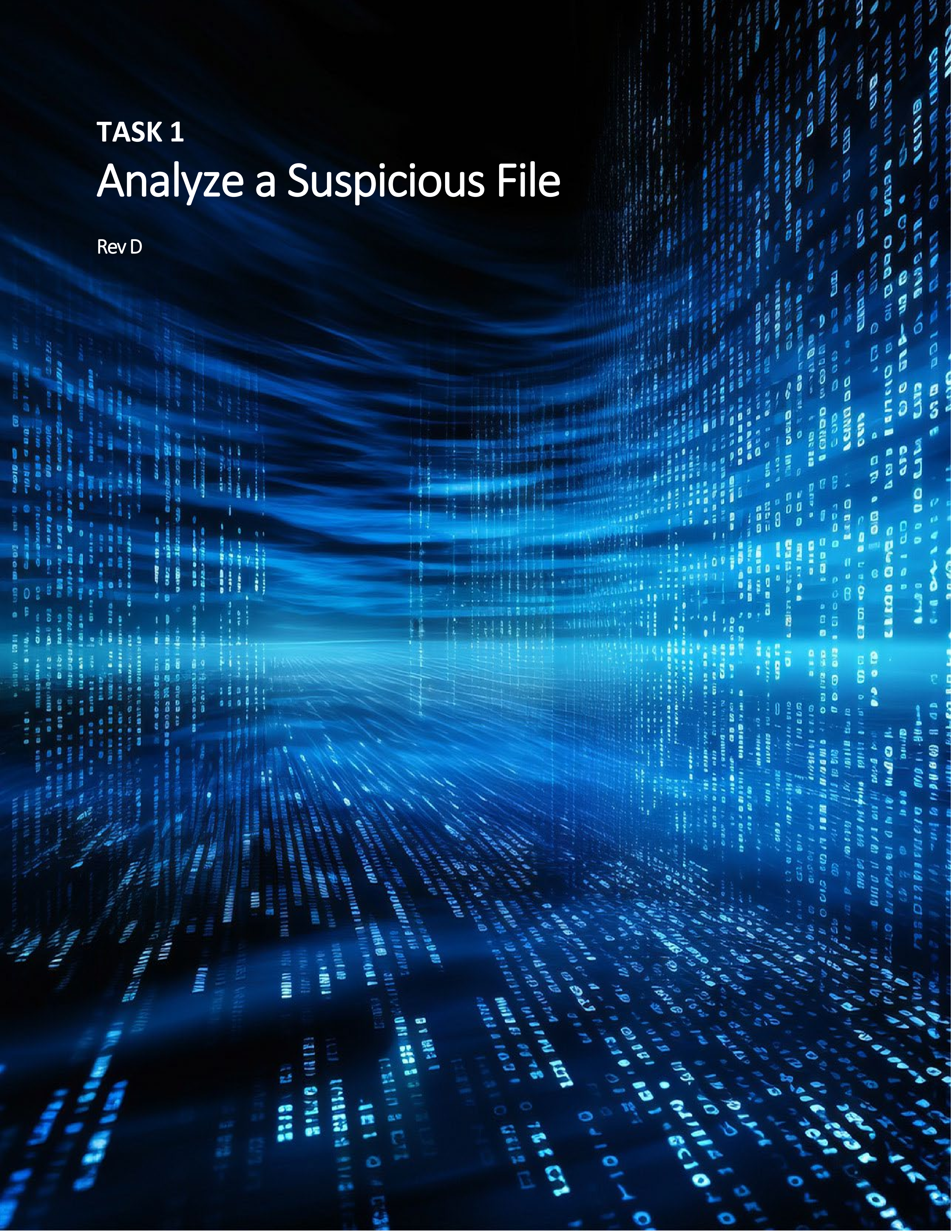
TASK 1

Analyze a Suspicious File

Rev D



Analyze a Suspicious File

Analyze a Suspicious File

1 Analyzing a Piece of Intel

This appears to be an entry into an IRC…with the topic of discussion based on “This week’s IRC info:”.
I know it starts with an entry form…but I’m not sure where it leads to…

The password is: ThisPasswordSux!

