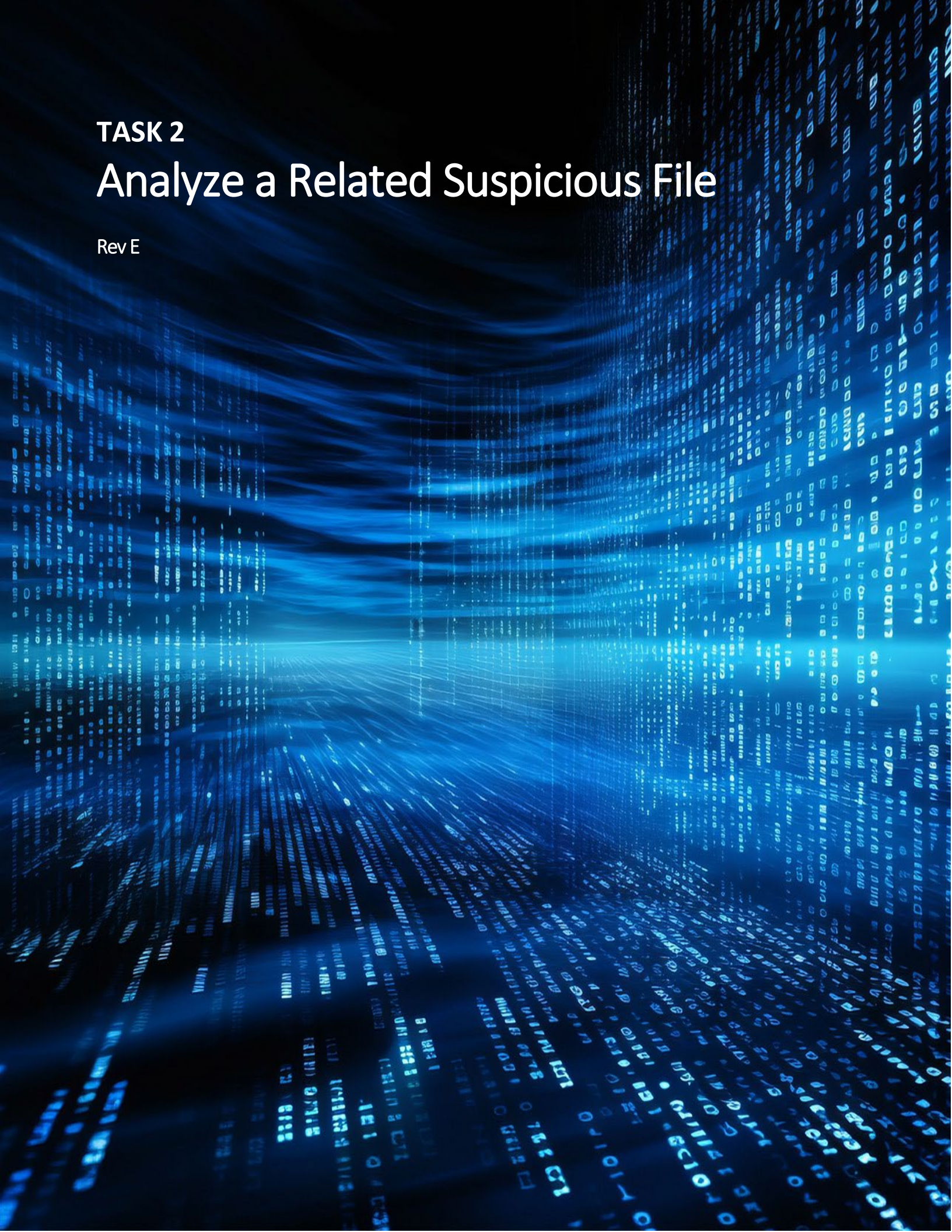


TASK 2

Analyze a Related Suspicious File

Rev E

Analyze a Related Suspicious File

Analyze a Related Suspicious File

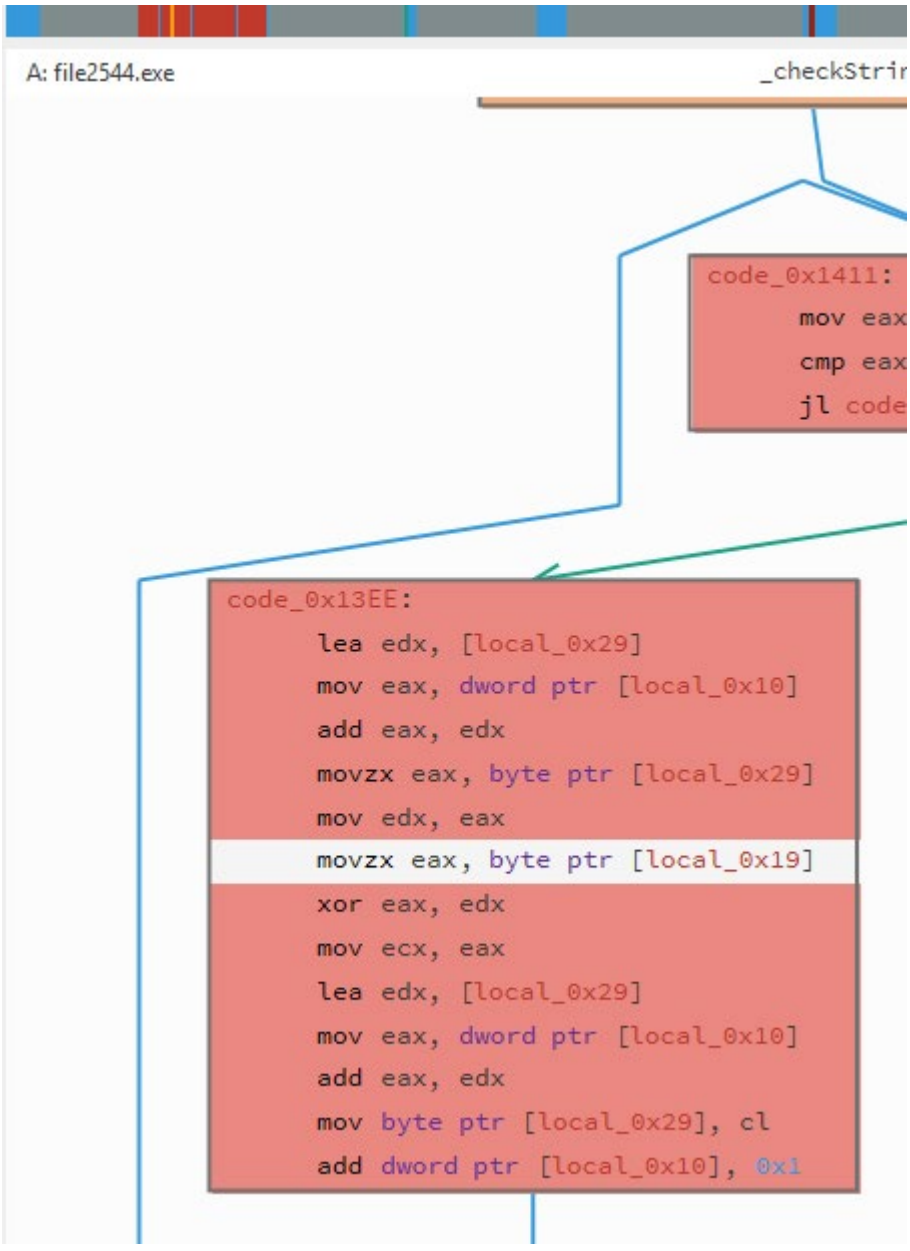
1 Comparing Binaries Using Relyze

In Relyze we see in code_0x13EE:

