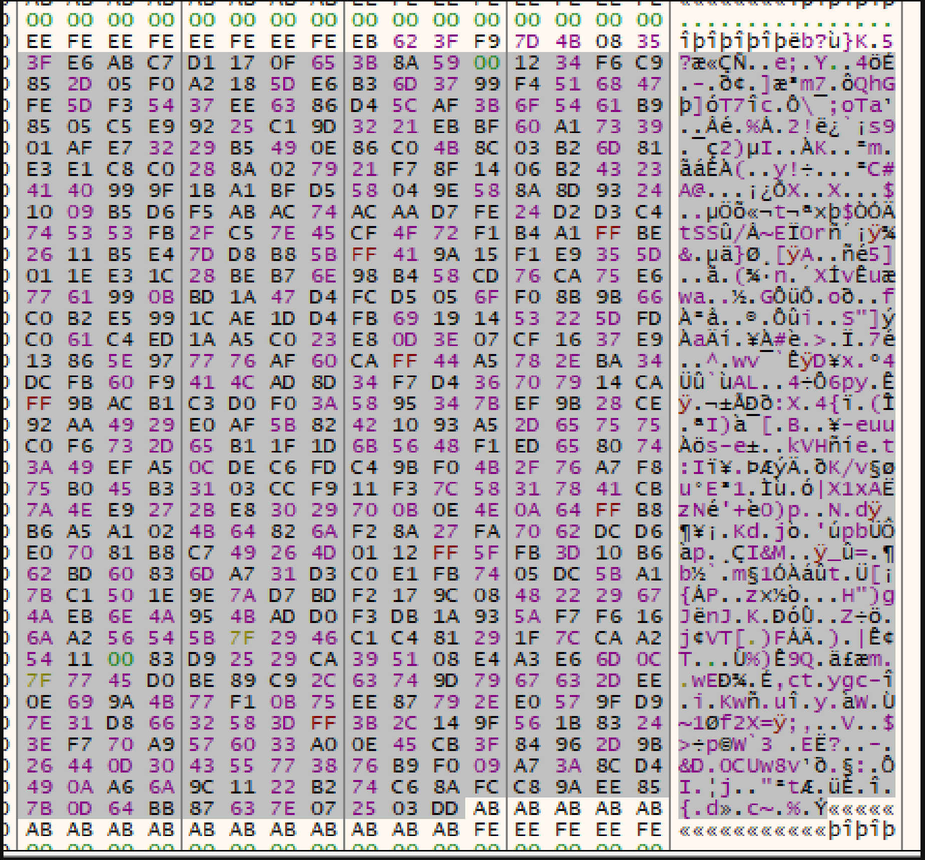
```
00007FF7EFB8EC36
00007FF7EFB8EC36 loc_7FF7EFB8EC36:
00007FF7EFB8EC36 mov     r11d, edx
00007FF7EFB8EC39 movzx   eax, byte ptr [rdx+rsi]
00007FF7EFB8EC3D xor     [r9], al
00007FF7EFB8EC40 movzx   ecx, r10b
00007FF7EFB8EC44 movzx   eax, byte ptr [rdx+rsi]
00007FF7EFB8EC48 mov     byte ptr [rbp+rcx+8C0h+var_280], al
00007FF7EFB8EC4F inc     r10
00007FF7EFB8EC52 inc     r9
00007FF7EFB8EC55 dec     r14
00007FF7EFB8EC58 jnz     loc_7FF7EFB8EBB0
```

XOR 1 byte plaintext with 1 byte keystream

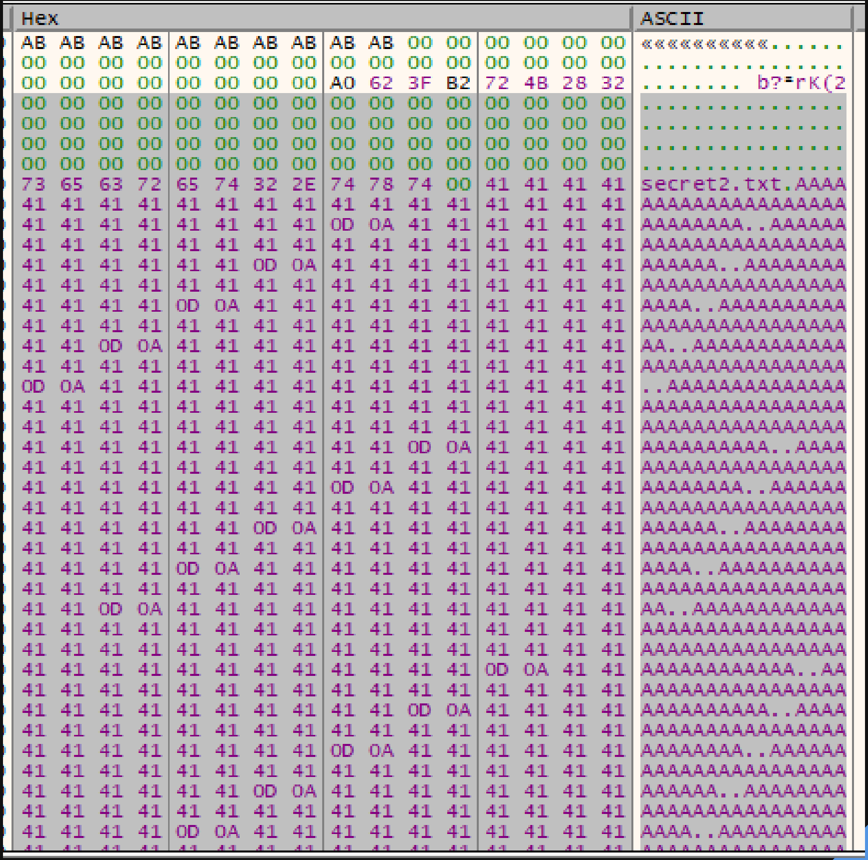
Symmetric Encryption

- Ciphertext is deterministic:
  - Same inputs create same outputs.
- Encryption is performed by xor…
  - … so we can “decrypt” by xoring again!
- We have symmetric encryption!

Extract Ciphertext, Create New LockBox

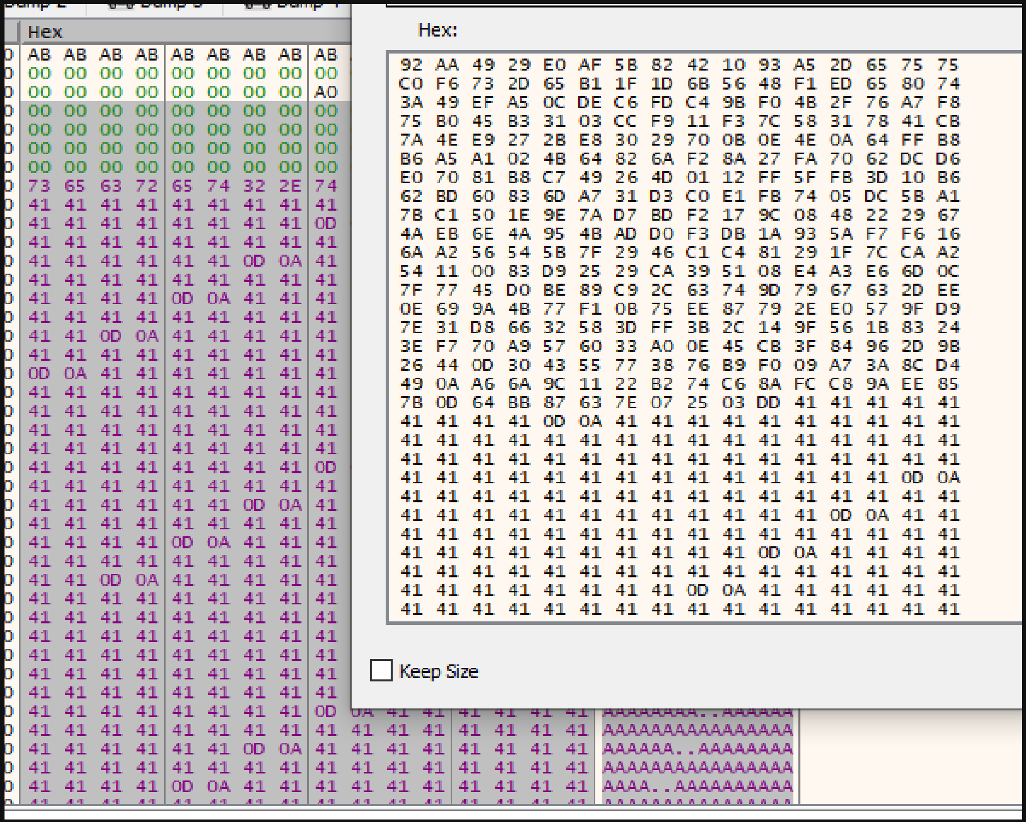


```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
EE FE EE FE EE FE EE FE EB 62 3F F9 7D 4B 08 35  îþîþîþîþëb?ù}K.5
3F E6 AB C7 D1 17 0F 65 3B 8A 59 00 12 34 F6 C9  ?æ«ÇÑ..e;.Y..4öÉ
85 2D 05 F0 A2 18 5D E6 B3 6D 37 99 F4 51 68 47  .-.ð¢.]æ³m7.ôQhG
FE 5D F3 54 37 EE 63 86 D4 5C AF 3B 6F 54 61 B9  þ]óT7îc.Ô\¯;oTa¹
85 05 C5 E9 92 25 C1 9D 32 21 EB BF 60 A1 73 39  ..Åé.%Á.2!ë¿`¡s9
01 AF E7 32 29 B5 49 0E 86 C0 4B 8C 03 B2 6D 81  .¯ç2)µI..ÀK..²m.
E3 E1 C8 C0 28 8A 02 79 21 F7 8F 14 06 B2 43 23  ãáÈÀ(..y!÷...²C#
41 40 99 9F 1B A1 BF D5 58 04 9E 58 8A 8D 93 24  A@...¡¿ÕX..X...$
10 09 B5 D6 F5 AB AC 74 AC AA D7 FE 24 D2 D3 C4  ..µÖõ«¬t¬ª×þ$ÒÓÄ
74 53 53 FB 2F C5 7E 45 CF 4F 72 F1 B4 A1 FF BE  tSSû/Å~EÏOrñ´¡ÿ¾
26 11 B5 E4 7D D8 B8 5B FF 41 9A 15 F1 E9 35 5D  &.µä}Ø¸[ÿA..ñé5]
01 1E E3 1C 28 BE B7 6E 98 B4 58 CD 76 CA 75 E6  ..ã.(¾·n.´XÍvÊuæ
77 61 99 0B BD 1A 47 D4 FC D5 05 6F F0 8B 9B 66  wa..½.GÔüÕ.oð..f
C0 B2 E5 99 1C AE 1D D4 FB 69 19 14 53 22 5D FD  À²å..®.Ôûi..S"]ý
C0 61 C4 ED 1A A5 C0 23 E8 0D 3E 07 CF 16 37 E9  ÀaÄí.¥À#è.>.Ï.7é
13 86 5E 97 77 76 AF 60 CA FF 44 A5 78 2E BA 34  ..^.wv¯`ÊÿD¥x.º4
DC FB 60 F9 41 4C AD 8D 34 F7 D4 36 70 79 14 CA  Üû`ùAL..4÷Ô6py.Ê
FF 9B AC B1 C3 D0 F0 3A 58 95 34 7B EF 9B 28 CE  ÿ.¬±ÃÐð:X.4{ï.(Î
92 AA 49 29 E0 AF 5B 82 42 10 93 A5 2D 65 75 75  .ªI)à¯[.B..¥-euu
C0 F6 73 2D 65 B1 1F 1D 6B 56 48 F1 ED 65 80 74  Àös-e±..kVHñíe.t
3A 49 EF A5 0C DE C6 FD C4 9B F0 4B 2F 76 A7 F8  :Iï¥.ÞÆýÄ.ðK/v§ø
75 B0 45 B3 31 03 CC F9 11 F3 7C 58 31 78 41 CB  u°E³1.Ìù.ó|X1xAË
7A 4E E9 27 2B E8 30 29 70 0B 0E 4E 0A 64 FF B8  zNé'+è0)p..N.dÿ¸
B6 A5 A1 02 4B 64 82 6A F2 8A 27 FA 70 62 DC D6  ¶¥¡.Kd.jò.'úpbÜÖ
E0 70 81 B8 C7 49 26 4D 01 12 FF 5F FB 3D 10 B6  àp.¸ÇI&M..ÿ_û=.¶
62 BD 60 83 6D A7 31 D3 C0 E1 FB 74 05 DC 5B A1  b½`.m§1ÓÀáût.Ü[¡
7B C1 50 1E 9E 7A D7 BD F2 17 9C 08 48 22 29 67  {ÁP..z×½ò...H")g
4A EB 6E 4A 95 4B AD D0 F3 DB 1A 93 5A F7 F6 16  JënJ.K.ÐóÛ..Z÷ö.
6A A2 56 54 5B 7F 29 46 C1 C4 81 29 1F 7C CA A2  j¢VT[.)FÁÄ.).|Ê¢
54 11 00 83 D9 25 29 CA 39 51 08 E4 A3 E6 6D 0C  T...Ù%)Ê9Q.ä£æm.
7F 77 45 D0 BE 89 C9 2C 63 74 9D 79 67 63 2D EE  .wEÐ¾.É,ct.ygc-î
0E 69 9A 4B 77 F1 0B 75 EE 87 79 2E E0 57 9F D9  .i.Kwñ.uî.y.àW.Ù
7E 31 D8 66 32 58 3D FF 3B 2C 14 9F 56 1B 83 24  ~1Øf2X=ÿ;,..V..$
3E F7 70 A9 57 60 33 A0 0E 45 CB 3F 84 96 2D 9B  >÷p©W`3 .EË?..-.
26 44 0D 30 43 55 77 38 76 B9 F0 09 A7 3A 8C D4  &D.0CUw8v¹ð.§:.Ô
49 0A A6 6A 9C 11 22 B2 74 C6 8A FC C8 9A EE 85  I.¦j.."²tÆ.üÈ.î.
7B 0D 64 BB 87 63 7E 07 25 03 DD AB AB AB AB AB  {.d».c~.%.Ý«««««
AB AB AB AB AB AB AB AB AB AB AB FE EE FE EE FE  «««««««««««þîþîþ
```