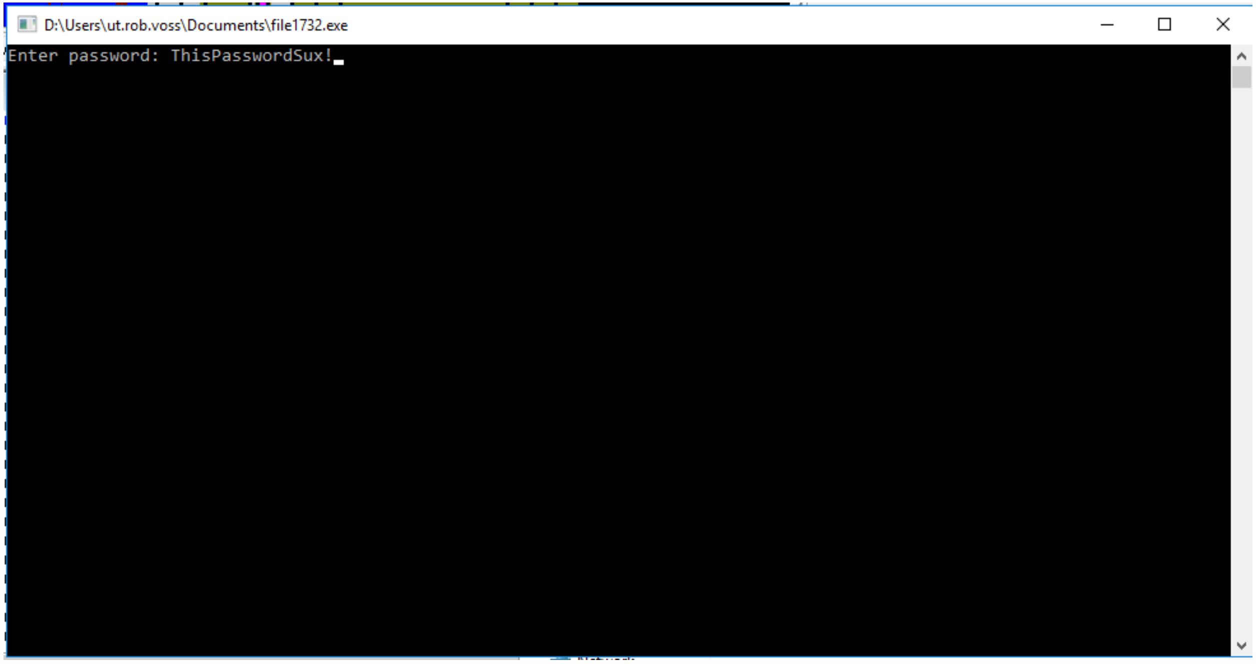
Function Call	Sub
start	401280
TlsCallback_0	401630
__getmainargs	401DFC
_setmode	401E04
__p__fmode	401E0C
__p__environ	401E14
_cexit	401E1C
signal	401E24
printf	401E2C
fgets	401E34
getchar	401E3C
strlen	401E44
puts	401E4C
putchar	401E54
fgetc	401E5C
clearerr	401E64
fflush	401E6C
fwrite	401E74
vfprintf	401E7C
abort	401E84
memcpy	401E8C
calloc	401E94
free	401E9C
SetUnhandledExceptionFilter	401EA4
ExitProcess	401EAC
GetModuleHandleA	401EB4
GetProcAddress	401EBC
VirtualQuery	401EC4
VirtualProtect	401ECC
EnterCriticalSection	401ED4
TlsGetValue	401EDC
GetLastError	401EE4
LeaveCriticalSection	401EEC
DeleteCriticalSection	401EF4
InitializeCriticalSection	401EFC

Interesting Text:
_Jv_REgisterClasses Enter password This Week’s IRC info: ThisPasswordSux! Press [Enter] to continue Mingw runtime failure: \n VirtualQuery failed for %d bytes at address %p Unknown pseudo relocation protocol version %d. \n Unknown pseudo relocation bit size %d. \n