xor eax, edx

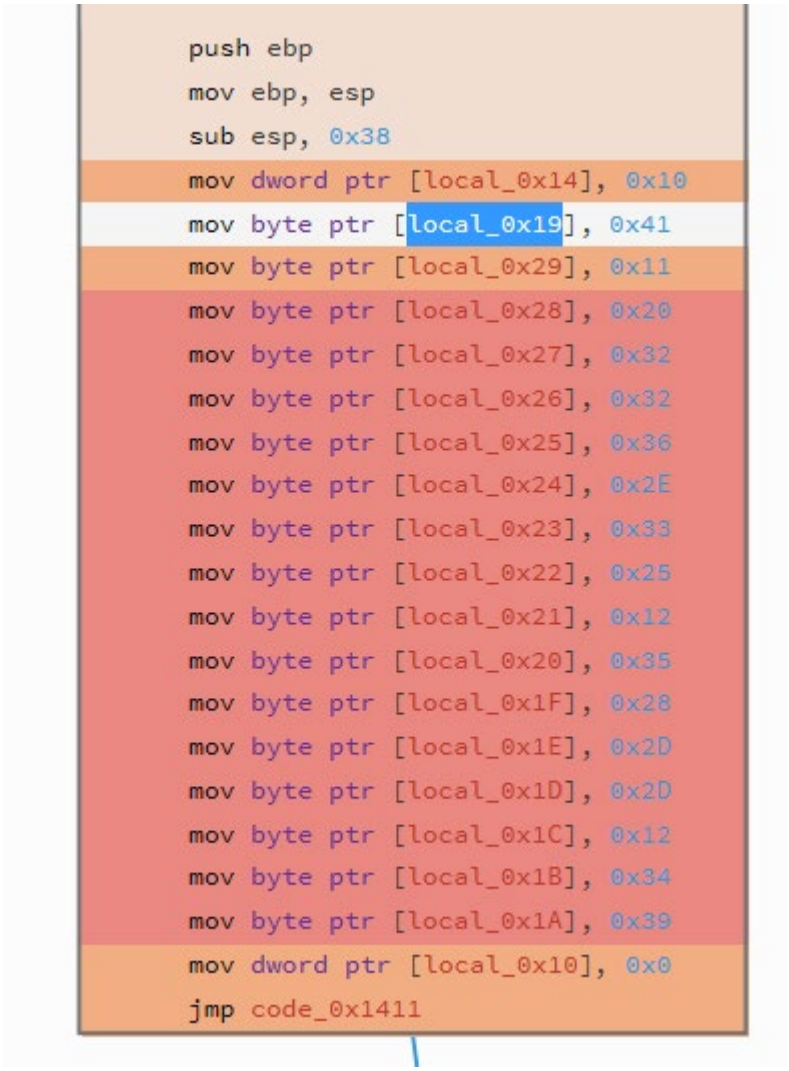
and just above it

movzx eax, byte ptr [local_0x19]



Analyze a Related Suspicious File

Search local_0x19 it brings you to what appears could be an obfuscated password

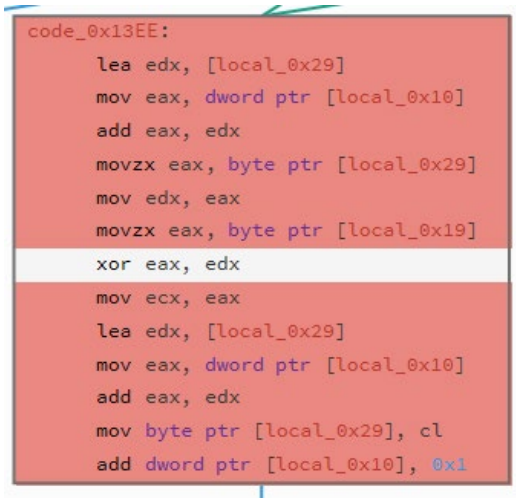


Analyze a Related Suspicious File

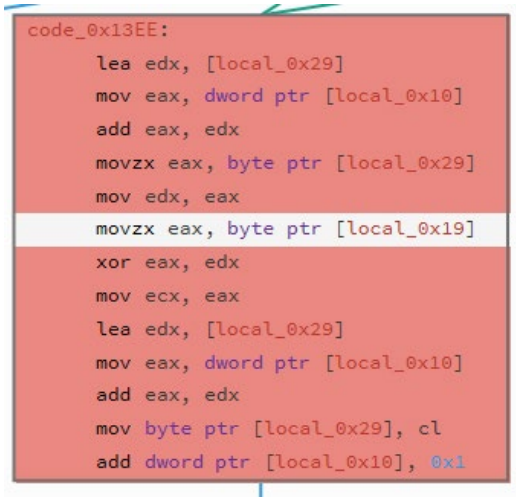
2 Crack and Decrypt the Password

Search for xor and key
Found in 0x13EE:
xor eax, edx

one will be the data
one will be the key
work backwards to determine which is which

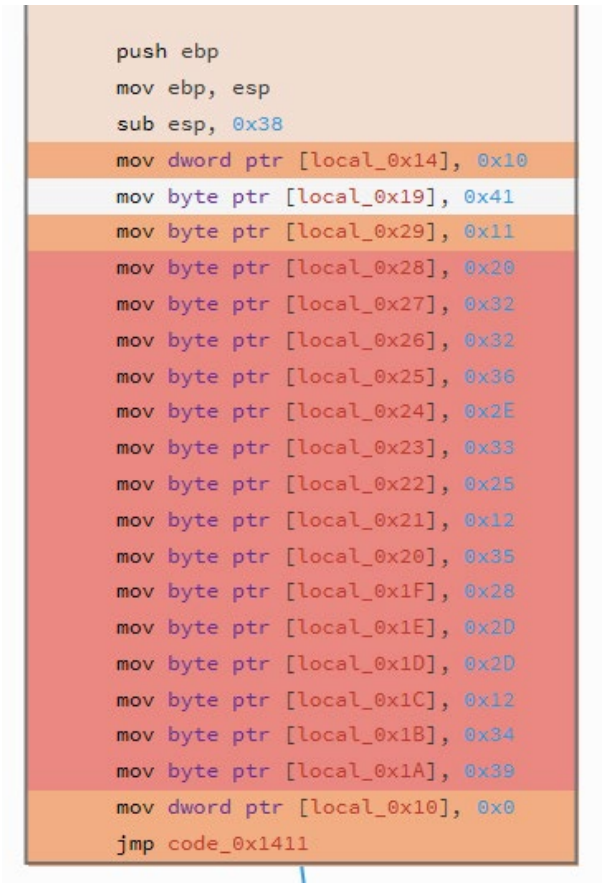


One step above you can see movzx eax



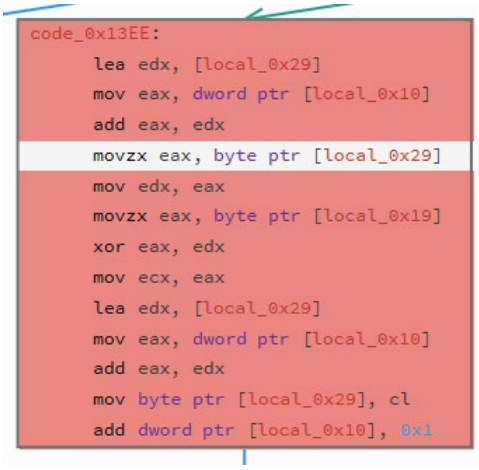
Follow the path to local_0x19 in the boxes above