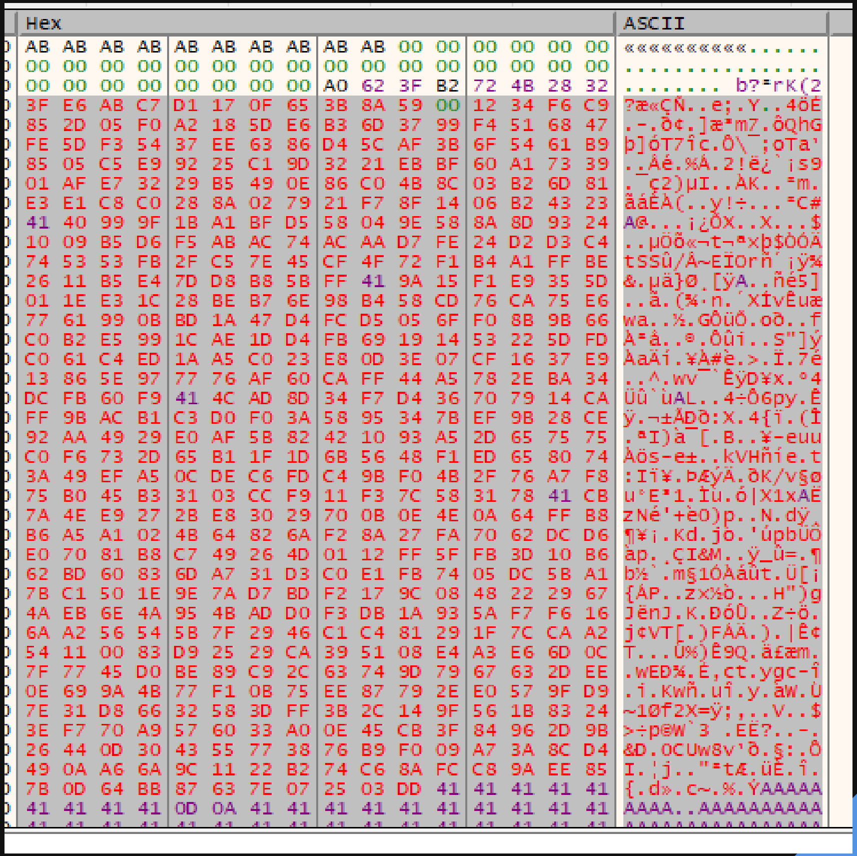
```
Hex                                                ASCII
AB AB AB AB AB AB AB AB AB AB 00 00 00 00 00 00  ««««««««««......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 A0 62 3F B2 72 4B 28 32  ........ b?²rK(2
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
73 65 63 72 65 74 32 2E 74 78 74 00 41 41 41 41  secret2.txt.AAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 0D 0A 41 41 41 41 41 41  AAAAAAAA..AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 0D 0A 41 41 41 41 41 41 41 41  AAAAAA..AAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 0D 0A 41 41 41 41 41 41 41 41 41 41  AAAA..AAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 0D 0A 41 41 41 41 41 41 41 41 41 41 41 41  AA..AAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0D 0A 41 41 41 41 41 41 41 41 41 41 41 41 41 41  ..AAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 0D 0A 41 41 41 41  AAAAAAAAAA..AAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 0D 0A 41 41 41 41 41 41  AAAAAAAA..AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 0D 0A 41 41 41 41 41 41 41 41  AAAAAA..AAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 0D 0A 41 41 41 41 41 41 41 41 41 41  AAAA..AAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 0D 0A 41 41 41 41 41 41 41 41 41 41 41 41  AA..AAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 0D 0A 41 41  AAAAAAAAAAAA..AA
41 41 41 41 41 41 41 41 41 41 0D 0A 41 41 41 41  AAAAAAAAAA..AAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 0D 0A 41 41 41 41 41 41  AAAAAAAA..AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 0D 0A 41 41 41 41 41 41 41 41  AAAAAA..AAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 0D 0A 41 41 41 41 41 41 41 41 41 41  AAAA..AAAAAAAAAA
```

Replace Dummy Data With Ciphertext



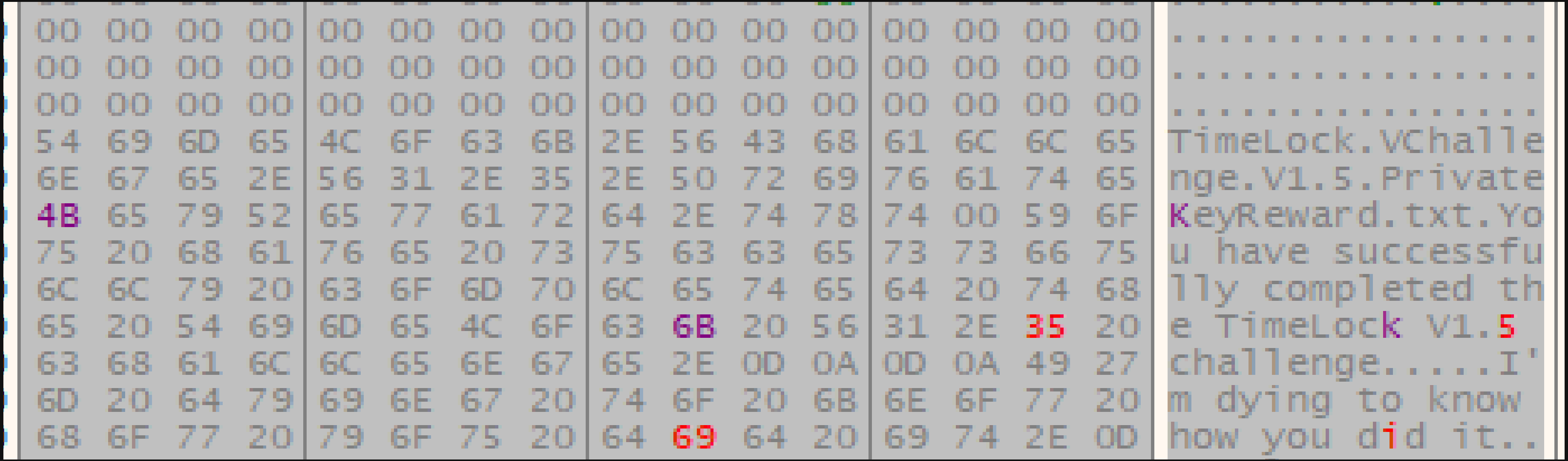
```
Hex
AB AB AB AB  AB AB AB AB  AB
00 00 00 00  00 00 00 00  00
00 00 00 00  00 00 00 00  A0
00 00 00 00  00 00 00 00  00
00 00 00 00  00 00 00 00  00
00 00 00 00  00 00 00 00  00
00 00 00 00  00 00 00 00  00
73 65 63 72  65 74 32 2E  74
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  0D
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 0D 0A  41
41 41 41 41  41 41 41 41  41
41 41 41 41  0D 0A 41 41  41
41 41 41 41  41 41 41 41  41
41 41 0D 0A  41 41 41 41  41
41 41 41 41  41 41 41 41  41
0D 0A 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  0D
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 0D 0A  41
41 41 41 41  41 41 41 41  41
41 41 41 41  0D 0A 41 41  41
41 41 41 41  41 41 41 41  41
41 41 0D 0A  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  41
41 41 41 41  41 41 41 41  0D 0A 41 41  41 41 41 41  AAAAAAAA..AAAAAA
41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41  41 41 0D 0A  41 41 41 41  41 41 41 41  AAAAAA..AAAAAAAA
41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41  0D 0A 41 41  41 41 41 41  41 41 41 41  AAAA..AAAAAAAAAA
```

```
Hex:

92 AA 49 29 E0 AF 5B 82 42 10 93 A5 2D 65 75 75
C0 F6 73 2D 65 B1 1F 1D 6B 56 48 F1 ED 65 80 74
3A 49 EF A5 0C DE C6 FD C4 9B F0 4B 2F 76 A7 F8
75 B0 45 B3 31 03 CC F9 11 F3 7C 58 31 78 41 CB
7A 4E E9 27 2B E8 30 29 70 0B 0E 4E 0A 64 FF B8
B6 A5 A1 02 4B 64 82 6A F2 8A 27 FA 70 62 DC D6
E0 70 81 B8 C7 49 26 4D 01 12 FF 5F FB 3D 10 B6
62 BD 60 83 6D A7 31 D3 C0 E1 FB 74 05 DC 5B A1
7B C1 50 1E 9E 7A D7 BD F2 17 9C 08 48 22 29 67
4A EB 6E 4A 95 4B AD D0 F3 DB 1A 93 5A F7 F6 16
6A A2 56 54 5B 7F 29 46 C1 C4 81 29 1F 7C CA A2
54 11 00 83 D9 25 29 CA 39 51 08 E4 A3 E6 6D 0C
7F 77 45 D0 BE 89 C9 2C 63 74 9D 79 67 63 2D EE
0E 69 9A 4B 77 F1 0B 75 EE 87 79 2E E0 57 9F D9
7E 31 D8 66 32 58 3D FF 3B 2C 14 9F 56 1B 83 24
3E F7 70 A9 57 60 33 A0 0E 45 CB 3F 84 96 2D 9B
26 44 0D 30 43 55 77 38 76 B9 F0 09 A7 3A 8C D4
49 0A A6 6A 9C 11 22 B2 74 C6 8A FC C8 9A EE 85
7B 0D 64 BB 87 63 7E 07 25 03 DD 41 41 41 41 41
41 41 41 41 0D 0A 41 41 41 41 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 0D 0A
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 0D 0A 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 0D 0A 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
41 41 41 41 41 41 41 41 0D 0A 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41

[ ] Keep Size
```