Analyze a Suspicious File

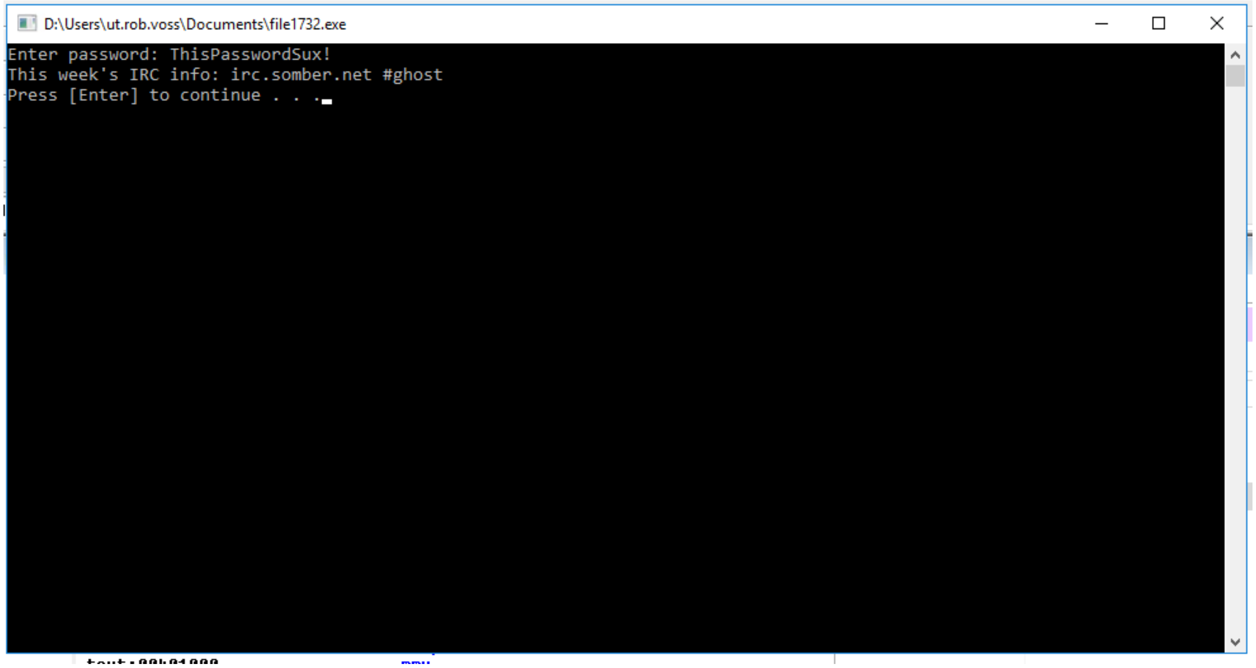
2 Running the Binary

Enter the password: ThisPasswordSux!



```
Enter password: ThisPasswordSux!
```

Press enter



```
Enter password: ThisPasswordSux!
This week's IRC info: irc.somber.net #ghost
Press [Enter] to continue . . .
```

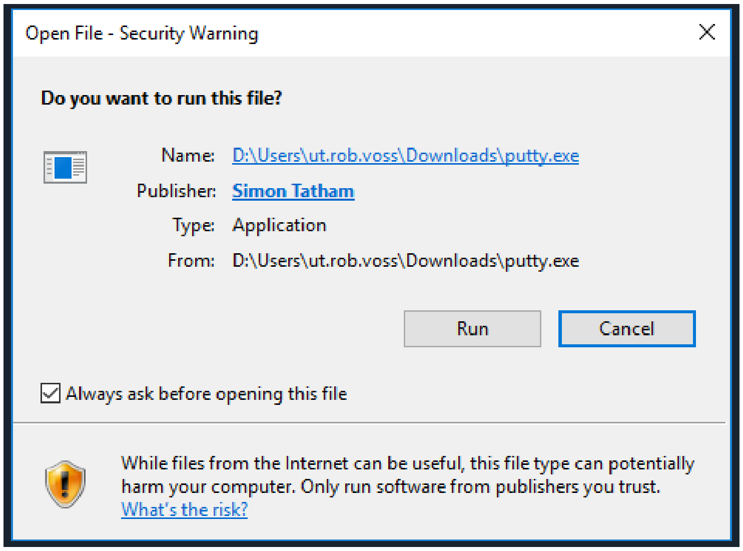
Entering the password, you get: This week’s IRC info: irc.somber.net #ghost

When you follow the command press enter the command prompt window vanishes…

Analyze a Suspicious File

3 Connecting to the IRC Channel

3.1 Run PuTTY



Do you want to run this file?