Analyze a Related Suspicious File



This shows that eax is the static value and is 41…41 is the key

With eax established now look into edx



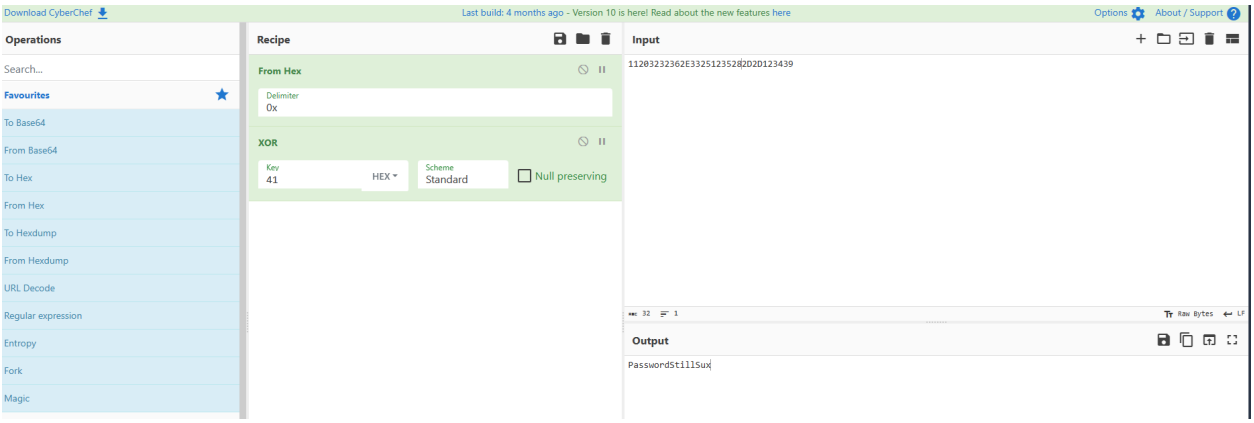
Analyze a Related Suspicious File

```
push ebp
mov ebp, esp
sub esp, 0x38
mov dword ptr [local_0x14], 0x10
mov byte ptr [local_0x19], 0x41
mov byte ptr [local_0x29], 0x11
mov byte ptr [local_0x28], 0x20
mov byte ptr [local_0x27], 0x32
mov byte ptr [local_0x26], 0x32
mov byte ptr [local_0x25], 0x36
mov byte ptr [local_0x24], 0x2E
mov byte ptr [local_0x23], 0x33
mov byte ptr [local_0x22], 0x25
mov byte ptr [local_0x21], 0x12
mov byte ptr [local_0x20], 0x35
mov byte ptr [local_0x1F], 0x28
mov byte ptr [local_0x1E], 0x2D
mov byte ptr [local_0x1D], 0x2D
mov byte ptr [local_0x1C], 0x12
mov byte ptr [local_0x1B], 0x34
mov byte ptr [local_0x1A], 0x39
mov dword ptr [local_0x10], 0x0
jmp code_0x1411
```

Looking at the above starting at local_0x29 and moving down…you can see that each is decreasing by 1 which has this appear to be a loop…

Using 41 as the key…cross referencing each corresponding number as a hexadecimal converting it over to ascii to get a corresponding number or letter…