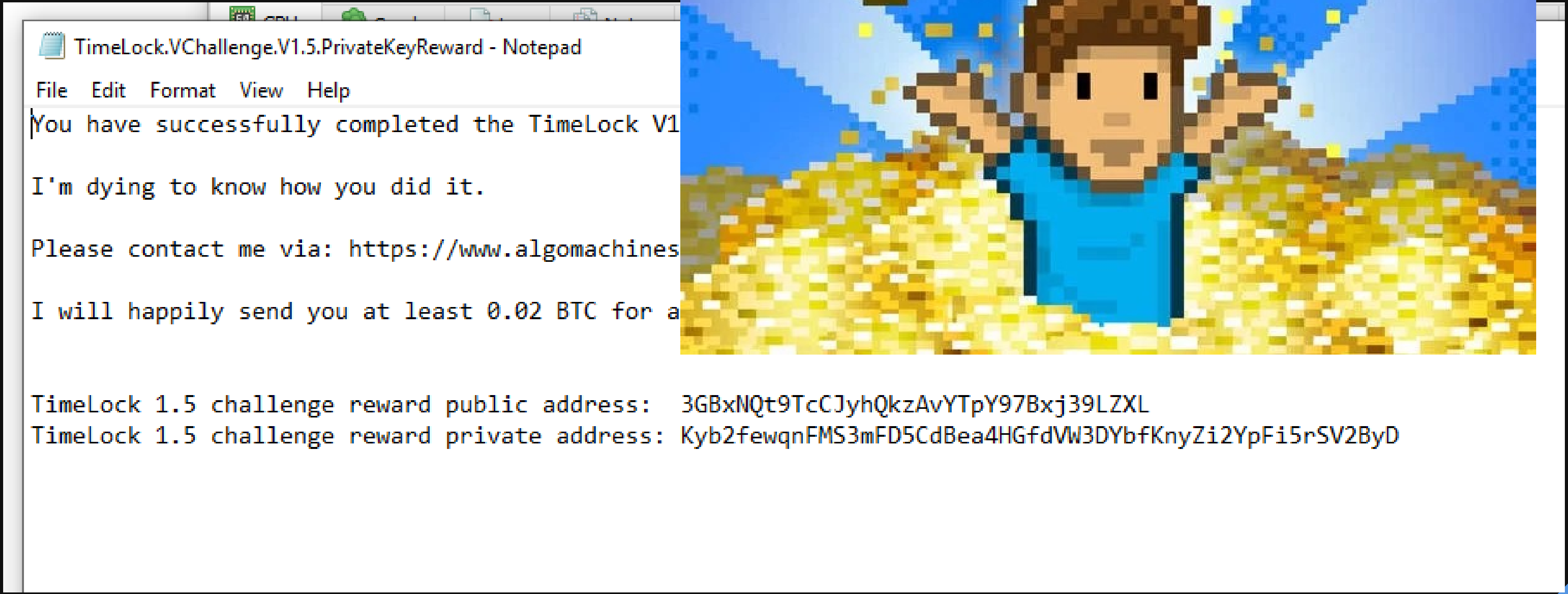
```
Hex                                                  ASCII
AB AB AB AB  AB AB AB AB  AB AB 00 00  00 00 00 00   ««««««««««......
00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00 00 00 00  00 00 00 00  A0 62 3F B2  72 4B 28 32   ........ b?²rK(2
3F E6 AB C7  D1 17 0F 65  3B 8A 59 00  12 34 F6 C9   ?æ«ÇÑ..e;.Y..4öÉ
85 2D 05 F0  A2 18 5D E6  B3 6D 37 99  F4 51 68 47   .-.ð¢.]æ³m7.ôQhG
FE 5D F3 54  37 EE 63 86  D4 5C AF 3B  6F 54 61 B9   þ]óT7îc.Ô\¯;oTa¹
85 05 C5 E9  92 25 C1 9D  32 21 EB BF  60 A1 73 39   ..Åé.%Á.2!ë¿`¡s9
01 AF E7 32  29 B5 49 0E  86 C0 4B 8C  03 B2 6D 81   .¯ç2)µI..ÀK..²m.
E3 E1 C8 C0  28 8A 02 79  21 F7 8F 14  06 B2 43 23   ãáÈÀ(..y!÷...²C#
41 40 99 9F  1B A1 BF D5  58 04 9E 58  8A 8D 93 24   A@...¡¿ÕX..X...$
10 09 B5 D6  F5 AB AC 74  AC AA D7 FE  24 D2 D3 C4   ..µÖõ«¬t¬ª×þ$ÒÓÄ
74 53 53 FB  2F C5 7E 45  CF 4F 72 F1  B4 A1 FF BE   tSSû/Å~EÏOrñ´¡ÿ¾
26 11 B5 E4  7D D8 B8 5B  FF 41 9A 15  F1 E9 35 5D   &.µä}Ø¸[ÿA..ñé5]
01 1E E3 1C  28 BE B7 6E  98 B4 58 CD  76 CA 75 E6   ..ã.(¾·n.´XÍvÊuæ
77 61 99 0B  BD 1A 47 D4  FC D5 05 6F  F0 8B 9B 66   wa..½.GÔüÕ.oð..f
C0 B2 E5 99  1C AE 1D D4  FB 69 19 14  53 22 5D FD   À²å..®.Ôûi..S"]ý
C0 61 C4 ED  1A A5 C0 23  E8 0D 3E 07  CF 16 37 E9   ÀaÄí.¥À#è.>.Ï.7é
13 86 5E 97  77 76 AF 60  CA FF 44 A5  78 2E BA 34   ..^.wv¯`ÊÿD¥x.º4
DC FB 60 F9  41 4C AD 8D  34 F7 D4 36  70 79 14 CA   Üû`ùAL..4÷Ô6py.Ê
FF 9B AC B1  C3 D0 F0 3A  58 95 34 7B  EF 9B 28 CE   ÿ.¬±ÃÐð:X.4{ï.(Î
92 AA 49 29  E0 AF 5B 82  42 10 93 A5  2D 65 75 75   .ªI)à¯[.B..¥-euu
C0 F6 73 2D  65 B1 1F 1D  6B 56 48 F1  ED 65 80 74   Àös-e±..kVHñíe.t
3A 49 EF A5  0C DE C6 FD  C4 9B F0 4B  2F 76 A7 F8   :Iï¥.ÞÆýÄ.ðK/v§ø
75 B0 45 B3  31 03 CC F9  11 F3 7C 58  31 78 41 CB   u°E³1.Ìù.ó|X1xAË
7A 4E E9 27  2B E8 30 29  70 0B 0E 4E  0A 64 FF B8   zNé'+è0)p..N.dÿ¸
B6 A5 A1 02  4B 64 82 6A  F2 8A 27 FA  70 62 DC D6   ¶¥¡.Kd.jò.'úpbÜÖ
E0 70 81 B8  C7 49 26 4D  01 12 FF 5F  FB 3D 10 B6   àp.¸ÇI&M..ÿ_û=.¶
62 BD 60 83  6D A7 31 D3  C0 E1 FB 74  05 DC 5B A1   b½`.m§1ÓÀáût.Ü[¡
7B C1 50 1E  9E 7A D7 BD  F2 17 9C 08  48 22 29 67   {ÁP..z×½ò...H")g
4A EB 6E 4A  95 4B AD D0  F3 DB 1A 93  5A F7 F6 16   JënJ.K.ÐóÛ..Z÷ö.
6A A2 56 54  5B 7F 29 46  C1 C4 81 29  1F 7C CA A2   j¢VT[.)FÁÄ.).|Ê¢
54 11 00 83  D9 25 29 CA  39 51 08 E4  A3 E6 6D 0C   T...Ù%)Ê9Q.ä£æm.
7F 77 45 D0  BE 89 C9 2C  63 74 9D 79  67 63 2D EE   .wEÐ¾.É,ct.ygc-î
0E 69 9A 4B  77 F1 0B 75  EE 87 79 2E  E0 57 9F D9   .i.Kwñ.uî.y.àW.Ù
7E 31 D8 66  32 58 3D FF  3B 2C 14 9F  56 1B 83 24   ~1Øf2X=ÿ;,..V..$
3E F7 70 A9  57 60 33 A0  0E 45 CB 3F  84 96 2D 9B   >÷p©W`3 .EË?..-.
26 44 0D 30  43 55 77 38  76 B9 F0 09  A7 3A 8C D4   &D.0CUw8v¹ð.§:.Ô
49 0A A6 6A  9C 11 22 B2  74 C6 8A FC  C8 9A EE 85   I.¦j.."²tÆ.üÈ.î.
7B 0D 64 BB  87 63 7E 07  25 03 DD 41  41 41 41 41   {.d».c~.%.ÝAAAAA
41 41 41 41  0D 0A 41 41  41 41 41 41  41 41 41 41   AAAA..AAAAAAAAAA
```

Success! Symmetric Encryption Used!



```
00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
54 69 6D 65  4C 6F 63 6B  2E 56 43 68  61 6C 6C 65  TimeLock.VChalle
6E 67 65 2E  56 31 2E 35  2E 50 72 69  76 61 74 65  nge.V1.5.Private
4B 65 79 52  65 77 61 72  64 2E 74 78  74 00 59 6F  KeyReward.txt.Yo
75 20 68 61  76 65 20 73  75 63 63 65  73 73 66 75  u have successfu
6C 6C 79 20  63 6F 6D 70  6C 65 74 65  64 20 74 68  lly completed th
65 20 54 69  6D 65 4C 6F  63 6B 20 56  31 2E 35 20  e TimeLock V1.5 
63 68 61 6C  6C 65 6E 67  65 2E 0D 0A  0D 0A 49 27  challenge.....I'
6D 20 64 79  69 6E 67 20  74 6F 20 6B  6E 6F 77 20  m dying to know 
68 6F 77 20  79 6F 75 20  64 69 64 20  69 74 2E 0D  how you did it..
```

Loot #4

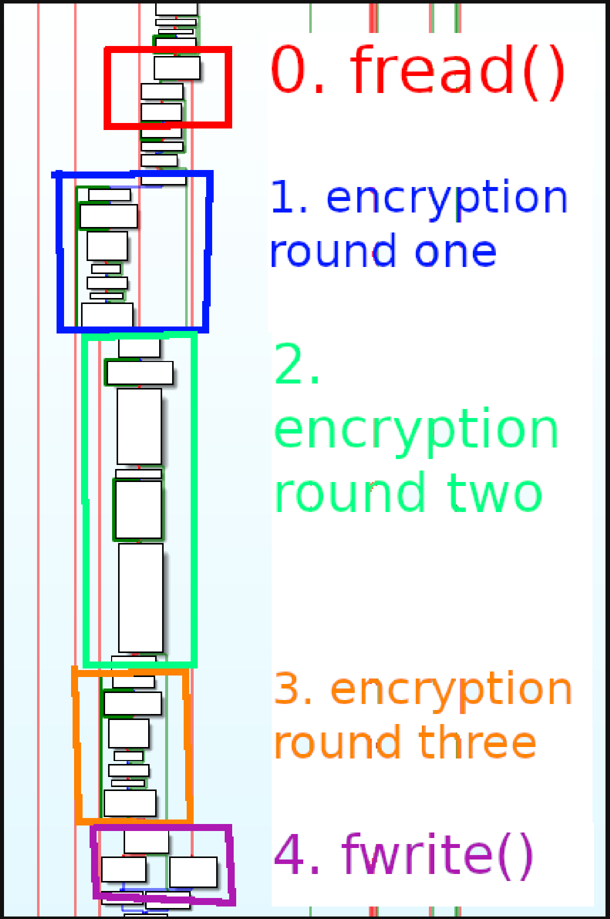


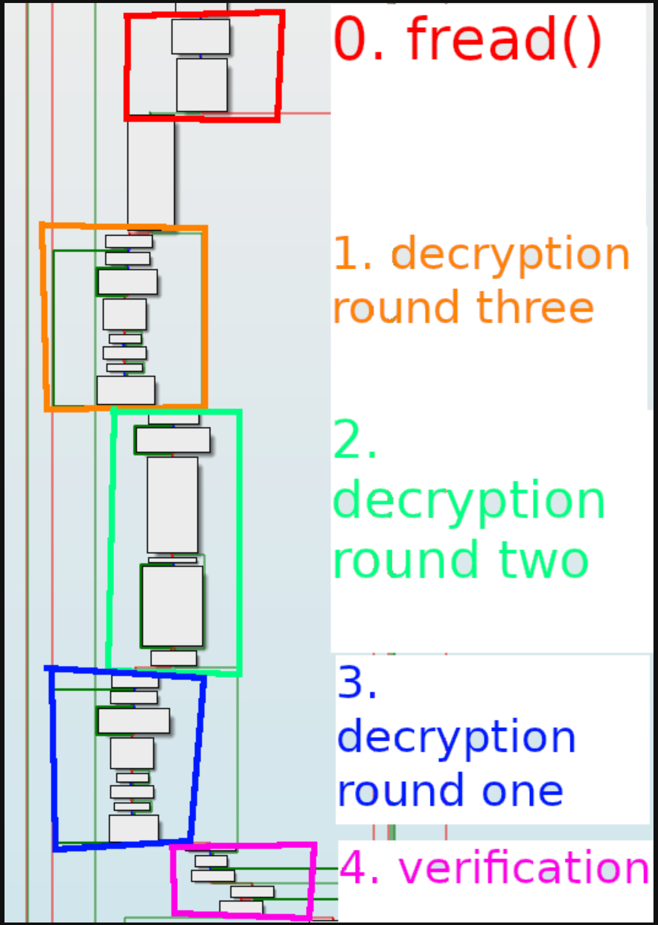
TimeLock.VChallenge.V1.5.PrivateKeyReward - Notepad

File Edit Format View Help

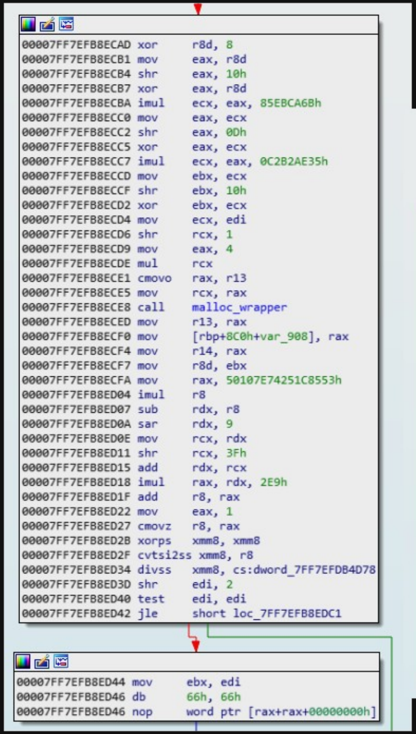
```
You have successfully completed the TimeLock V1

I'm dying to know how you did it.

Please contact me via: https://www.algomachines

I will happily send you at least 0.02 BTC for a


TimeLock 1.5 challenge reward public address:  3GBxNQt9TcCJyhQkzAvYTpY97Bxj39LZXL
TimeLock 1.5 challenge reward private address: Kyb2fewqnFMS3mFD5CdBea4HGfdVW3DYbfKnyZi2YpFi5rSV2ByD
```