Name: D:\Users\ut.rob.voss\Downloads\putty.exe

Publisher: **Simon Tatham**

Type: Application

From: D:\Users\ut.rob.voss\Downloads\putty.exe

☑ Always ask before opening this file

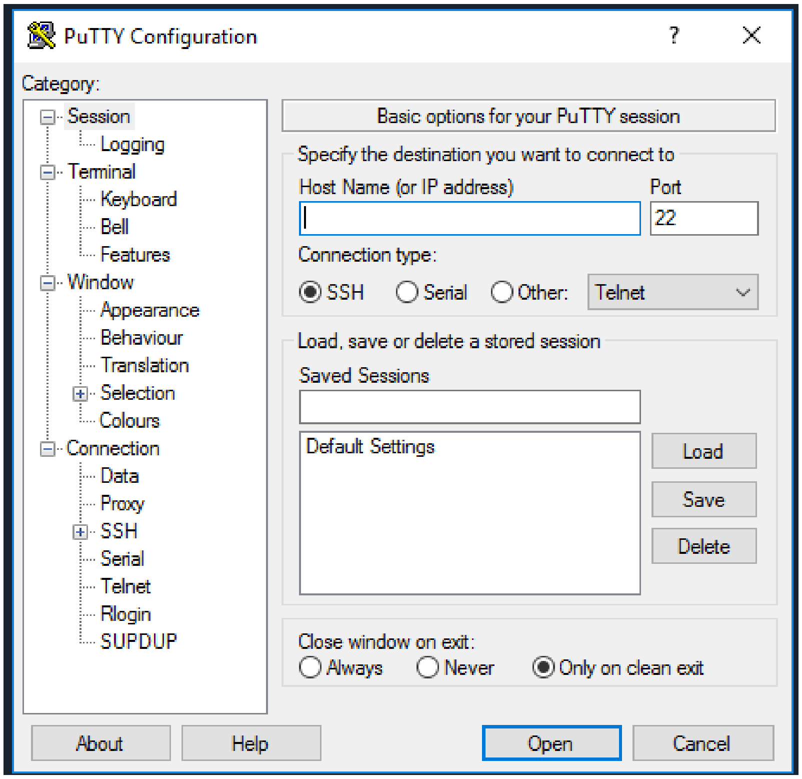
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

IP: 10.0.100.30

Username: travler2721

Password: EuD3jwtre4jGlEt07Tej

Analyze a Suspicious File

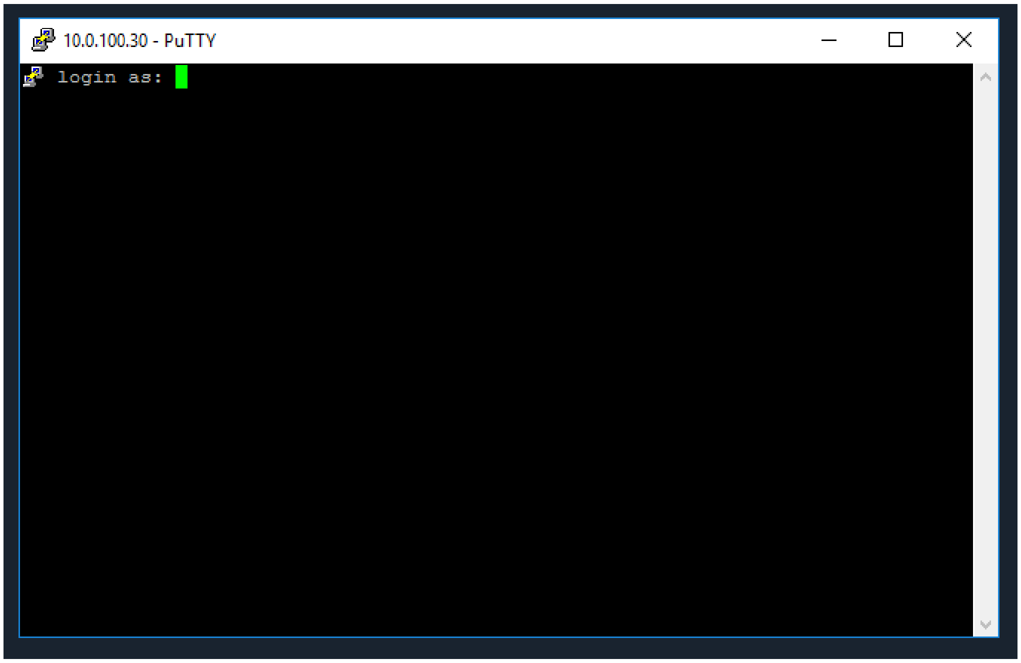


Host Name (or IP address):