Use CyberChef or XOR Cipher to convert the Hex



Analyze a Related Suspicious File

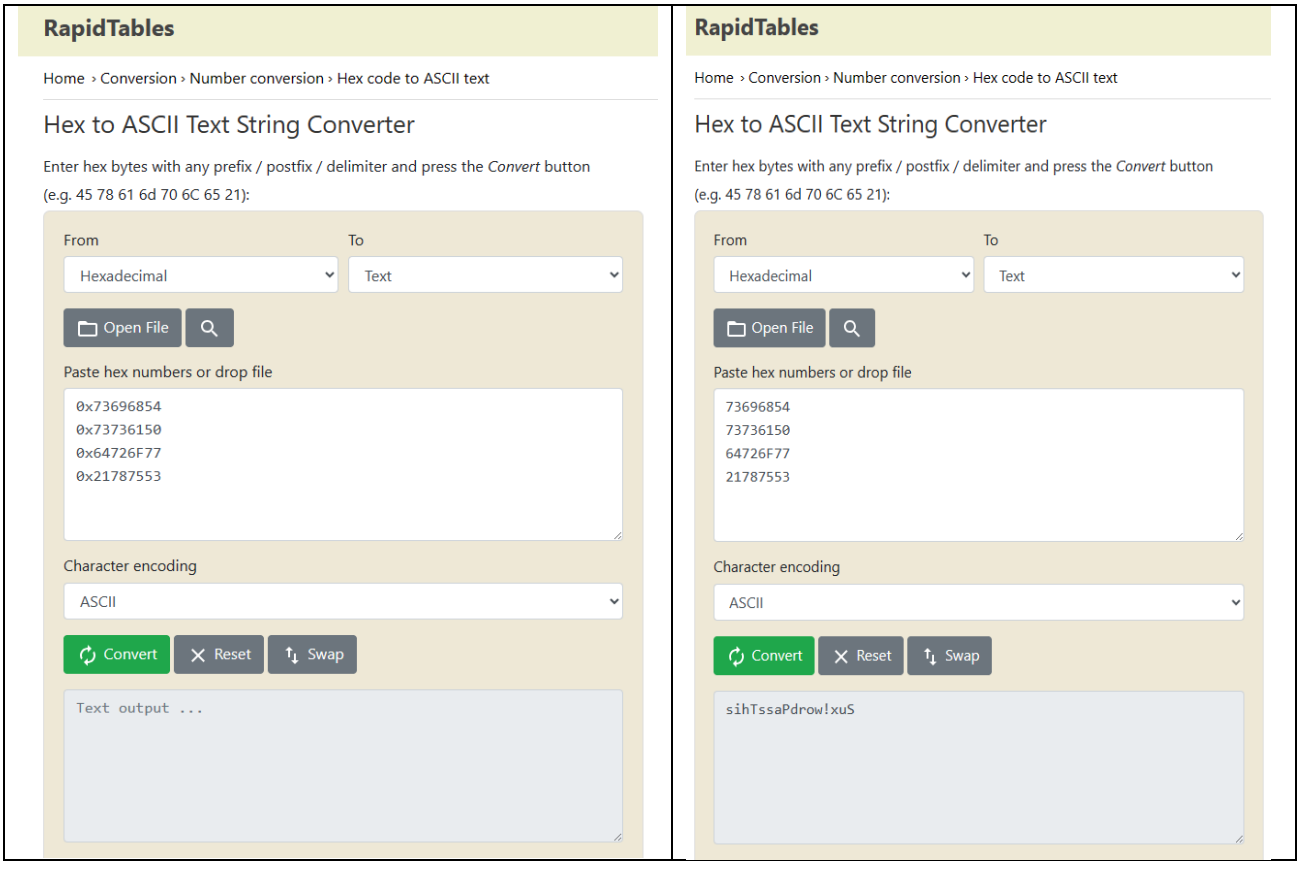
Analyze a Related Suspicious File

3 Converting From HEX to ASCII

Converting file 1732 from HEX into ASCII

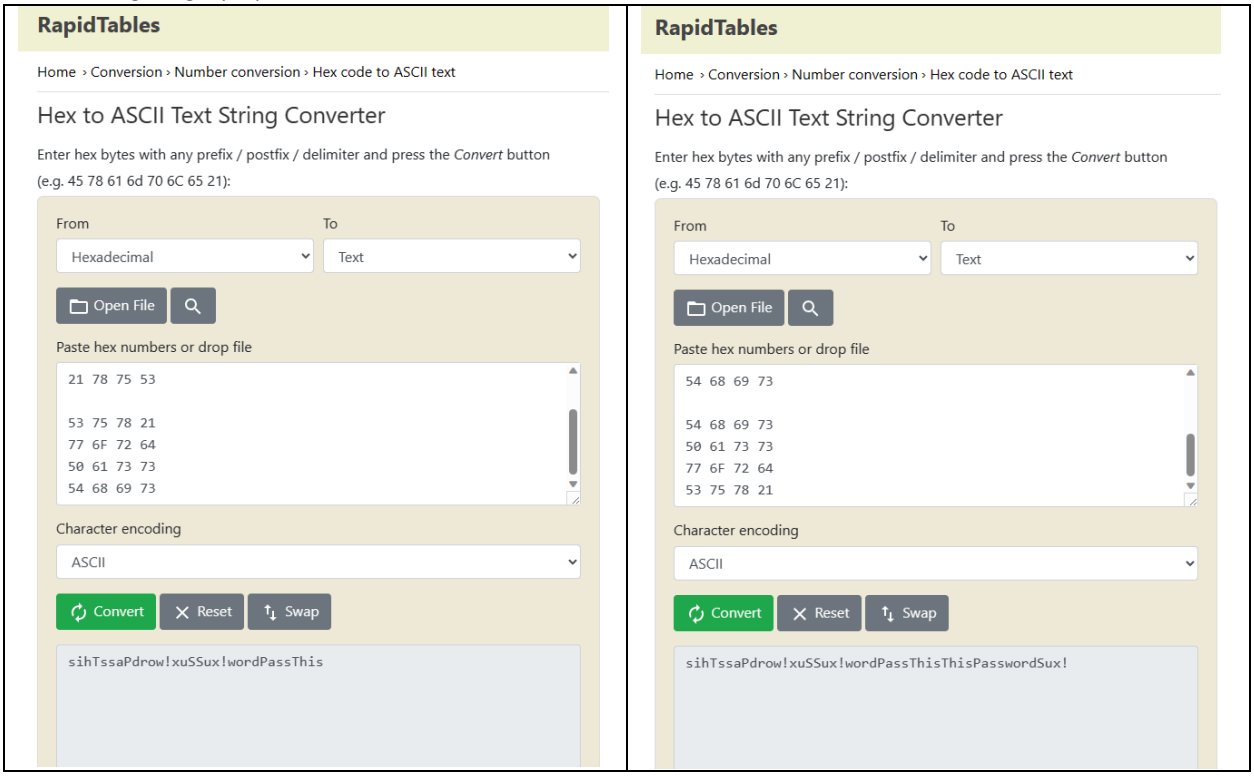
```
void __cdecl _checkString( int32_t p1 )
{
   uint32_t local_0x3C;
   uint32_t local_0x38;
   uint32_t local_0x34;
   uint32_t local_0x20;
   uint32_t local_0x1C;
   uint32_t local_0x18;
   uint32_t local_0x14;
   uint32_t local_0x10;

      push ebp
      mov ebp, esp
      sub esp, 0x38
      mov dword ptr [local_0x20], 0x73696854
      mov dword ptr [local_0x1C], 0x73736150
      mov dword ptr [local_0x18], 0x64726F77
      mov dword ptr [local_0x14], 0x21787553
      mov eax, dword ptr [p1]
      mov dword ptr [local_0x3C], eax
      call .idata$5_59   ; unsigned int __cdecl( char * _Str )
      cmp eax, 0x10
      jnz code_0x13FE
```