Encryption and Decryption



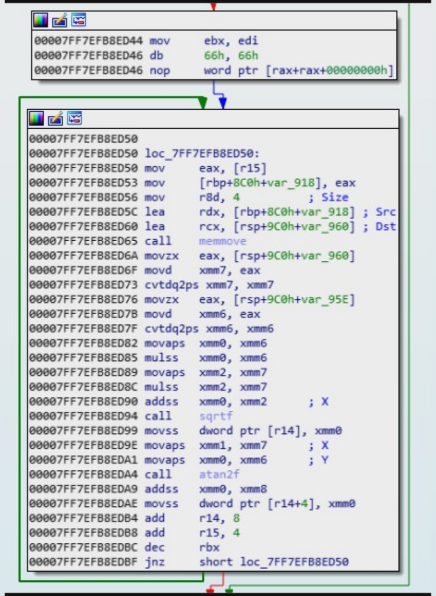


Encryption Round Two



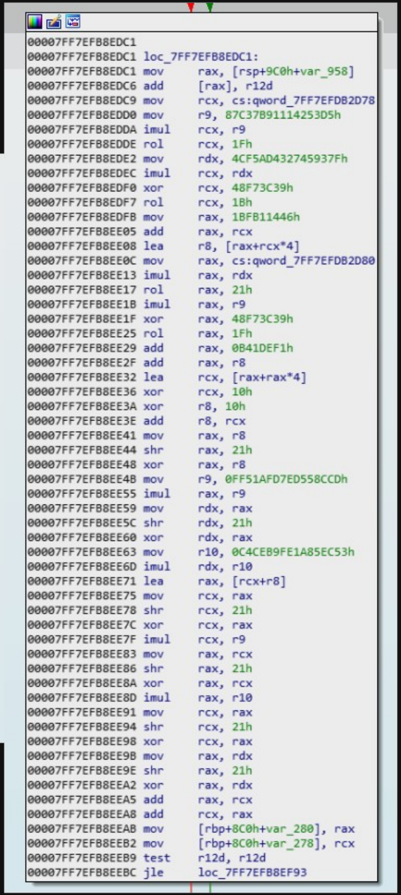
```
00007FF7EFB8ECAD xor     r8d, 8
00007FF7EFB8ECB1 mov     eax, r8d
00007FF7EFB8ECB4 shr     eax, 10h
00007FF7EFB8ECB7 xor     eax, r8d
00007FF7EFB8ECBA imul    ecx, eax, 85EBCA6Bh
00007FF7EFB8ECC0 mov     eax, ecx
00007FF7EFB8ECC2 shr     eax, 0Dh
00007FF7EFB8ECC5 xor     eax, ecx
00007FF7EFB8ECC7 imul    ecx, eax, 0C2B2AE35h
00007FF7EFB8ECCD mov     ebx, ecx
00007FF7EFB8ECCF shr     ebx, 10h
00007FF7EFB8ECD2 xor     ebx, ecx
00007FF7EFB8ECD4 mov     ecx, edi
00007FF7EFB8ECD6 shr     rcx, 1
00007FF7EFB8ECD9 mov     eax, 4
00007FF7EFB8ECDE mul     rcx
00007FF7EFB8ECE1 cmovo   rax, r13
00007FF7EFB8ECE5 mov     rcx, rax
00007FF7EFB8ECE8 call    malloc_wrapper
00007FF7EFB8ECED mov     r13, rax
00007FF7EFB8ECF0 mov     [rbp+8C0h+var_908], rax
00007FF7EFB8ECF4 mov     r14, rax
00007FF7EFB8ECF7 mov     r8d, ebx
00007FF7EFB8ECFA mov     rax, 50107E74251C8553h
00007FF7EFB8ED04 imul    r8
00007FF7EFB8ED07 sub     rdx, r8
00007FF7EFB8ED0A sar     rdx, 9
00007FF7EFB8ED0E mov     rcx, rdx
00007FF7EFB8ED11 shr     rcx, 3Fh
00007FF7EFB8ED15 add     rdx, rcx
00007FF7EFB8ED18 imul    rax, rdx, 2E9h
00007FF7EFB8ED1F add     r8, rax
00007FF7EFB8ED22 mov     eax, 1
00007FF7EFB8ED27 cmovz   r8, rax
00007FF7EFB8ED2B xorps   xmm8, xmm8
00007FF7EFB8ED2F cvtsi2ss xmm8, r8
00007FF7EFB8ED34 divss   xmm8, cs:dword_7FF7EFDB4D78
00007FF7EFB8ED3D shr     edi, 2
00007FF7EFB8ED40 test    edi, edi
00007FF7EFB8ED42 jle     short loc_7FF7EFB8EDC1
```

```
00007FF7EFB8ED44 mov     ebx, edi
00007FF7EFB8ED46 db      66h, 66h
00007FF7EFB8ED46 nop     word ptr [rax+rax+00000000h]
```



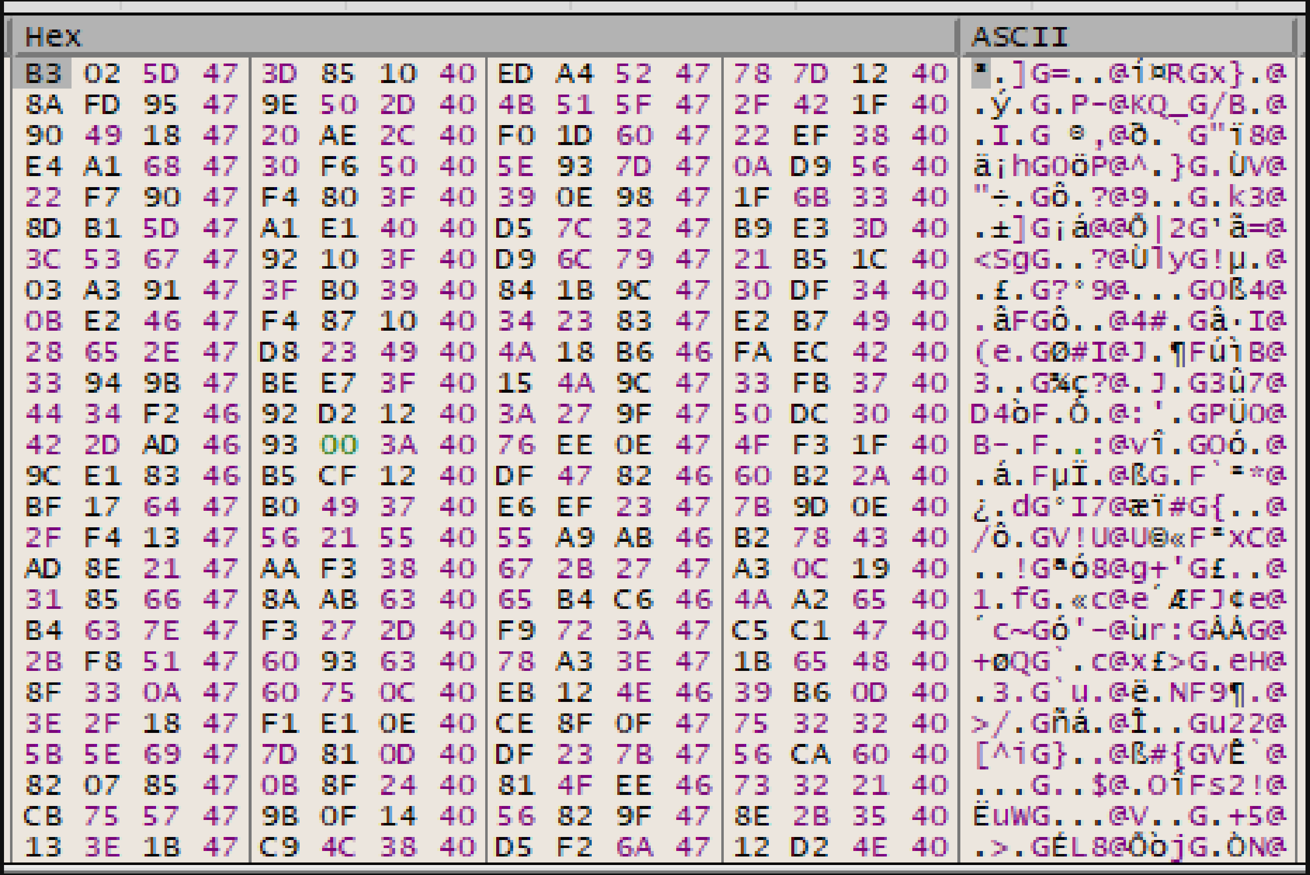
```
00007FF7EFB8ED44 mov     ebx, edi
00007FF7EFB8ED46 db      66h, 66h
00007FF7EFB8ED46 nop     word ptr [rax+rax+00000000h]
```

```
00007FF7EFB8ED50
00007FF7EFB8ED50 loc_7FF7EFB8ED50:
00007FF7EFB8ED50 mov     eax, [r15]
00007FF7EFB8ED53 mov     [rbp+8C0h+var_918], eax
00007FF7EFB8ED56 mov     r8d, 4          ; Size
00007FF7EFB8ED5C lea     rdx, [rbp+8C0h+var_918] ; Src
00007FF7EFB8ED60 lea     rcx, [rsp+9C0h+var_960] ; Dst
00007FF7EFB8ED65 call    memmove
00007FF7EFB8ED6A movzx   eax, [rsp+9C0h+var_960]
00007FF7EFB8ED6F movd    xmm7, eax
00007FF7EFB8ED73 cvtdq2ps xmm7, xmm7
00007FF7EFB8ED76 movzx   eax, [rsp+9C0h+var_95E]
00007FF7EFB8ED7B movd    xmm6, eax
00007FF7EFB8ED7F cvtdq2ps xmm6, xmm6
00007FF7EFB8ED82 movaps  xmm0, xmm6
00007FF7EFB8ED85 mulss   xmm0, xmm6
00007FF7EFB8ED89 movaps  xmm2, xmm7
00007FF7EFB8ED8C mulss   xmm2, xmm7
00007FF7EFB8ED90 addss   xmm0, xmm2      ; X
00007FF7EFB8ED94 call    sqrtf
00007FF7EFB8ED99 movss   dword ptr [r14], xmm0
00007FF7EFB8ED9E movaps  xmm1, xmm7      ; X
00007FF7EFB8EDA1 movaps  xmm0, xmm6      ; Y
00007FF7EFB8EDA4 call    atan2f
00007FF7EFB8EDA9 addss   xmm0, xmm8
00007FF7EFB8EDAE movss   dword ptr [r14+4], xmm0
00007FF7EFB8EDB4 add     r14, 8
00007FF7EFB8EDB8 add     r15, 4
00007FF7EFB8EDBC dec     rbx
00007FF7EFB8EDBF jnz     short loc_7FF7EFB8ED50
```



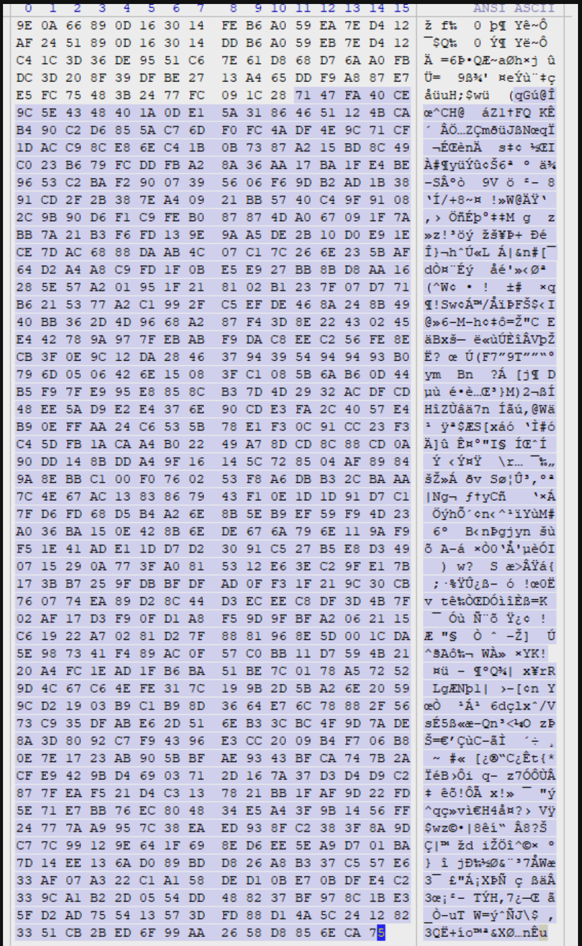
```
00007FF7EFB8EDC1
00007FF7EFB8EDC1 loc_7FF7EFB8EDC1:
00007FF7EFB8EDC1 mov     rax, [rsp+9C0h+var_958]
00007FF7EFB8EDC6 add     [rax], r12d
00007FF7EFB8EDC9 mov     rcx, cs:qword_7FF7EFDB2D78
00007FF7EFB8EDD0 mov     r9, 87C37B91114253D5h
00007FF7EFB8EDDA imul    rcx, r9
00007FF7EFB8EDDE rol     rcx, 1Fh
00007FF7EFB8EDE2 mov     rdx, 4CF5AD432745937Fh
00007FF7EFB8EDEC imul    rcx, rdx
00007FF7EFB8EDF0 xor     rcx, 48F73C39h
00007FF7EFB8EDF7 rol     rcx, 1Bh
00007FF7EFB8EDFB mov     rax, 1BFB11446h
00007FF7EFB8EE05 add     rax, rcx
00007FF7EFB8EE08 lea     r8, [rax+rcx*4]
00007FF7EFB8EE0C mov     rax, cs:qword_7FF7EFDB2D80
00007FF7EFB8EE13 imul    rax, rdx
00007FF7EFB8EE17 rol     rax, 21h
00007FF7EFB8EE1B imul    rax, r9
00007FF7EFB8EE1F xor     rax, 48F73C39h
00007FF7EFB8EE25 rol     rax, 1Fh
00007FF7EFB8EE29 add     rax, 0B41DEF1h
00007FF7EFB8EE2F add     rax, r8
00007FF7EFB8EE32 lea     rcx, [rax+rax*4]
00007FF7EFB8EE36 xor     rcx, 10h
00007FF7EFB8EE3A xor     r8, 10h
00007FF7EFB8EE3E add     r8, rcx
00007FF7EFB8EE41 mov     rax, r8
00007FF7EFB8EE44 shr     rax, 21h
00007FF7EFB8EE48 xor     rax, r8
00007FF7EFB8EE4B mov     r9, 0FF51AFD7ED558CCDh
00007FF7EFB8EE55 imul    rax, r9
00007FF7EFB8EE59 mov     rdx, rax
00007FF7EFB8EE5C shr     rdx, 21h
00007FF7EFB8EE60 xor     rdx, rax
00007FF7EFB8EE63 mov     r10, 0C4CEB9FE1A85EC53h
00007FF7EFB8EE6D imul    rdx, r10
00007FF7EFB8EE71 lea     rax, [rcx+r8]
00007FF7EFB8EE75 mov     rcx, rax
00007FF7EFB8EE78 shr     rcx, 21h
00007FF7EFB8EE7C xor     rcx, rax
00007FF7EFB8EE7F imul    rcx, r9
00007FF7EFB8EE83 mov     rax, rcx
00007FF7EFB8EE86 shr     rax, 21h
00007FF7EFB8EE8A xor     rax, rcx
00007FF7EFB8EE8D imul    rax, r10
00007FF7EFB8EE91 mov     rcx, rax
00007FF7EFB8EE94 shr     rcx, 21h
00007FF7EFB8EE98 xor     rcx, rax
00007FF7EFB8EE9B mov     rax, rdx
00007FF7EFB8EE9E shr     rax, 21h
00007FF7EFB8EEA2 xor     rax, rdx
00007FF7EFB8EEA5 add     rax, rcx
00007FF7EFB8EEA8 add     rcx, rax
00007FF7EFB8EEAB mov     [rbp+8C0h+var_280], rax
00007FF7EFB8EEB2 mov     [rbp+8C0h+var_278], rcx
00007FF7EFB8EEB9 test    r12d, r12d
00007FF7EFB8EEBC jle     loc_7FF7EFB8EF93
```