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

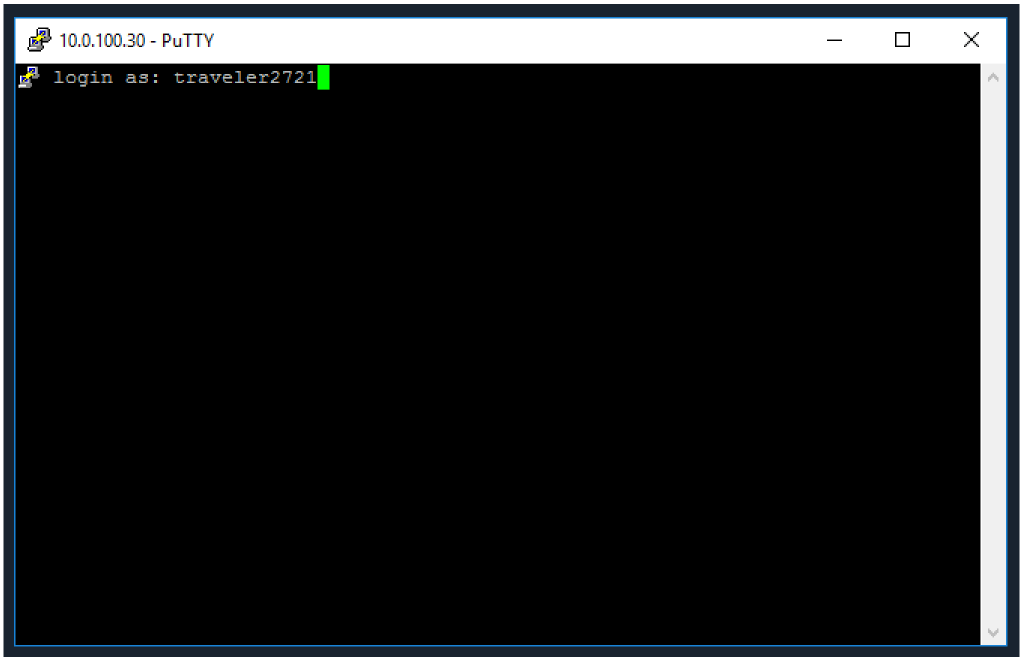
Close window on exit: ○ Always ○ Never ● Only on clean exit



```
login as:
```

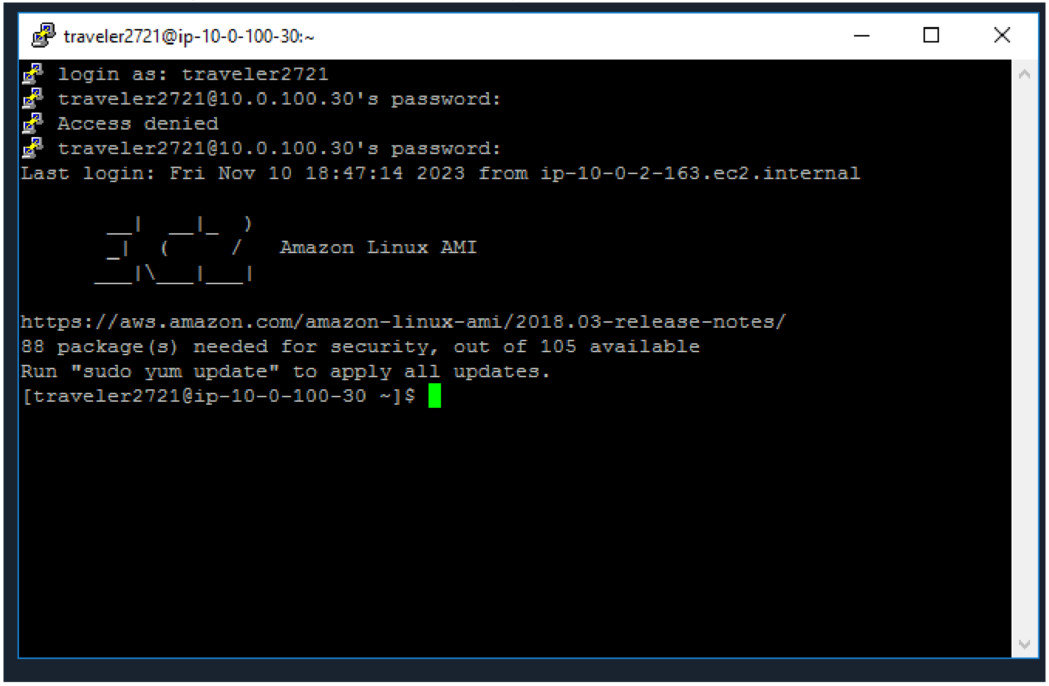
Input Username (right click on the mouse will paste in Linux) and hit enter.