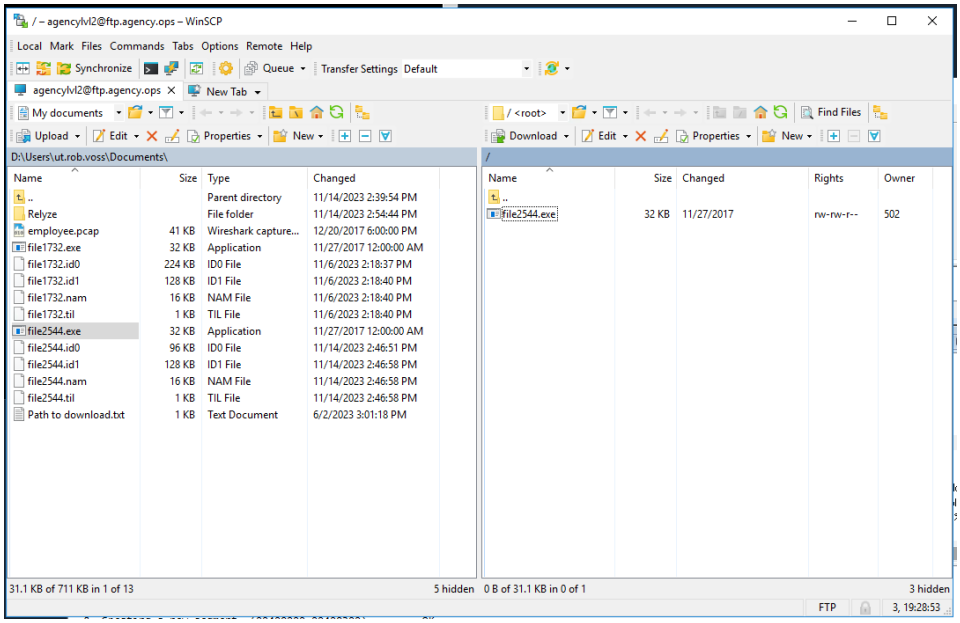
Analyze a Related Suspicious File

Reverse the hexadecimal
Then rearrange to get proper order



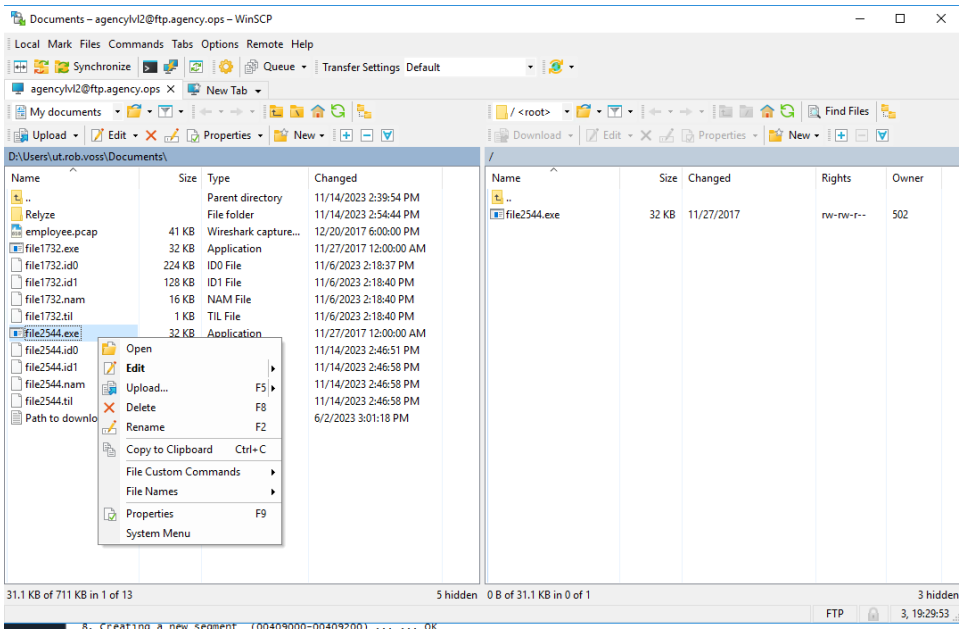
4 Run the Program

Open the Desktop and select the program

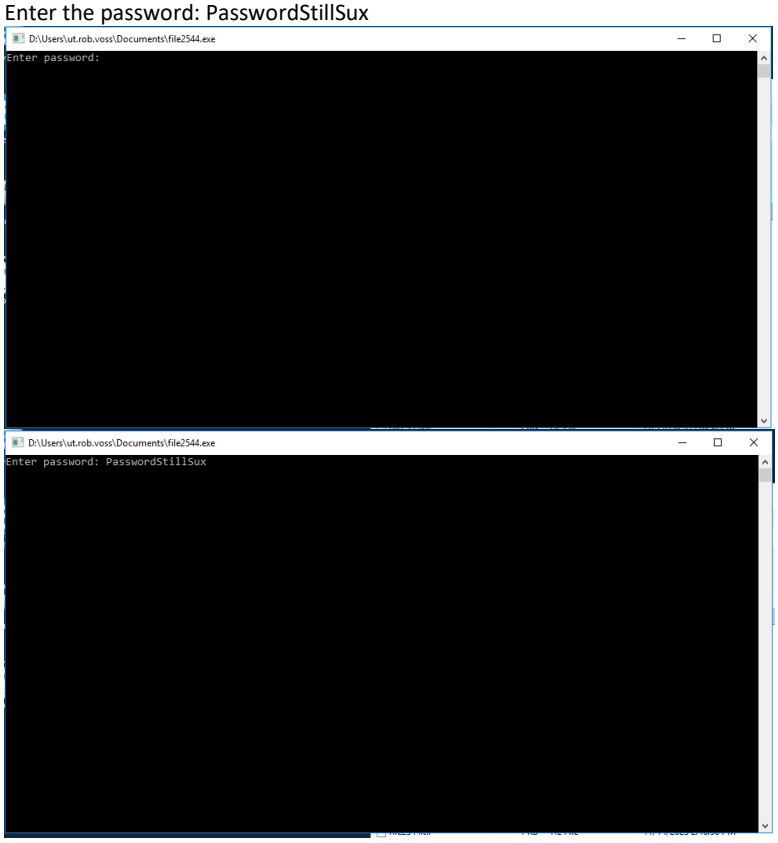


Open the program

Analyze a Related Suspicious File

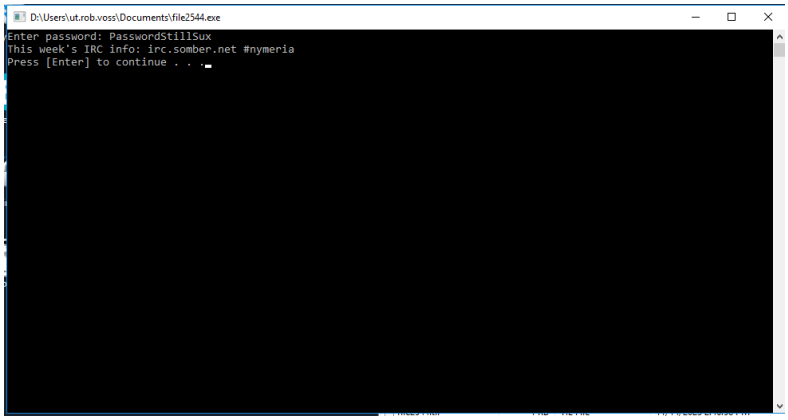


Enter the password: PasswordStillSux



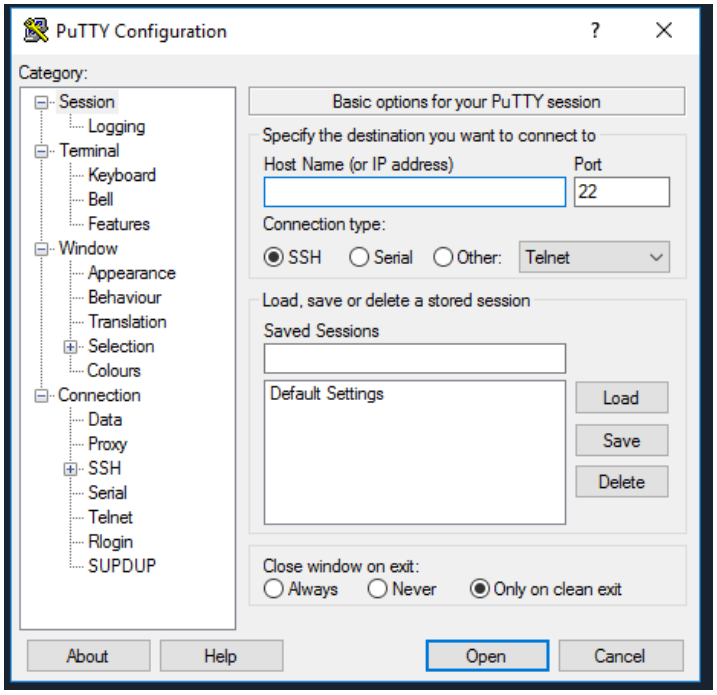
Analyze a Related Suspicious File

Hit enter:



5 Connect to the IRC Channel

5.1 Open PuTTY

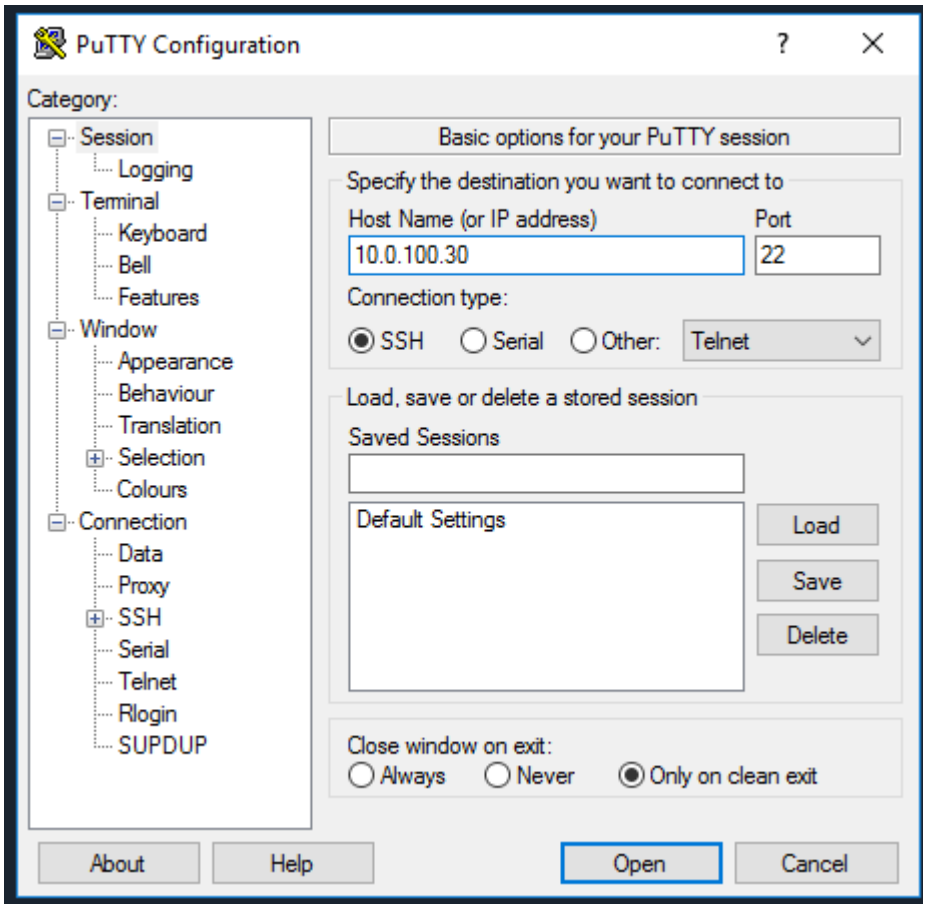


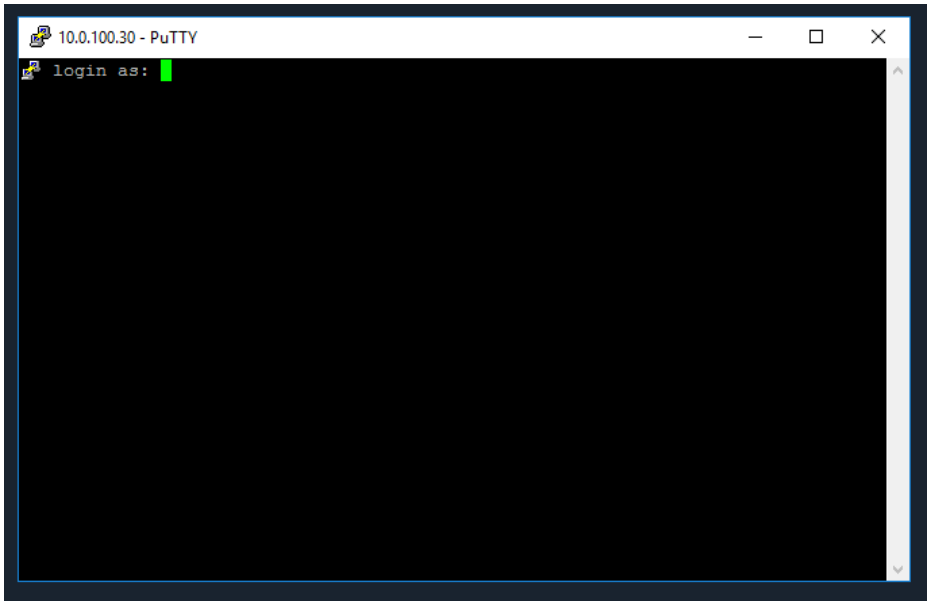
IP: 10.0.100.30
Username: traveler2721
Password: EuD3jwtre4jGlEt07Tej