Encryption Round Two is Not Symmetric

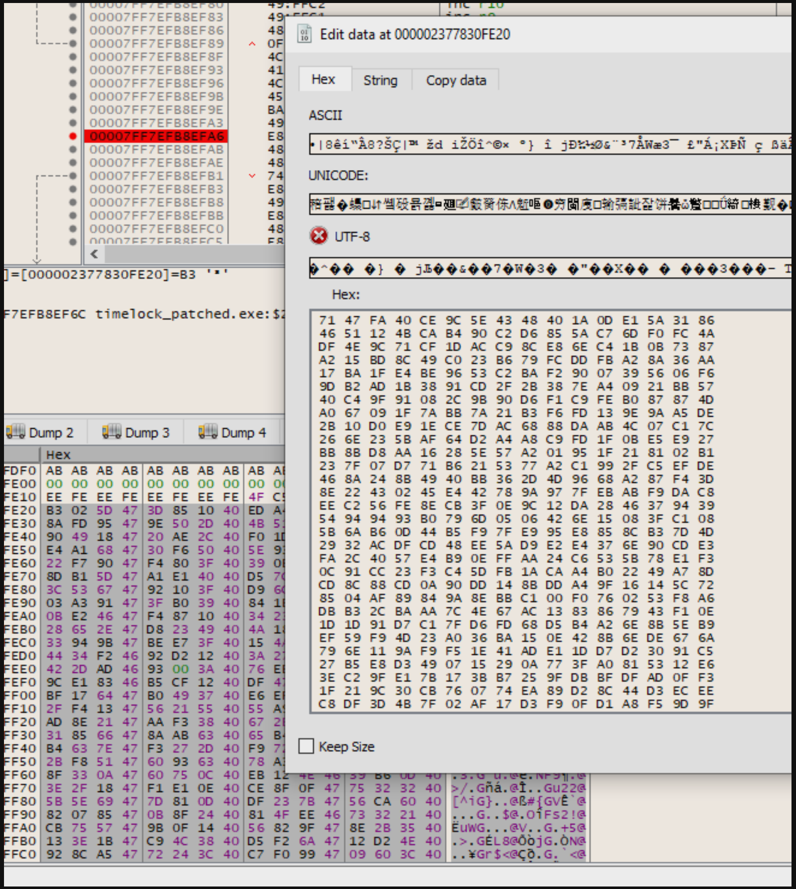


```
Hex                                                                  ASCII
B3 02 5D 47  3D 85 10 40  ED A4 52 47  78 7D 12 40  ■.]G=..@í¤RGx}.@
8A FD 95 47  9E 50 2D 40  4B 51 5F 47  2F 42 1F 40  .ý.G.P-@KQ_G/B.@
90 49 18 47  20 AE 2C 40  F0 1D 60 47  22 EF 38 40  .I.G ®,@ð.`G"ï8@
E4 A1 68 47  30 F6 50 40  5E 93 7D 47  0A D9 56 40  ä¡hG0öP@^.}G.ÙV@
22 F7 90 47  F4 80 3F 40  39 0E 98 47  1F 6B 33 40  "÷.Gô.?@9..G.k3@
8D B1 5D 47  A1 E1 40 40  D5 7C 32 47  B9 E3 3D 40  .±]G¡á@@Õ|2G¹ã=@
3C 53 67 47  92 10 3F 40  D9 6C 79 47  21 B5 1C 40  <SgG..?@ÙlyG!µ.@
03 A3 91 47  3F B0 39 40  84 1B 9C 47  30 DF 34 40  .£.G?°9@...G0ß4@
0B E2 46 47  F4 87 10 40  34 23 83 47  E2 B7 49 40  .âFGô..@4#.Gâ·I@
28 65 2E 47  D8 23 49 40  4A 18 B6 46  FA EC 42 40  (e.GØ#I@J.¶FúìB@
33 94 9B 47  BE E7 3F 40  15 4A 9C 47  33 FB 37 40  3..G¾ç?@.J.G3û7@
44 34 F2 46  92 D2 12 40  3A 27 9F 47  50 DC 30 40  D4òF.Ò.@:'.GPÜ0@
42 2D AD 46  93 00 3A 40  76 EE 0E 47  4F F3 1F 40  B-.F..:@vî.GOó.@
9C E1 83 46  B5 CF 12 40  DF 47 82 46  60 B2 2A 40  .á.FµÏ.@ßG.F`²*@
BF 17 64 47  B0 49 37 40  E6 EF 23 47  7B 9D 0E 40  ¿.dG°I7@æï#G{..@
2F F4 13 47  56 21 55 40  55 A9 AB 46  B2 78 43 40  /ô.GV!U@U©«F²xC@
AD 8E 21 47  AA F3 38 40  67 2B 27 47  A3 0C 19 40  ..!GªóS@g+'G£..@
31 85 66 47  8A AB 63 40  65 B4 C6 46  4A A2 65 40  1.fG.«c@e´ÆFJ¢e@
B4 63 7E 47  F3 27 2D 40  F9 72 3A 47  C5 C1 47 40  ´c~Gó'-@ùr:GÅÁG@
2B F8 51 47  60 93 63 40  78 A3 3E 47  1B 65 48 40  +øQG`.c@x£>G.eH@
8F 33 0A 47  60 75 0C 40  EB 12 4E 46  39 B6 0D 40  .3.G`u.@ë.NF9¶.@
3E 2F 18 47  F1 E1 0E 40  CE 8F 0F 47  75 32 32 40  >/.Gñá.@Î..Gu22@
5B 5E 69 47  7D 81 0D 40  DF 23 7B 47  56 CA 60 40  [^iG}..@ß#{GVÊ`@
82 07 85 47  0B 8F 24 40  81 4F EE 46  73 32 21 40  ...G..$@.OîFs2!@
CB 75 57 47  9B 0F 14 40  56 82 9F 47  8E 2B 35 40  ËuWG...@V..G.+5@
13 3E 1B 47  C9 4C 38 40  D5 F2 6A 47  12 D2 4E 40  .>.GÉL8@ÕòjG.ÒN@
```

Extract Ciphertext, Third Round of Encryption



```
 0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   ANSI ASCII
9E 0A 66 89 0D 16 30 14  FE B6 A0 59 EA 7E D4 12   ž f‰  0 þ¶ Yê~Ô
AF 24 51 89 0D 16 30 14  DD B6 A0 59 EB 7E D4 12   ¯$Q‰  0 Ý¶ Yë~Ô
C4 1C 3D 36 DE 95 51 C6  7E 61 D8 68 D7 6A A0 FB   Ä =6Þ•QÆ~aØh×j û
DC 3D 20 8F 39 DF BE 27  13 A4 65 DD F9 A8 87 E7   Ü=  9ß¾' ¤eÝù¨‡ç
E5 FC 75 48 3B 24 77 FC  09 1C 28 71 47 FA 40 CE   åüuH;$wü  (qGú@Î
9C 5E 43 48 40 1A 0D E1  5A 31 86 46 51 12 4B CA   œ^CH@  áZ1†FQ KÊ
B4 90 C2 D6 85 5A C7 6D  F0 FC 4A DF 4E 9C 71 CF   ´ ÂÖ…ZÇmðüJßNœqÏ
1D AC C9 8C E8 6E C4 1B  0B 73 87 A2 15 BD 8C 49    ¬ÉŒènÄ  s‡¢ ½ŒI
C0 23 B6 79 FC DD FB A2  8A 36 AA 17 BA 1F E4 BE   À#¶yüÝû¢Š6ª º ä¾
96 53 C2 BA F2 90 07 39  56 06 F6 9D B2 AD 1B 38   –SÂºò  9V ö ² 8
91 CD 2F 2B 38 7E A4 09  21 BB 57 40 C4 9F 91 08   'Í/+8~¤ !»W@ÄŸ'
2C 9B 90 D6 F1 C9 FE B0  87 87 4D A0 67 09 1F 7A   ,› ÖñÉþ°‡‡M g  z
BB 7A 21 B3 F6 FD 13 9E  9A A5 DE 2B 10 D0 E9 1E   »z!³öý žš¥Þ+ Ðé
CE 7D AC 68 88 DA AB 4C  07 C1 7C 26 6E 23 5B AF   Î}¬hˆÚ«L Á|&n#[¯
64 D2 A4 A8 C9 FD 1F 0B  E5 E9 27 BB 8B D8 AA 16   dÒ¤¨Éý  åé'»‹Øª
28 5E 57 A2 01 95 1F 21  81 02 B1 23 7F 07 D7 71   (^W¢ • !  ±#  ×q
B6 21 53 77 A2 C1 99 2F  C5 EF DE 46 8A 24 8B 49   ¶!Sw¢Á™/ÅïÞFŠ$‹I
40 BB 36 2D 4D 96 68 A2  87 F4 3D 8E 22 43 02 45   @»6-M–h¢‡ô=Ž"C E
E4 42 78 9A 97 7F EB AB  F9 DA C8 EE C2 56 FE 8E   äBxš— ë«ùÚÈîÂVþŽ
CB 3F 0E 9C 12 DA 28 46  37 94 39 54 94 94 93 B0   Ë? œ Ú(F7”9T”””°
79 6D 05 06 42 6E 15 08  3F C1 08 5B 6A B6 0D 44   ym  Bn  ?Á [j¶ D
B5 F9 7F E9 95 E8 85 8C  B3 7D 4D 29 32 AC DF CD   µù é•è…Œ³}M)2¬ßÍ
48 EE 5A D9 E2 E4 37 6E  90 CD E3 FA 2C 40 57 E4   HîZÙâä7n Íãú,@Wä
B9 0E FF AA 24 C6 53 5B  78 E1 F3 0C 91 CC 23 F3   ¹ ÿª$ÆS[xáó 'Ì#ó
C4 5D FB 1A CA A4 B0 22  49 A7 8D CD 8C 88 CD 0A   Ä]û Ê¤°"I§ ÍŒˆÍ
90 DD 14 8B DD A4 9F 16  14 5C 72 85 04 AF 89 84    Ý ‹Ý¤Ÿ  \r… ¯‰„
9A 8E BB C1 00 F0 76 02  53 F8 A6 DB B3 2C BA AA   šŽ»Á ðv Sø¦Û³,ºª
7C 4E 67 AC 13 83 86 79  43 F1 0E 1D 1D 91 D7 C1   |Ng¬ ƒ†yCñ   '×Á
7F D6 FD 68 D5 B4 A2 6E  8B 5E B9 EF 59 F9 4D 23    ÖýhÕ´¢n‹^¹ïYùM#
A0 36 BA 15 0E 42 8B 6E  DE 67 6A 79 6E 11 9A F9    6º  B‹nÞgjyn šù
F5 1E 41 AD E1 1D D7 D2  30 91 C5 27 B5 E8 D3 49   õ Aá ×Ò0'Å'µèÓI
07 15 29 0A 77 3F A0 81  53 12 E6 3E C2 9F E1 7B     ) w?  S æ>ÂŸá{
17 3B B7 25 9F DB BF DF  AD 0F F3 1F 21 9C 30 CB    ;·%ŸÛ¿ß ó !œ0Ë
76 07 74 EA 89 D2 8C 44  D3 EC EE C8 DF 3D 4B 7F   v tê‰ÒŒDÓìîÈß=K
02 AF 17 D3 F9 0F D1 A8  F5 9D 9F BF A2 06 21 15    ¯ Óù Ñ¨õ Ÿ¿¢ !
C6 19 22 A7 02 81 D2 7F  88 81 96 8E 5D 00 1C DA   Æ "§  Ò ˆ –Ž]  Ú
5E 98 73 41 F4 89 AC 0F  57 C0 BB 11 D7 59 4B 21   ^˜sAô‰¬ WÀ» ×YK!
20 A4 FC 1E AD 1F B6 BA  51 BE 7C 01 78 A5 72 52    ¤ü  ¶ºQ¾| x¥rR
9D 4C 67 C6 4E FE 31 7C  19 9B 2D 5B A2 6E 20 59    LgÆNþ1| ›-[¢n Y
9C D2 19 03 B9 C1 B9 8D  36 64 E7 6C 78 88 2F 56   œÒ  ¹Á¹ 6dçlxˆ/V
73 C9 35 DF AB E6 2D 51  6E B3 3C BC 4F 9D 7A DE   sÉ5ß«æ-Qn³<¼O zÞ
8A 3D 80 92 C7 F9 43 96  E3 CC 20 09 B4 F7 06 B8   Š=€'ÇùC–ãÌ  ´÷ ¸
0E 7E 17 23 AB 90 5B BF  AE 93 43 BF CA 74 7B 2A    ~ #« [¿®"C¿Êt{*
CF E9 42 9B D4 69 03 71  2D 16 7A 37 D3 D4 D9 C2   ÏéB›Ôi q- z7ÓÔÙÂ
87 7F EA F5 21 D4 C3 13  78 21 BB 1F AF 9D 22 FD   ‡ êõ!ÔÃ x!» ¯ "ý
5E 71 E7 BB 76 EC 80 48  34 E5 A4 3F 9B 14 56 FF   ^qç»vì€H4å¤?› Vÿ
24 77 7A A9 95 7C 38 EA  ED 93 8F C2 38 3F 8A 9D   $wz©•|8êí" Â8?Š
C7 7C 99 12 9E 64 1F 69  8E D6 EE 5E A9 D7 01 BA   Ç|™ žd iŽÖî^©× º
7D 14 EE 13 6A D0 89 BD  D8 26 A8 B3 37 C5 57 E6   } î jÐ‰½Ø&¨³7ÅWæ
33 AF 07 A3 22 C1 A1 58  DE D1 0B E7 0B DF E4 C2   3¯ £"Á¡XÞÑ ç ßäÂ
33 9C A1 B2 2D 05 54 DD  48 82 37 BF 97 8C 1B E3   3œ¡²- TÝH‚7¿—Œ ã
5F D2 AD 75 54 13 57 3D  FD 88 D1 4A 5C 24 12 82   _ÒuT W=ýˆÑJ\$ ‚
33 51 CB 2B ED 6F 99 AA  26 58 D8 85 6E CA 75      3QË+íо™ª&XØ…nÊu
```



```
00007FF7EFB8EF83   49:FFC1
00007FF7EFB8EF86   48
00007FF7EFB8EF89   0F
00007FF7EFB8EF8F   4C
00007FF7EFB8EF93   41
00007FF7EFB8EF96   4C
00007FF7EFB8EF9B   45
00007FF7EFB8EF9E   BA
00007FF7EFB8EFA3   49
00007FF7EFB8EFA6   E8
00007FF7EFB8EFAB   48
00007FF7EFB8EFAE   48
00007FF7EFB8EFB1   74
00007FF7EFB8EFB3   E8
00007FF7EFB8EFB8   49
00007FF7EFB8EFBB   E8
00007FF7EFB8EFC0   48

]=[000002377830FE20]=B3 '³'

F7EFB8EF6C timelock_patched.exe:$2
```