Analyze a Suspicious File



```
login as: traveler2721
```

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



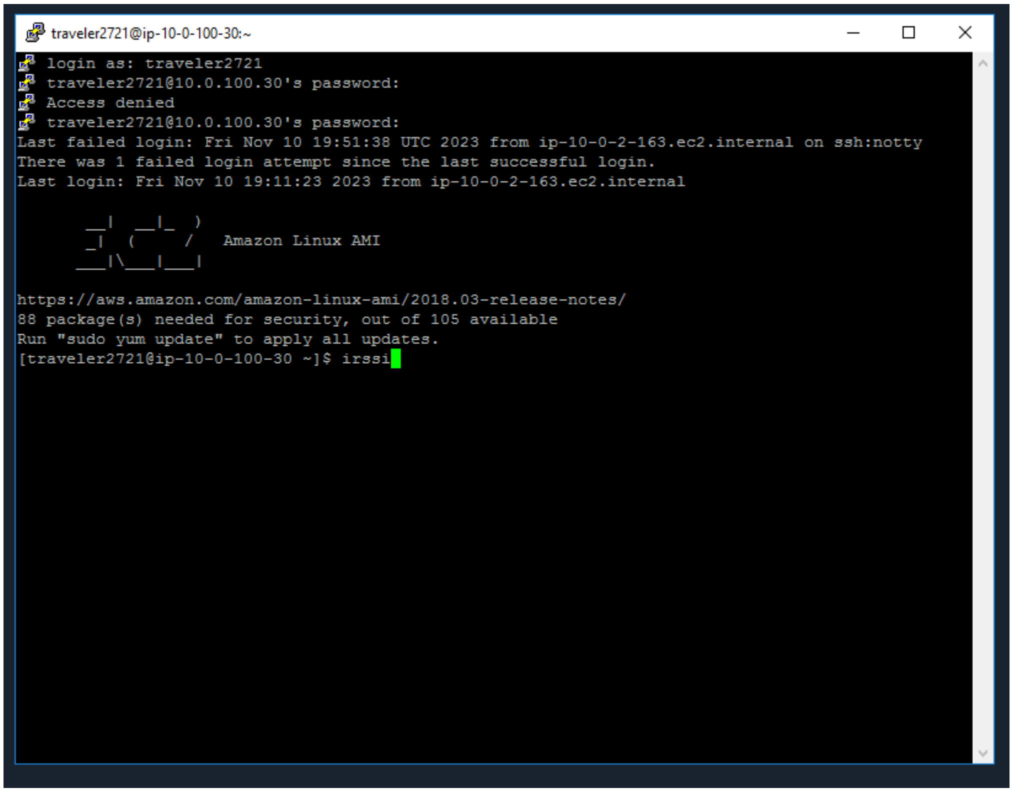
```
login as: traveler2721
traveler2721@10.0.100.30's password:
Access denied
traveler2721@10.0.100.30's password:
Last login: Fri Nov 10 18:47:14 2023 from ip-10-0-2-163.ec2.internal

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
88 package(s) needed for security, out of 105 available
Run "sudo yum update" to apply all updates.
[traveler2721@ip-10-0-100-30 ~]$
```