Analyze a Related Suspicious File

5.1.1 Input Host Name

IP: 10.0.100.30

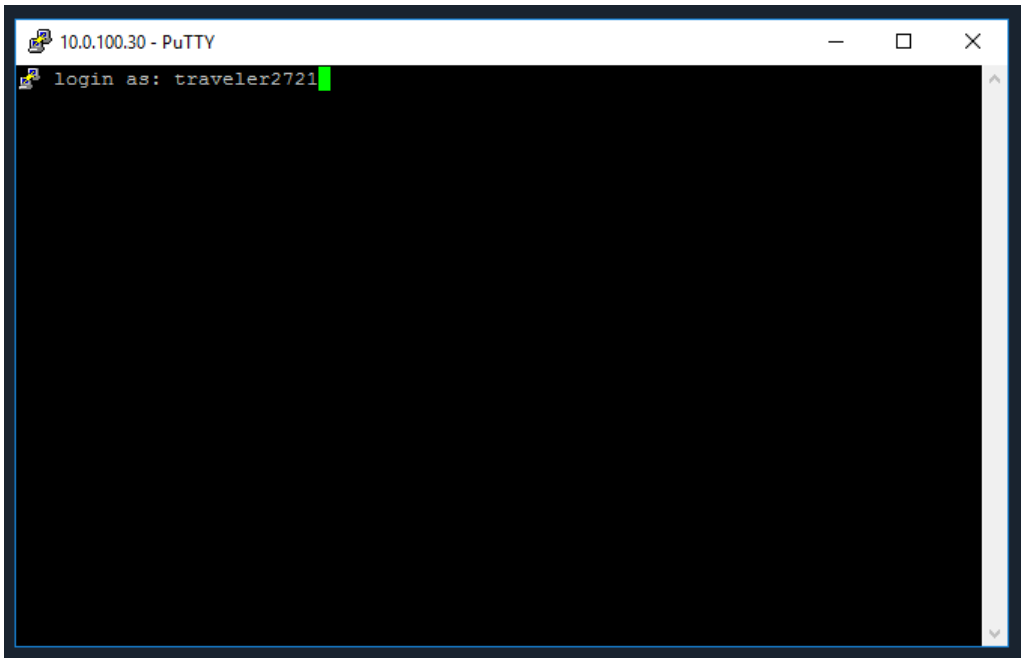




Analyze a Related Suspicious File

5.1.2 Input Username

Username: traveler2721(copy from above and right click on the mouse will paste in Linux) hit enter.

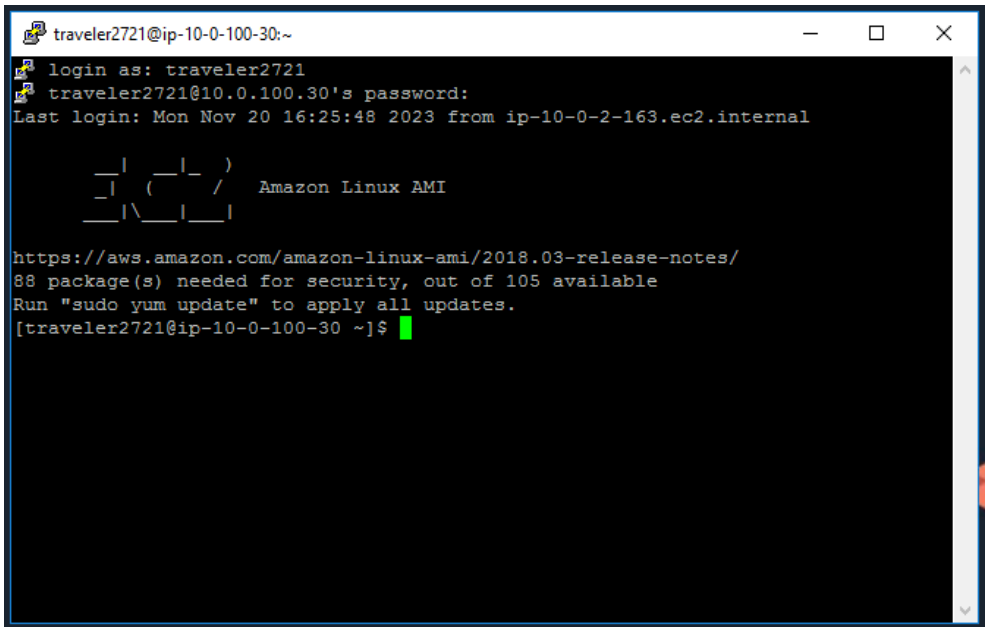


5.1.3 Input Password

Input Password (copy from above and right click on the mouse will paste in Linux) hit enter.

REMEMBER: PASSWORD IS ALWAYS INVISIBLE…YOU MIGHT NEED TO PUT IT IN TWICE TO MAKE THE CONNECTION.