Edit data at 000002377830FE20

Hex | String | Copy data

ASCII

```
•|8êí"Â8?ŠÇ|™ žd iŽÖî^©× º} î jÐ‰½Ø&¨³7ÅWæ3¯ £"Á¡XÞÑ ç ßäÂ
```

UNICODE:

```
[illegible]
```

UTF-8

```
�^�� �} � jЉ��&��7�W�3� �"��X�� � ���3���- T
```

Hex:

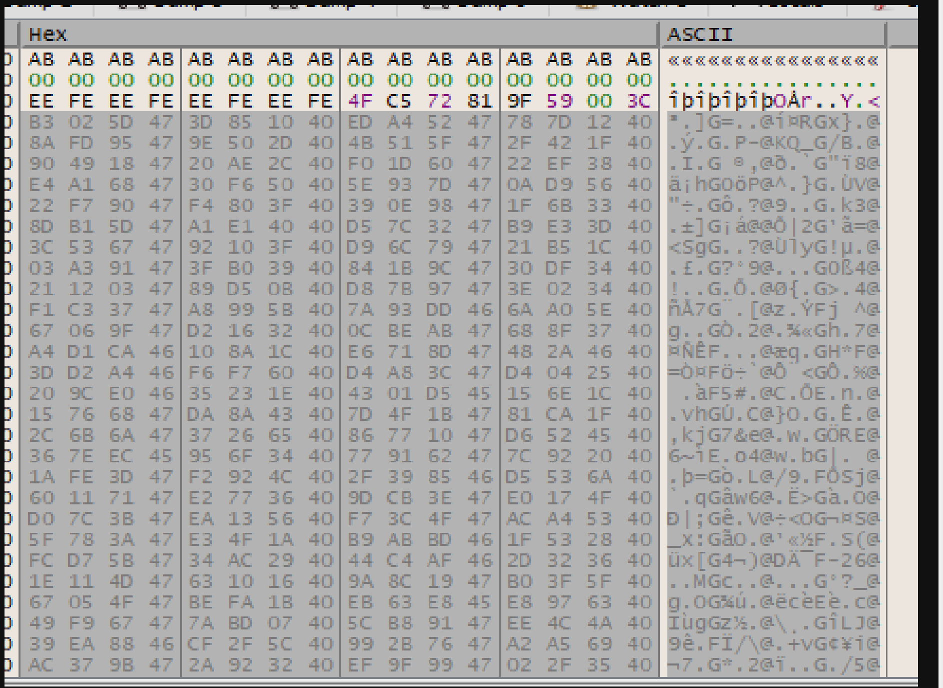
```
71 47 FA 40 CE 9C 5E 43 48 40 1A 0D E1 5A 31 86
46 51 12 4B CA B4 90 C2 D6 85 5A C7 6D F0 FC 4A
DF 4E 9C 71 CF 1D AC C9 8C E8 6E C4 1B 0B 73 87
A2 15 BD 8C 49 C0 23 B6 79 FC DD FB A2 8A 36 AA
17 BA 1F E4 BE 96 53 C2 BA F2 90 07 39 56 06 F6
9D B2 AD 1B 38 91 CD 2F 2B 38 7E A4 09 21 BB 57
40 C4 9F 91 08 2C 9B 90 D6 F1 C9 FE B0 87 87 4D
A0 67 09 1F 7A BB 7A 21 B3 F6 FD 13 9E 9A A5 DE
2B 10 D0 E9 1E CE 7D AC 68 88 DA AB 4C 07 C1 7C
26 6E 23 5B AF 64 D2 A4 A8 C9 FD 1F 0B E5 E9 27
BB 8B D8 AA 16 28 5E 57 A2 01 95 1F 21 81 02 B1
23 7F 07 D7 71 B6 21 53 77 A2 C1 99 2F C5 EF DE
46 8A 24 8B 49 40 BB 36 2D 4D 96 68 A2 87 F4 3D
8E 22 43 02 45 E4 42 78 9A 97 7F EB AB F9 DA C8
EE C2 56 FE 8E CB 3F 0E 9C 12 DA 28 46 37 94 39
54 94 94 93 B0 79 6D 05 06 42 6E 15 08 3F C1 08
5B 6A B6 0D 44 B5 F9 7F E9 95 E8 85 8C B3 7D 4D
29 32 AC DF CD 48 EE 5A D9 E2 E4 37 6E 90 CD E3
FA 2C 40 57 E4 B9 0E FF AA 24 C6 53 5B 78 E1 F3
0C 91 CC 23 F3 C4 5D FB 1A CA A4 B0 22 49 A7 8D
CD 8C 88 CD 0A 90 DD 14 8B DD A4 9F 16 14 5C 72
85 04 AF 89 84 9A 8E BB C1 00 F0 76 02 53 F8 A6
DB B3 2C BA AA 7C 4E 67 AC 13 83 86 79 43 F1 0E
1D 1D 91 D7 C1 7F D6 FD 68 D5 B4 A2 6E 8B 5E B9
EF 59 F9 4D 23 A0 36 BA 15 0E 42 8B 6E DE 67 6A
79 6E 11 9A F9 F5 1E 41 AD E1 1D D7 D2 30 91 C5
27 B5 E8 D3 49 07 15 29 0A 77 3F A0 81 53 12 E6
3E C2 9F E1 7B 17 3B B7 25 9F DB BF DF AD 0F F3
1F 21 9C 30 CB 76 07 74 EA 89 D2 8C 44 D3 EC EE
C8 DF 3D 4B 7F 02 AF 17 D3 F9 0F D1 A8 F5 9D 9F
```

☐ Keep Size

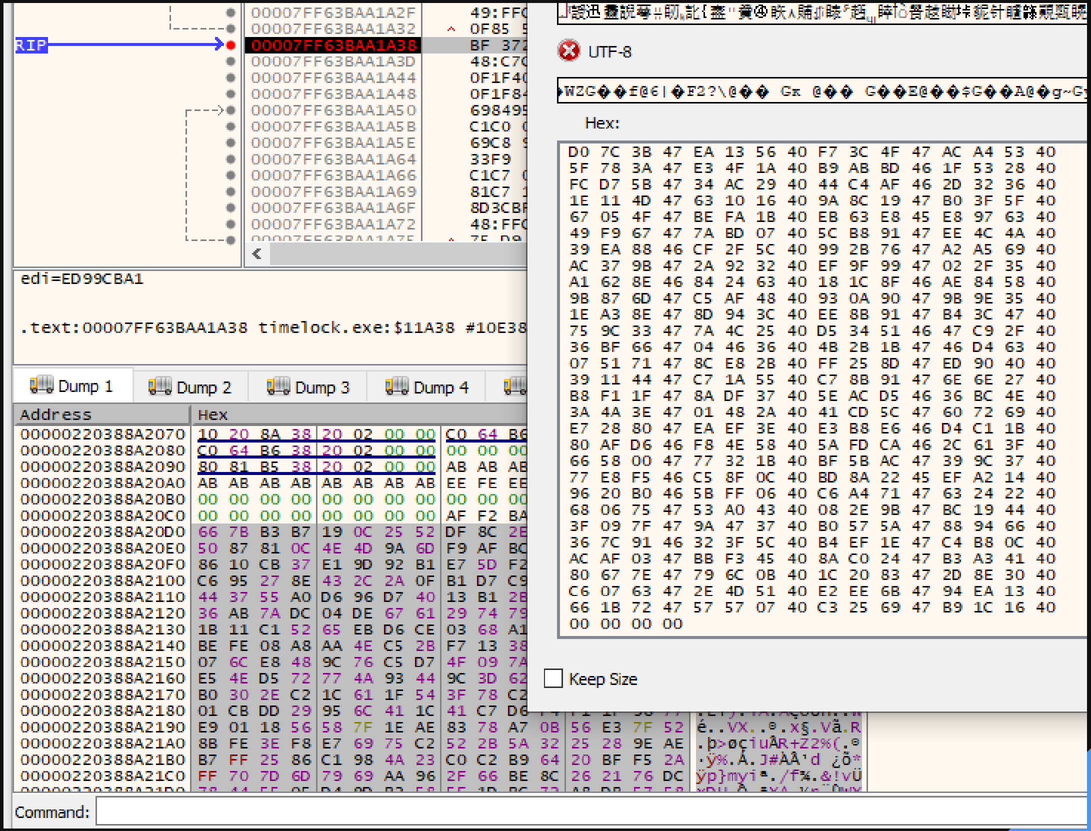
Dump 2 | Dump 3 | Dump 4

```
      Hex
FDF0  AB AB AB AB  AB AB AB AB  AB
FE00  00 00 00 00  00 00 00 00  00
FE10  EE FE EE FE  EE FE EE FE  4F
FE20  B3 02 5D 47  3D 85 10 40  ED
FE30  8A FD 95 47  9E 50 2D 40  4B
FE40  90 49 18 47  20 AE 2C 40  F0
FE50  E4 A1 68 47  30 F6 50 40  5E
FE60  22 F7 90 47  F4 80 3F 40  39
FE70  8D B1 5D 47  A1 E1 40 40  D5
FE80  3C 53 67 47  92 10 3F 40  D9
FE90  03 A3 91 47  3F B0 39 40  84
FEA0  0B E2 46 47  F4 87 10 40  34
FEB0  28 65 2E 47  D8 23 49 40  4A
FEC0  33 94 9B 47  BE E7 3F 40  15
FED0  44 34 F2 46  92 D2 12 40  3A
FEE0  42 2D AD 46  93 00 3A 40  76
FEF0  9C E1 83 46  B5 CF 12 40  DF
FF00  BF 17 64 47  B0 49 37 40  E6
FF10  2F F4 13 47  56 21 55 40  55
FF20  AD 8E 21 47  AA F3 38 40  67
FF30  31 85 66 47  8A AB 63 40  65
FF40  B4 63 7E 47  F3 27 2D 40  F9
FF50  2B F8 51 47  60 93 63 40  78
FF60  8F 33 0A 47  60 75 0C 40  EB 12
FF70  3E 2F 18 47  F1 E1 0E 40  CE 8F 0F 47  75 32 32 40  >/.Gñá.@Î..Gu22@
FF80  5B 5E 69 47  7D 81 0D 40  DF 23 7B 47  56 CA 60 40  [^iG}..@ß#{GVÊ`@
FF90  82 07 85 47  0B 8F 24 40  81 4F EE 46  73 32 21 40  ...G..$@.OîFs2!@
FFA0  CB 75 57 47  9B 0F 14 40  56 82 9F 47  8E 2B 35 40  ËuWG...@V..G.+5@
FFB0  13 3E 1B 47  C9 4C 38 40  D5 F2 6A 47  12 D2 4E 40  .>.GÉL8@ÕòjG.ÒN@
FFC0  92 8C A5 47  72 24 3C 40  C7 F0 99 47  09 60 3C 40  ..¥Gr$<@Çð.G.`<@
```