Analyze a Suspicious File

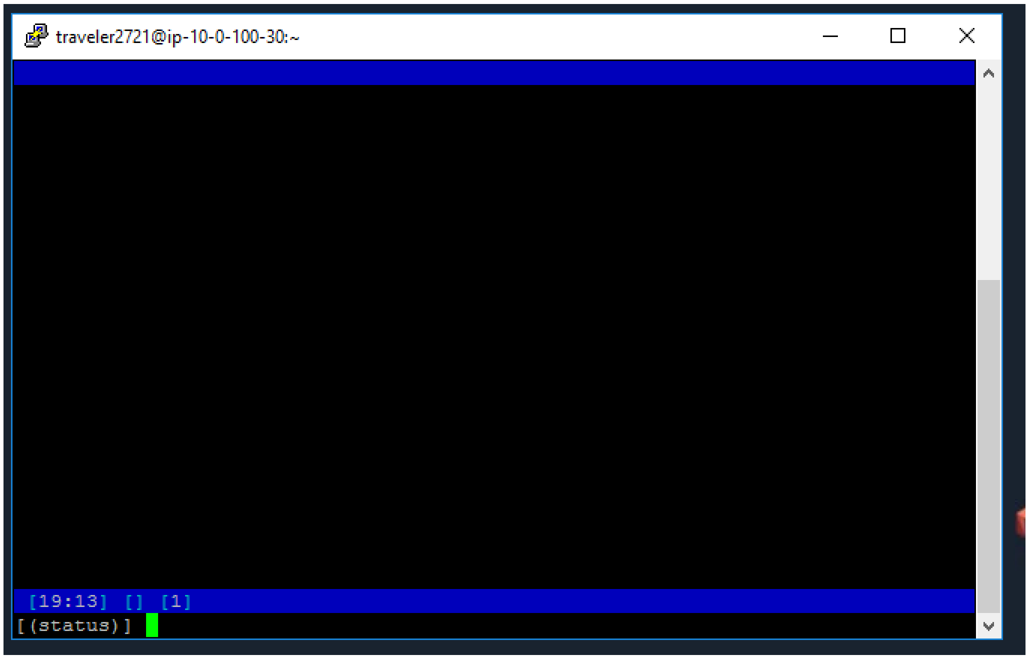
Input irssi and hit enter



```
login as: traveler2721
traveler2721@10.0.100.30's password:
Access denied
traveler2721@10.0.100.30's password:
Last failed login: Fri Nov 10 19:51:38 UTC 2023 from ip-10-0-2-163.ec2.internal on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Fri Nov 10 19:11:23 2023 from ip-10-0-2-163.ec2.internal

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
88 package(s) needed for security, out of 105 available
Run "sudo yum update" to apply all updates.
[traveler2721@ip-10-0-100-30 ~]$ irssi
```