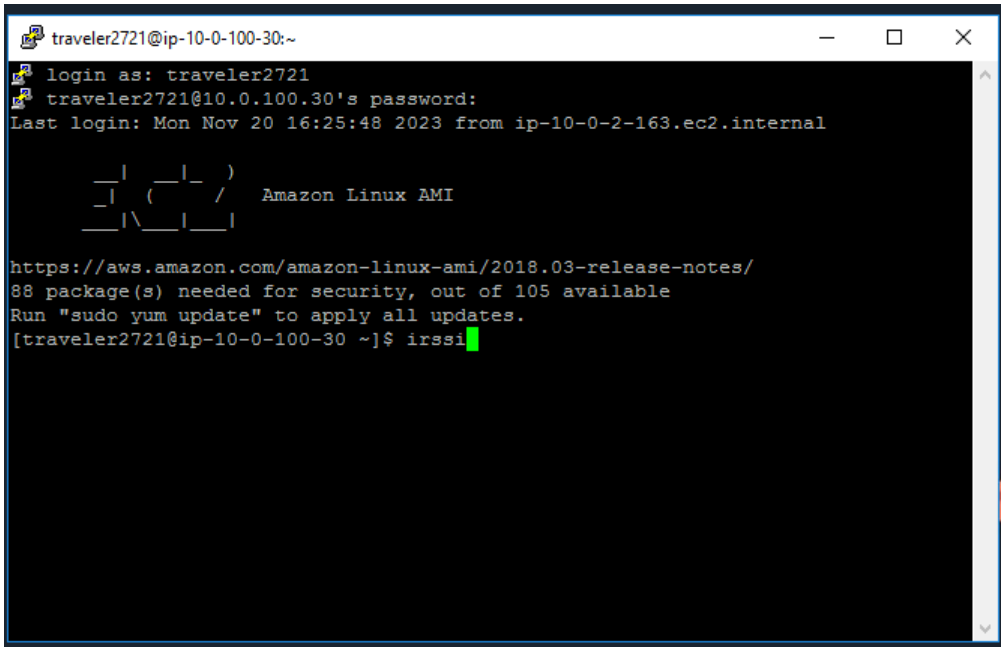
Password: EuD3jwtre4jGlEt07Tej

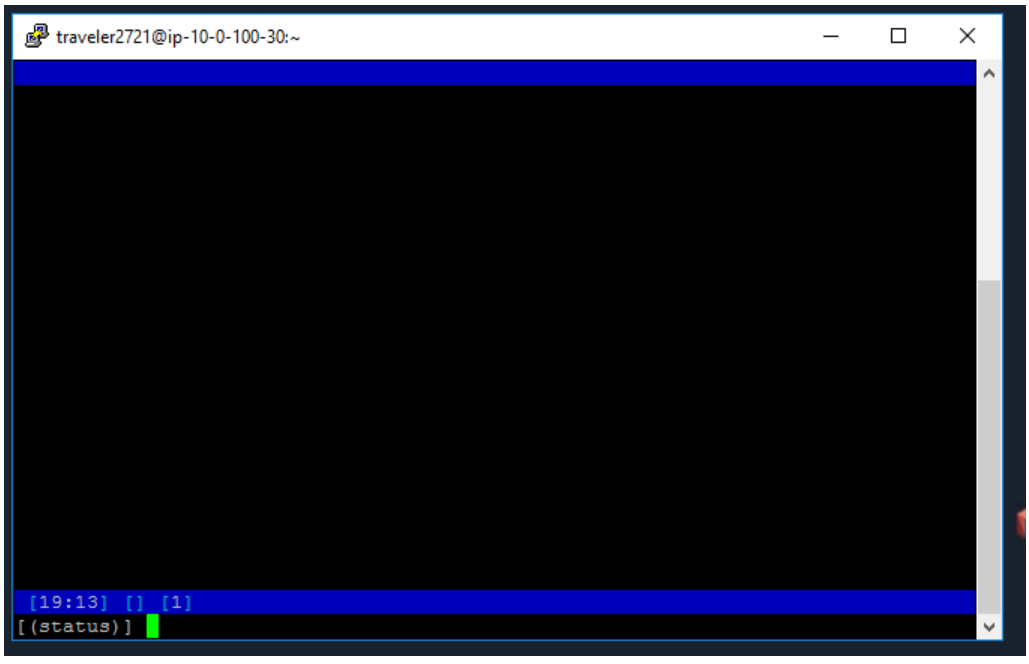


Analyze a Related Suspicious File

5.2 Input irssi

Input irssi and hit enter

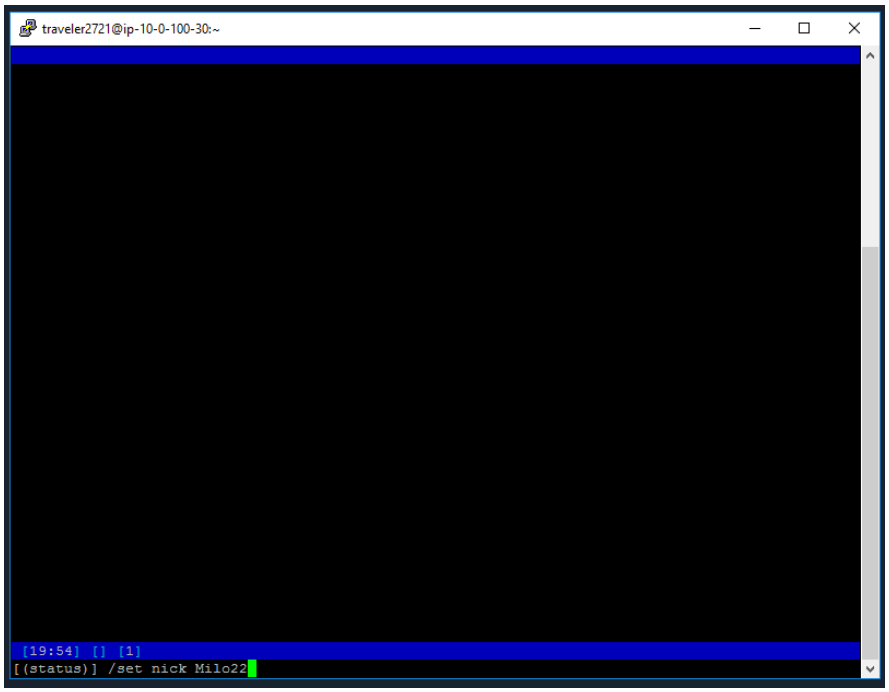




Analyze a Related Suspicious File

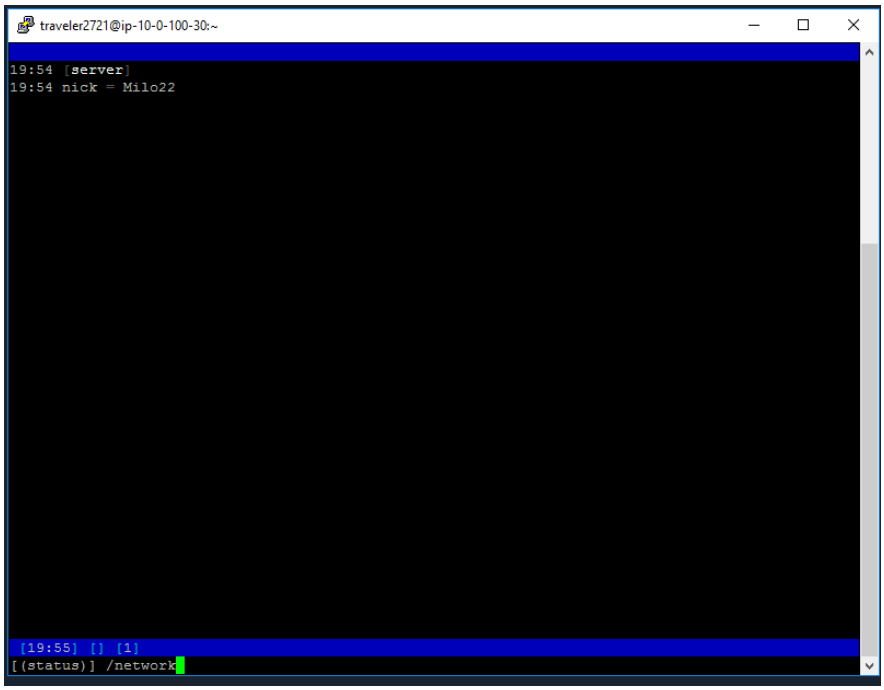
5.2.1 Set Nickname

NOW ENTER: /set nick <nick name of choice>



5.2.2 Request Network List

/network and hit enter

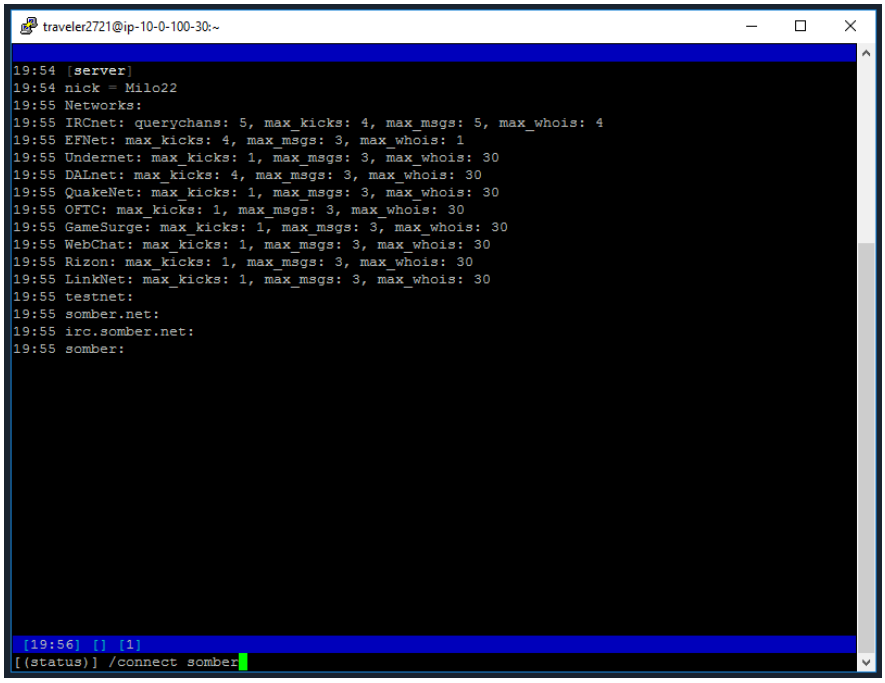


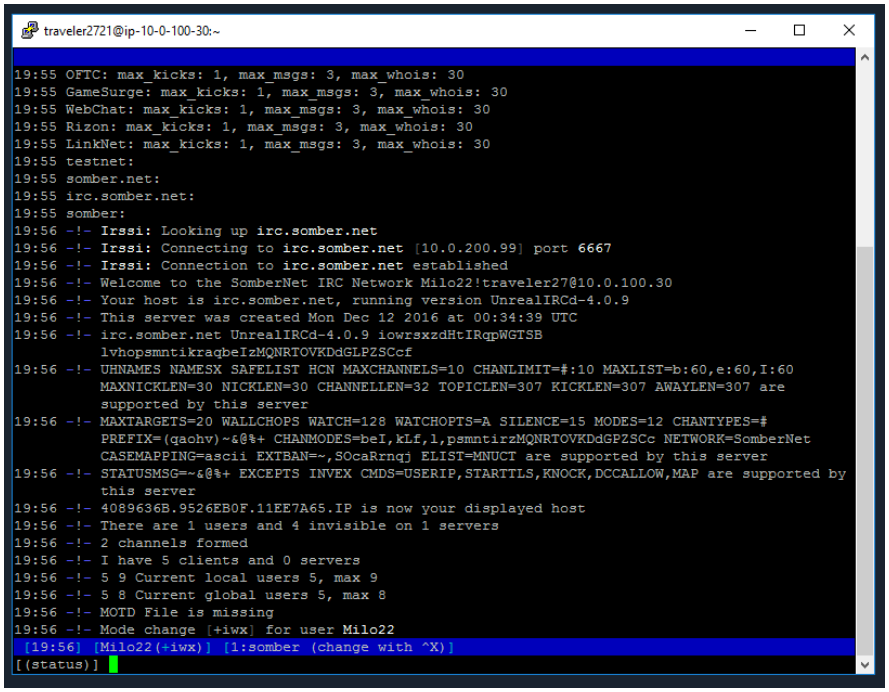