Extract Ciphertext, Second Round Decryption



```
Hex                                                 ASCII
AB AB AB AB  AB AB AB AB  AB AB AB AB  AB AB AB AB  ««««««««««««««««
00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
EE FE EE FE  EE FE EE FE  4F C5 72 81  9F 59 00 3C  îþîþîþîþOÅr..Y.<
B3 02 5D 47  3D 85 10 40  ED A4 52 47  78 7D 12 40  ³.]G=..@í¤RGx}.@
8A FD 95 47  9E 50 2D 40  4B 51 5F 47  2F 42 1F 40  .ý.G.P-@KQ_G/B.@
90 49 18 47  20 AE 2C 40  F0 1D 60 47  22 EF 38 40  .I.G ®,@ð.`G"ï8@
E4 A1 68 47  30 F6 50 40  5E 93 7D 47  0A D9 56 40  ä¡hG0öP@^.}G.ÙV@
22 F7 90 47  F4 80 3F 40  39 0E 98 47  1F 6B 33 40  "÷.Gô.?@9..G.k3@
8D B1 5D 47  A1 E1 40 40  D5 7C 32 47  B9 E3 3D 40  .±]G¡á@@Õ|2G¹ã=@
3C 53 67 47  92 10 3F 40  D9 6C 79 47  21 B5 1C 40  <SgG..?@ÙlyG!µ.@
03 A3 91 47  3F B0 39 40  84 1B 9C 47  30 DF 34 40  .£.G?°9@...G0ß4@
21 12 03 47  89 D5 0B 40  D8 7B 97 47  3E 02 34 40  !..G.Õ.@Ø{.G>.4@
F1 C3 37 47  A8 99 5B 40  7A 93 DD 46  6A A0 5E 40  ñÃ7G¨.[@z.ÝFj ^@
67 06 9F 47  D2 16 32 40  0C BE AB 47  68 8F 37 40  g..GÒ.2@.¾«Gh.7@
A4 D1 CA 46  10 8A 1C 40  E6 71 8D 47  48 2A 46 40  ¤ÑÊF...@æq.GH*F@
3D D2 A4 46  F6 F7 60 40  D4 A8 3C 47  D4 04 25 40  =Ò¤Fö÷`@Ô¨<GÔ.%@
20 9C E0 46  35 23 1E 40  43 01 D5 45  15 6E 1C 40   .àF5#.@C.ÕE.n.@
15 76 68 47  DA 8A 43 40  7D 4F 1B 47  81 CA 1F 40  .vhGÚ.C@}O.G.Ê.@
2C 6B 6A 47  37 26 65 40  86 77 10 47  D6 52 45 40  ,kjG7&e@.w.GÖRE@
36 7E EC 45  95 6F 34 40  77 91 62 47  7C 92 20 40  6~ìE.o4@w.bG|. @
1A FE 3D 47  F2 92 4C 40  2F 39 85 46  D5 53 6A 40  .þ=Gò.L@/9.FÕSj@
60 11 71 47  E2 77 36 40  9D CB 3E 47  E0 17 4F 40  `.qGâw6@.Ë>Gà.O@
D0 7C 3B 47  EA 13 56 40  F7 3C 4F 47  AC A4 53 40  Ð|;Gê.V@÷<OG¬¤S@
5F 78 3A 47  E3 4F 1A 40  B9 AB BD 46  1F 53 28 40  _x:GãO.@¹«½F.S(@
FC D7 5B 47  34 AC 29 40  44 C4 AF 46  2D 32 36 40  ü×[G4¬)@DÄ¯F-26@
1E 11 4D 47  63 10 16 40  9A 8C 19 47  B0 3F 5F 40  ..MGc..@...G°?_@
67 05 4F 47  BE FA 1B 40  EB 63 E8 45  E8 97 63 40  g.OG¾ú.@ëcèEè.c@
49 F9 67 47  7A BD 07 40  5C B8 91 47  EE 4C 4A 40  IùgGz½.@\¸.GîLJ@
39 EA 88 46  CF 2F 5C 40  99 2B 76 47  A2 A5 69 40  9ê.FÏ/\@.+vG¢¥i@
AC 37 9B 47  2A 92 32 40  EF 9F 99 47  02 2F 35 40  ¬7.G*.2@ï..G./5@
```



```
                  00007FF63BAA1A2F    49:FF
                  00007FF63BAA1A32  ^ 0F85 5
RIP ────────────► 00007FF63BAA1A38    BF 372
                  00007FF63BAA1A3D    48:C7
                  00007FF63BAA1A44    0F1F4
                  00007FF63BAA1A48    0F1F8
                  00007FF63BAA1A50    698495
                  00007FF63BAA1A5B    C1C0
                  00007FF63BAA1A5E    69C8
                  00007FF63BAA1A64    33F9
                  00007FF63BAA1A66    C1C7
                  00007FF63BAA1A69    81C7
                  00007FF63BAA1A6F    8D3CBF
                  00007FF63BAA1A72    48:FF

edi=ED99CBA1

.text:00007FF63BAA1A38 timelock.exe:$11A38 #10E38
```

Dump 1 | Dump 2 | Dump 3 | Dump 4

```
Address           Hex
0000022038 8A2070 10 20 8A 38  20 02 00 00  C0 64 B6
000002203 88A2080 C0 64 B6 38  20 02 00 00  00 00 00
00000220388A2090  80 81 B5 38  20 02 00 00  AB AB AB
00000220388A20A0  AB AB AB AB  AB AB AB AB  EE FE EE
00000220388A20B0  00 00 00 00  00 00 00 00  00 00 00
00000220388A20C0  00 00 00 00  00 00 00 00  AF F2 BA
00000220388A20D0  66 7B B3 B7  19 0C 25 52  DF 8C 2E
00000220388A20E0  50 87 81 0C  4E 4D 9A 6D  F9 AF BC
00000220388A20F0  86 10 CB 37  E1 9D 92 B1  E7 5D F2
00000220388A2100  C6 95 27 8E  43 2C 2A 0F  B1 D7 C9
00000220388A2110  44 37 55 A0  D6 96 D7 40  13 B1 2B
00000220388A2120  36 AB 7A DC  04 DE 67 61  29 74 79
00000220388A2130  1B 11 C1 52  65 EB D6 CE  03 68 A1
00000220388A2140  BE FE 08 A8  AA 4E C5 2B  F7 13 38
00000220388A2150  07 6C E8 48  9C 76 C5 D7  4F 09 7A
00000220388A2160  E5 4E D5 72  77 4A 93 44  9C 3D 62
00000220388A2170  B0 30 2E C2  1C 61 1F 54  3F 78 C2
00000220388A2180  01 CB DD 29  95 6C 41 1C  41 C7 D6
00000220388A2190  E9 01 18 56  58 7F 1E AE  83 78 A7 0B  56 E3 7F 52  é..VX..®.x§.Vã.R
00000220388A21A0  8B FE 3E F8  E7 69 75 C2  52 2B 5A 32  25 28 9E AE  .þ>øçiuÂR+Z2%(.®
00000220388A21B0  B7 FF 25 86  C1 98 4A 23  C0 C2 B9 64  20 BF F5 2A  ·ÿ%.Á.J#ÀÂ¹d ¿õ*
00000220388A21C0  FF 70 7D 6D  79 69 AA 96  2F 66 BE 8C  26 21 76 DC  ÿp}myiª./f¾.&!vÜ
```

Command:

```
」諛迅 疉詋辜ㅒ朙„訛{蓋"簣④眣ㅅ賄ㅃ睦『趦„ㅐ晫ᄒ咨趆瞯ㅊ鋺针瞳瑹覭覫晛
```

UTF-8

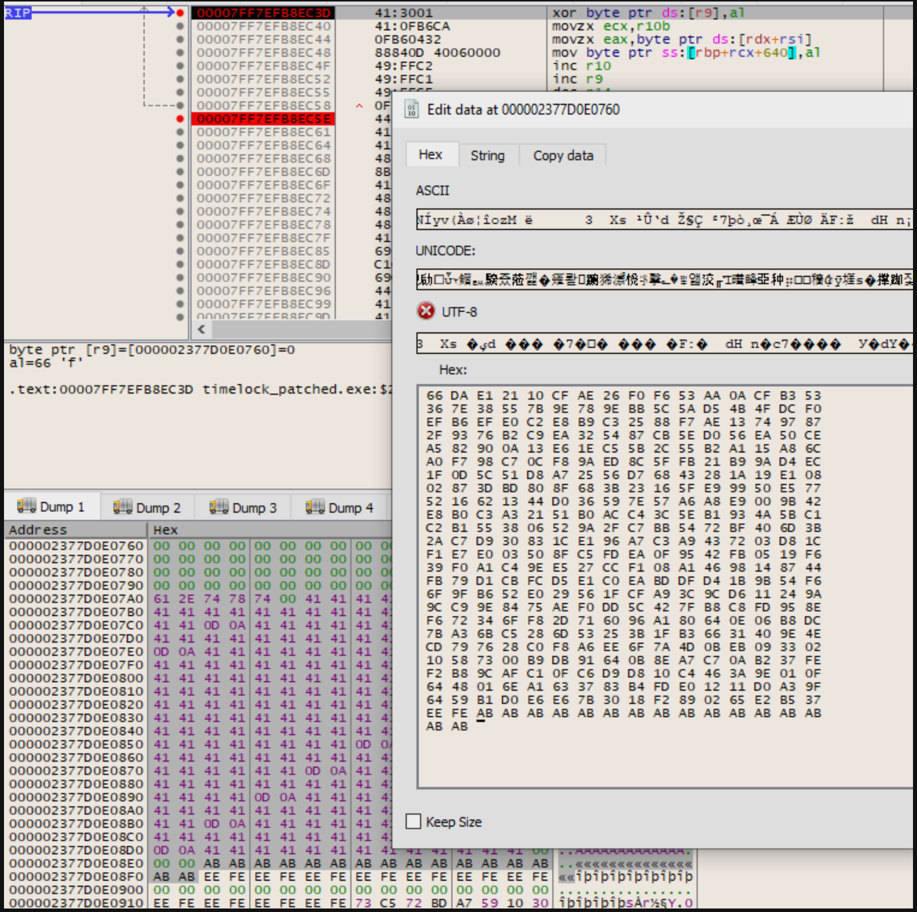
```
▸WZG��f@6|�F2?\@�� Gĸ @�� G��E@��$G��A@�g~G
```

Hex:

```
D0 7C 3B 47 EA 13 56 40 F7 3C 4F 47 AC A4 53 40
5F 78 3A 47 E3 4F 1A 40 B9 AB BD 46 1F 53 28 40
FC D7 5B 47 34 AC 29 40 44 C4 AF 46 2D 32 36 40
1E 11 4D 47 63 10 16 40 9A 8C 19 47 B0 3F 5F 40
67 05 4F 47 BE FA 1B 40 EB 63 E8 45 E8 97 63 40
49 F9 67 47 7A BD 07 40 5C B8 91 47 EE 4C 4A 40
39 EA 88 46 CF 2F 5C 40 99 2B 76 47 A2 A5 69 40
AC 37 9B 47 2A 92 32 40 EF 9F 99 47 02 2F 35 40
A1 62 8E 46 84 24 63 40 18 1C 8F 46 AE 84 58 40
9B 87 6D 47 C5 AF 48 40 93 0A 90 47 9B 9E 35 40
1E A3 8E 47 8D 94 3C 40 EE 8B 91 47 B4 3C 47 40
75 9C 33 47 7A 4C 25 40 D5 34 51 46 47 C9 2F 40
36 BF 66 47 04 46 36 40 4B 2B 1B 47 46 D4 63 40
07 51 71 47 8C E8 2B 40 FF 25 8D 47 ED 90 40 40
39 11 44 47 C7 1A 55 40 C7 8B 91 47 6E 6E 27 40
B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40
3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40
E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40
80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40
66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40
77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40
96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40
68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40
3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40
36 7C 91 46 32 3F 5C 40 B4 EF 1E 47 C4 B8 0C 40
AC AF 03 47 BB F3 45 40 8A C0 24 47 B3 A3 41 40
80 67 7E 47 79 6C 0B 40 1C 20 83 47 2D 8E 30 40
C6 07 63 47 2E 4D 51 40 E2 EE 6B 47 94 EA 13 40
66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40
00 00 00 00
```

☐ Keep Size

Extracting Ciphertext and First Round of Encryption



```
RIP ●  00007FF7EFB8EC3D   41:3001            xor byte ptr ds:[r9],al
    ●  00007FF7EFB8EC40   41:0FB6CA          movzx ecx,r10b
    ●  00007FF7EFB8EC44   0FB60432           movzx eax,byte ptr ds:[rdx+rsi]
    ●  00007FF7EFB8EC48   88840D 40060000    mov byte ptr ss:[rbp+rcx+640],al
    ●  00007FF7EFB8EC4F   49:FFC2            inc r10
    ●  00007FF7EFB8EC52   49:FFC1            inc r9
    ●  00007FF7EFB8EC55   49:
    ●  00007FF7EFB8EC58 ^ 0F
    ●  00007FF7EFB8EC5E   44
    ●  00007FF7EFB8EC61   41
    ●  00007FF7EFB8EC64   41
    ●  00007FF7EFB8EC68   48
    ●  00007FF7EFB8EC6D   8B
    ●  00007FF7EFB8EC6F   41
    ●  00007FF7EFB8EC72   48
    ●  00007FF7EFB8EC74   48
    ●  00007FF7EFB8EC78   48
    ●  00007FF7EFB8EC7F   41
    ●  00007FF7EFB8EC85   69
    ●  00007FF7EFB8EC8D   C1
    ●  00007FF7EFB8EC90   69
    ●  00007FF7EFB8EC96   44
    ●  00007FF7EFB8EC99   41
    ●  00007FF7EFB8EC9D   41

byte ptr [r9]=[000002377D0E0760]=0
al=66 'f'

.text:00007FF7EFB8EC3D timelock_patched.exe:$2
```