Connect to network as found in WinSCP (This week's IRC info: irc.somber.net #nymeria)

Analyze a Related Suspicious File

5.2.3 Connect to network (somber)

/connect somber and hit enter

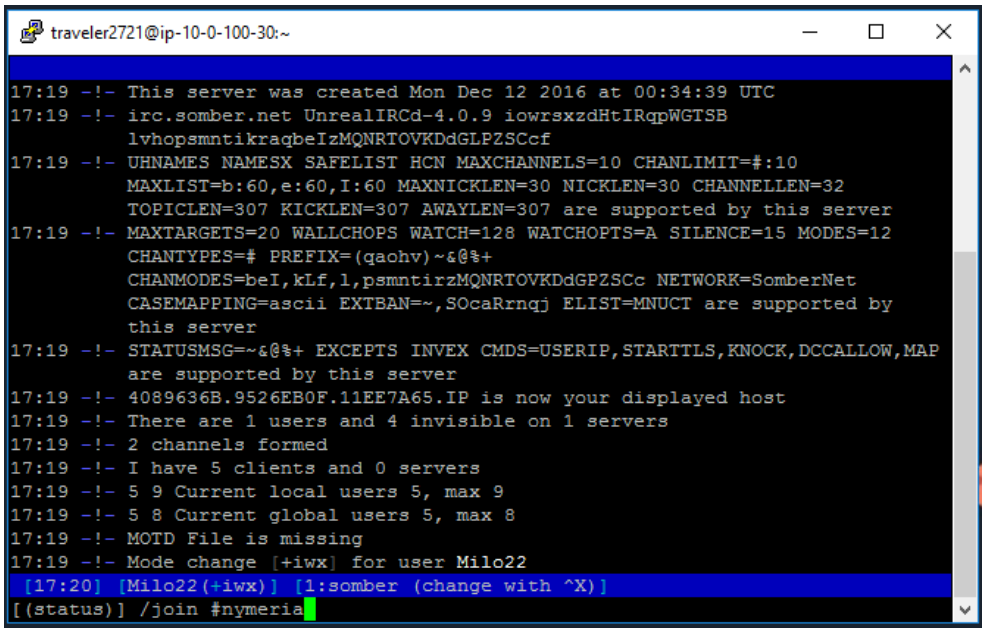




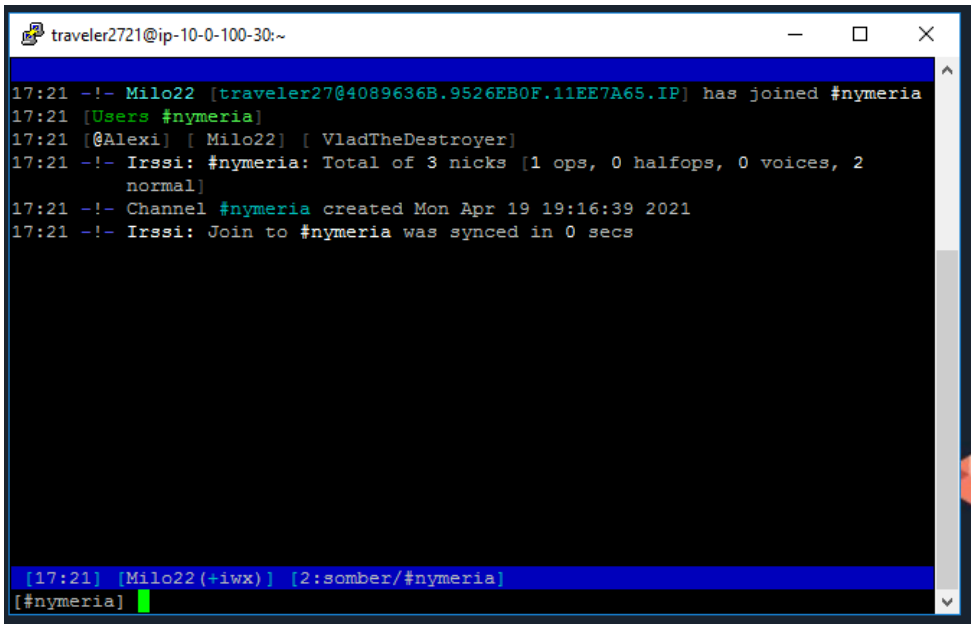
Analyze a Related Suspicious File

5.2.4 Join #nymeria

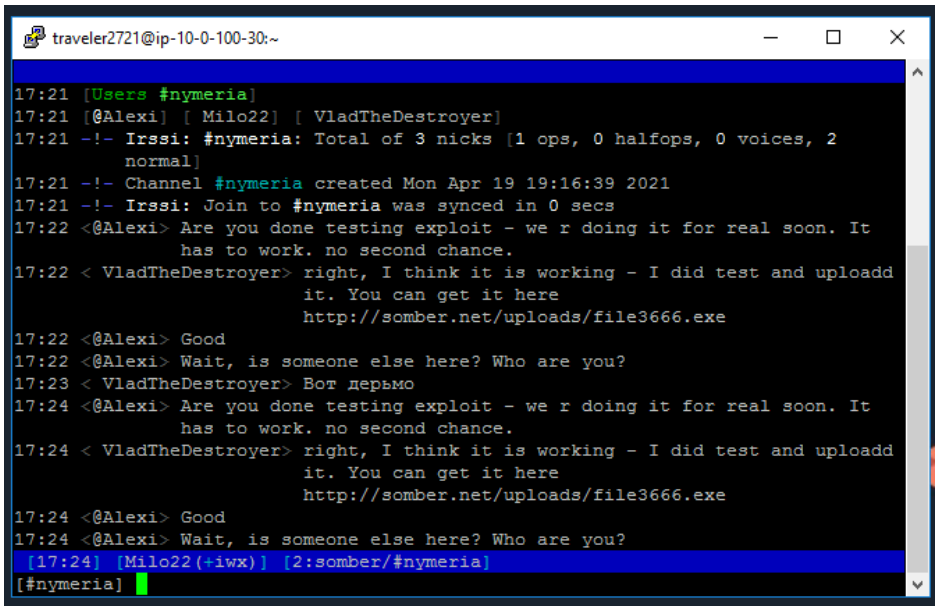
/join #nymeria and hit enter



5.3 Observe conversation



Analyze a Related Suspicious File



5.3.1 Identify Other Players

Other players noted are: VladTheDestroyer and Alexi

5.3.2 See Who the Players Are

/who and /whois