Dump 1 | Dump 2 | Dump 3 | Dump 4

```
Address           Hex
000002377D0E0760  00 00 00 00 00 00 00 00 00 00
000002377D0E0770  00 00 00 00 00 00 00 00 00 00
000002377D0E0780  00 00 00 00 00 00 00 00 00 00
000002377D0E0790  00 00 00 00 00 00 00 00 00 00
000002377D0E07A0  61 2E 74 78 74 00 41 41 41 41
000002377D0E07B0  41 41 41 41 41 41 41 41 41 41
000002377D0E07C0  41 41 0D 0A 41 41 41 41 41 41
000002377D0E07D0  41 41 41 41 41 41 41 41 41 41
000002377D0E07E0  0D 0A 41 41 41 41 41 41 41 41
000002377D0E07F0  41 41 41 41 41 41 41 41 41 41
000002377D0E0800  41 41 41 41 41 41 41 41 41 41
000002377D0E0810  41 41 41 41 41 41 41 41 41 41
000002377D0E0820  41 41 41 41 41 41 41 41 41 41
000002377D0E0830  41 41 41 41 41 41 41 41 41 41
000002377D0E0840  41 41 41 41 41 41 41 41 41 41
000002377D0E0850  41 41 41 41 41 41 41 41 0D 0A
000002377D0E0860  41 41 41 41 41 41 41 41 41 41
000002377D0E0870  41 41 41 41 41 41 0D 0A 41 41
000002377D0E0880  41 41 41 41 41 41 41 41 41 41
000002377D0E0890  41 41 41 41 0D 0A 41 41 41 41
000002377D0E08A0  41 41 41 41 41 41 41 41 41 41
000002377D0E08B0  41 41 0D 0A 41 41 41 41 41 41
000002377D0E08C0  41 41 41 41 41 41 41 41 41 41
000002377D0E08D0  0D 0A 41 41 41 41 41 41 41 41 41 41 41 41 41 00  ..AAAAAAAAAAAAA.
000002377D0E08E0  00 00 AB AB AB AB AB AB AB AB AB AB AB AB AB AB  ..««««««««««««««
000002377D0E08F0  AB AB EE FE EE FE EE FE EE FE EE FE EE FE EE FE  ««îþîþîþîþîþîþîþ
000002377D0E0900  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002377D0E0910  EE FE EE FE EE FE EE FE 73 C5 72 BD A7 59 10 30  îþîþîþîþsÅr½§Y.0
```

Edit data at 000002377D0E0760

Hex | String | Copy data

ASCII

```
NÍyv(Àø¦îozM ë       3  Xs ¹Û'd Ž§Ç ²7þò¸œ¯Á ÆÙØ ÄF:ž  dH n¡
```

UNICODE:

```
勆□ǚ٭鋼„騌忝菈㗭�穼뢌□鰤瀇澿悅ꭍ擊ـ�늹뗞滖╓T嚡鋒亞种;□□禮ό ỵ墶s�撐蹈
```

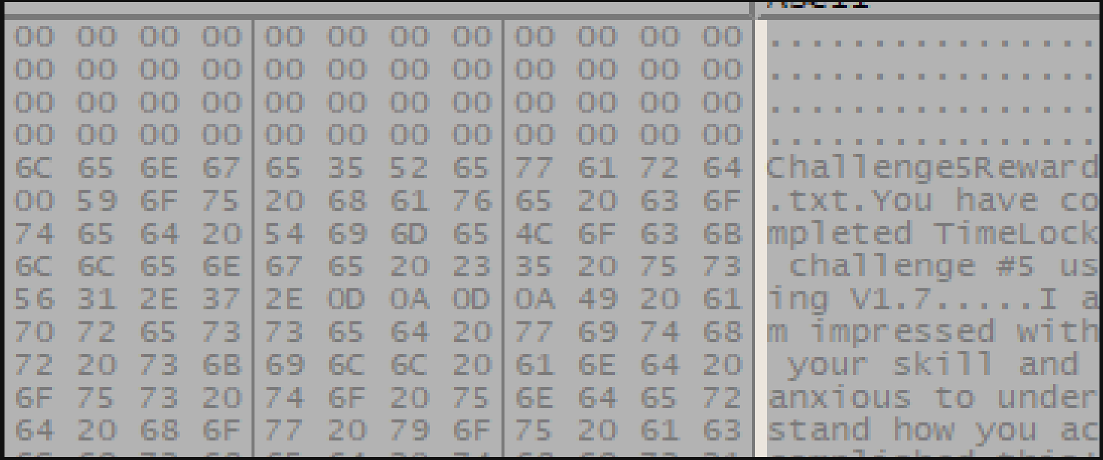
UTF-8

```
3  Xs �يd ��� �7�□� ��� �F:�  dH n�c7����  Y�dY�
```

Hex:

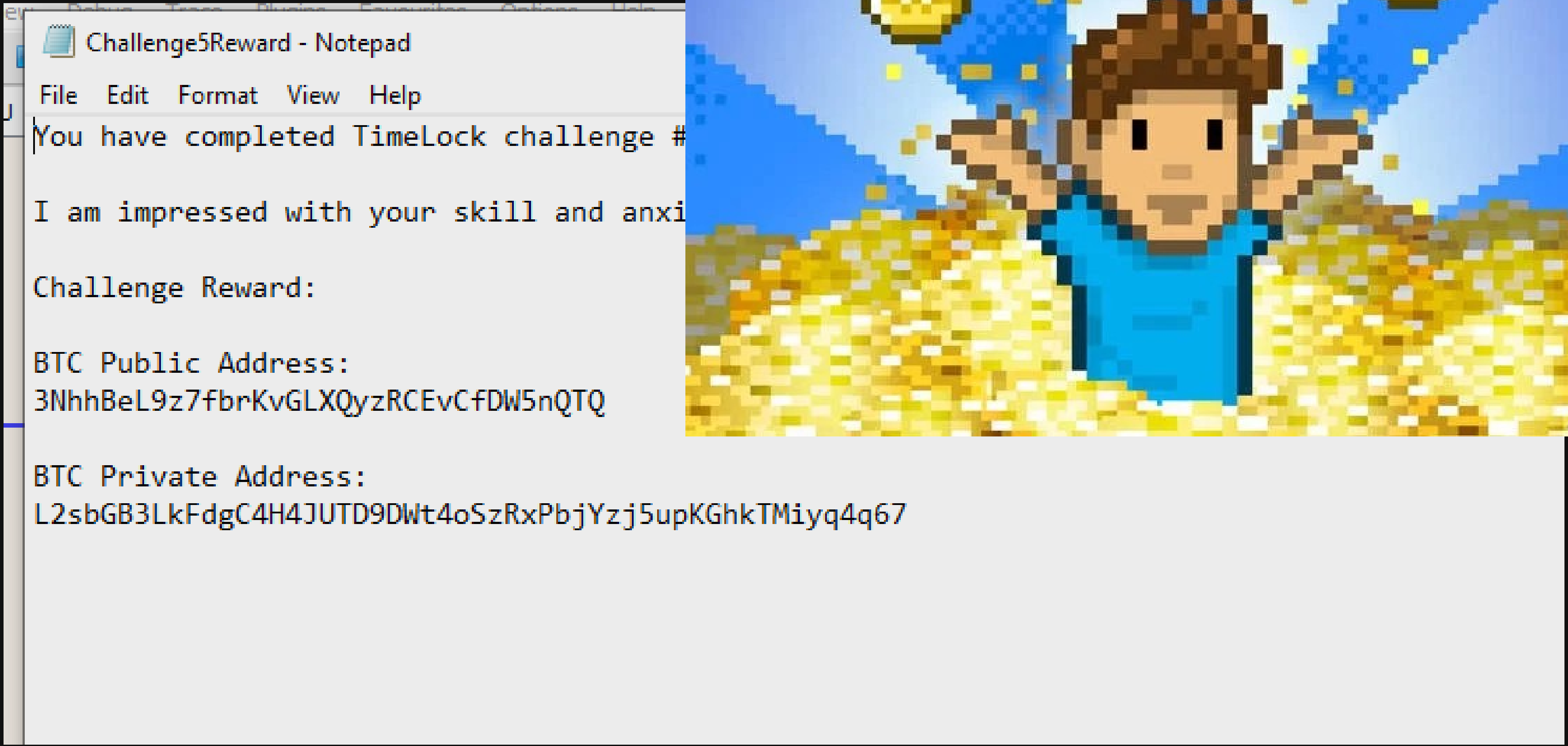
```
66 DA E1 21 10 CF AE 26 F0 F6 53 AA 0A CF B3 53
36 7E 38 55 7B 9E 78 9E BB 5C 5A D5 4B 4F DC F0
EF B6 EF E0 C2 E8 B9 C3 25 88 F7 AE 13 74 97 87
2F 93 76 B2 C9 EA 32 54 87 CB 5E D0 56 EA 50 CE
A5 82 90 0A 13 E6 1E C5 5B 2C 55 B2 A1 15 A8 6C
A0 F7 98 C7 0C F8 9A ED 8C 5F FB 21 B9 9A D4 EC
1F 0D 5C 51 D8 A7 25 56 D7 68 43 28 1A 19 E1 08
02 87 3D BD 80 8F 68 3B 23 16 5F E9 99 50 E5 77
52 16 62 13 44 D0 36 59 7E 57 A6 A8 E9 00 9B 42
E8 B0 C3 A3 21 51 B0 AC C4 3C 5E B1 93 4A 5B C1
C2 B1 55 38 06 52 9A 2F C7 BB 54 72 BF 40 6D 3B
2A C7 D9 30 83 1C E1 96 A7 C3 A9 43 72 03 D8 1C
F1 E7 E0 03 50 8F C5 FD EA 0F 95 42 FB 05 19 F6
39 F0 A1 C4 9E E5 27 CC F1 08 A1 46 98 14 87 44
FB 79 D1 CB FC D5 E1 C0 EA BD DF D4 1B 9B 54 F6
6F 9F B6 52 E0 29 56 1F CF A9 3C 9C D6 11 24 9A
9C C9 9E 84 75 AE F0 DD 5C 42 7F B8 C8 FD 95 8E
F6 72 34 6F F8 2D 71 60 96 A1 80 64 0E 06 B8 DC
7B A3 6B C5 28 6D 53 25 3B 1F B3 66 31 40 9E 4E
CD 79 76 28 C0 F8 A6 EE 6F 7A 4D 0B EB 09 33 02
10 58 73 00 B9 DB 91 64 0B 8E A7 C7 0A B2 37 FE
F2 B8 9C AF C1 0F C6 D9 D8 10 C4 46 3A 9E 01 0F
64 48 01 6E A1 63 37 83 B4 FD E0 12 11 D0 A3 9F
64 59 B1 D0 E6 E6 7B 30 18 F2 89 02 65 E2 B5 37
EE FE AB AB AB AB AB AB AB AB AB AB AB AB AB AB
AB AB
```

☐ Keep Size



```
00 00 00 00  00 00 00 00  00 00 00 00  ................
00 00 00 00  00 00 00 00  00 00 00 00  ................
00 00 00 00  00 00 00 00  00 00 00 00  ................
00 00 00 00  00 00 00 00  00 00 00 00  ................
6C 65 6E 67  65 35 52 65  77 61 72 64  Challenge5Reward
00 59 6F 75  20 68 61 76  65 20 63 6F  .txt.You have co
74 65 64 20  54 69 6D 65  4C 6F 63 6B  mpleted TimeLock
6C 6C 65 6E  67 65 20 23  35 20 75 73   challenge #5 us
56 31 2E 37  2E 0D 0A 0D  0A 49 20 61  ing V1.7.....I a
70 72 65 73  73 65 64 20  77 69 74 68  m impressed with
72 20 73 6B  69 6C 6C 20  61 6E 64 20   your skill and 
6F 75 73 20  74 6F 20 75  6E 64 65 72  anxious to under
64 20 68 6F  77 20 79 6F  75 20 61 63  stand how you ac
```

Loot #5



Challenge5Reward - Notepad

File Edit Format View Help

```
You have completed TimeLock challenge #

I am impressed with your skill and anxi

Challenge Reward:

BTC Public Address:
3NhhBeL9z7fbrKvGLXQyzRCEvCfDW5nQTQ

BTC Private Address:
L2sbGB3LkFdgC4H4JUTD9DWt4oSzRxPbjYzj5upKGhkTMiyq4q67
```

About Me

- Sustaining Engineer at Canonical.
  - Fixing gremlins in Ubuntu kernels.
  - Reversing is my fun hobby =p
- Read my blog:

https://ruffell.nz

matthew@ruffell.nz

THE WORLD'S FIRST? UBUNTU ROMANTIC SCHOOL COMEDY:
Ubunchu!
04
瀬尾 浩史
BY HIROSHI SEO
http://www.aerialline.com
THE THREE BUNNIES
LGPL
GPL
MPL
CC
BSD
GFDL
Ver 01 2010-01-17
First Printed In: ASCII Magazine "Saku Saku Ubuntu!"
Published by: ASCII MEDIA WORKS Inc.
http://ascii.asciimw.jp
Translated By: Anton Ekblad
Edited By: Arturo Silva and Martin Owens