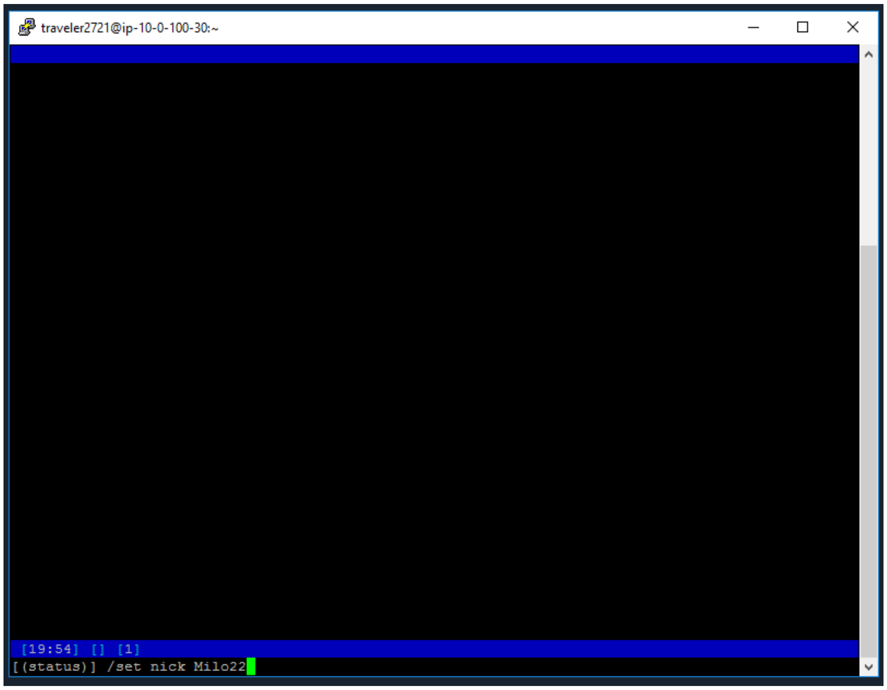


```
 [19:13] [] [1]
[(status)]
```

Analyze a Suspicious File

3.2 Set nickname

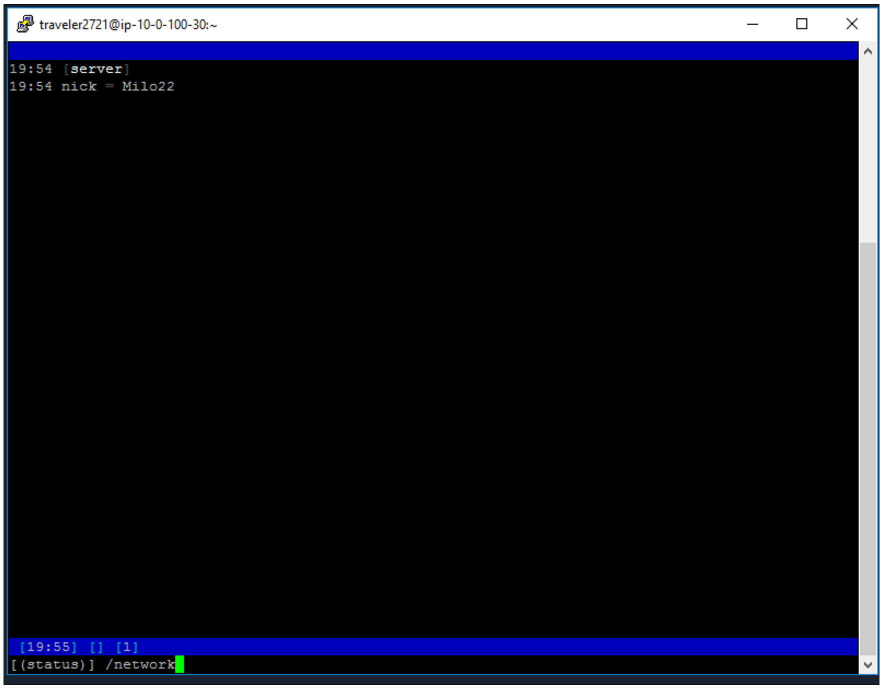
Set nick Milo22



```
[19:54] [] [1]
[(status)] /set nick Milo22
```

3.3 Request network list

network



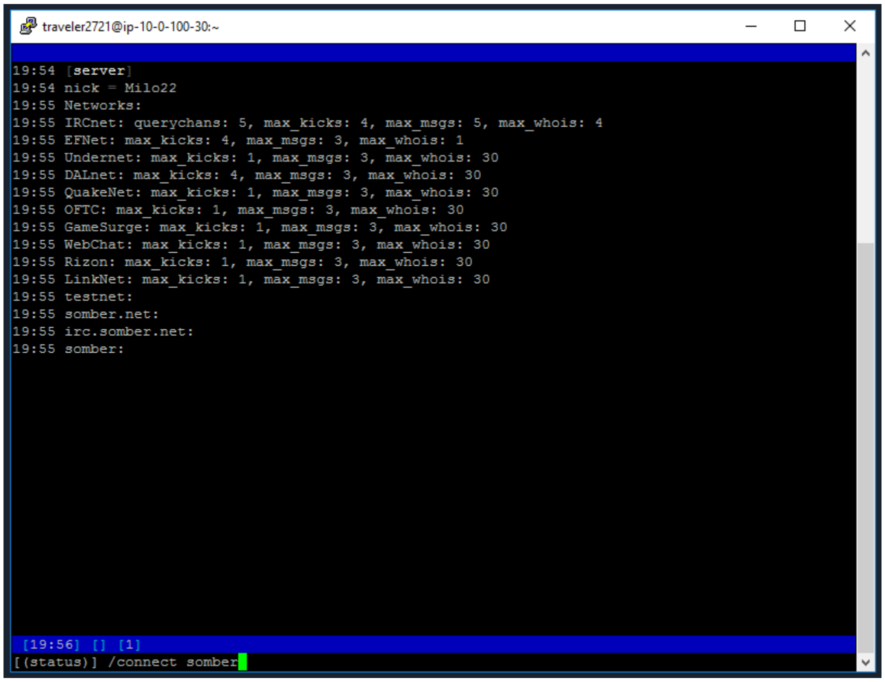
```
19:54 [server]
19:54 nick = Milo22
```

```
[19:55] [] [1]
[(status)] /network
```

Analyze a Suspicious File

3.4 Connect to network

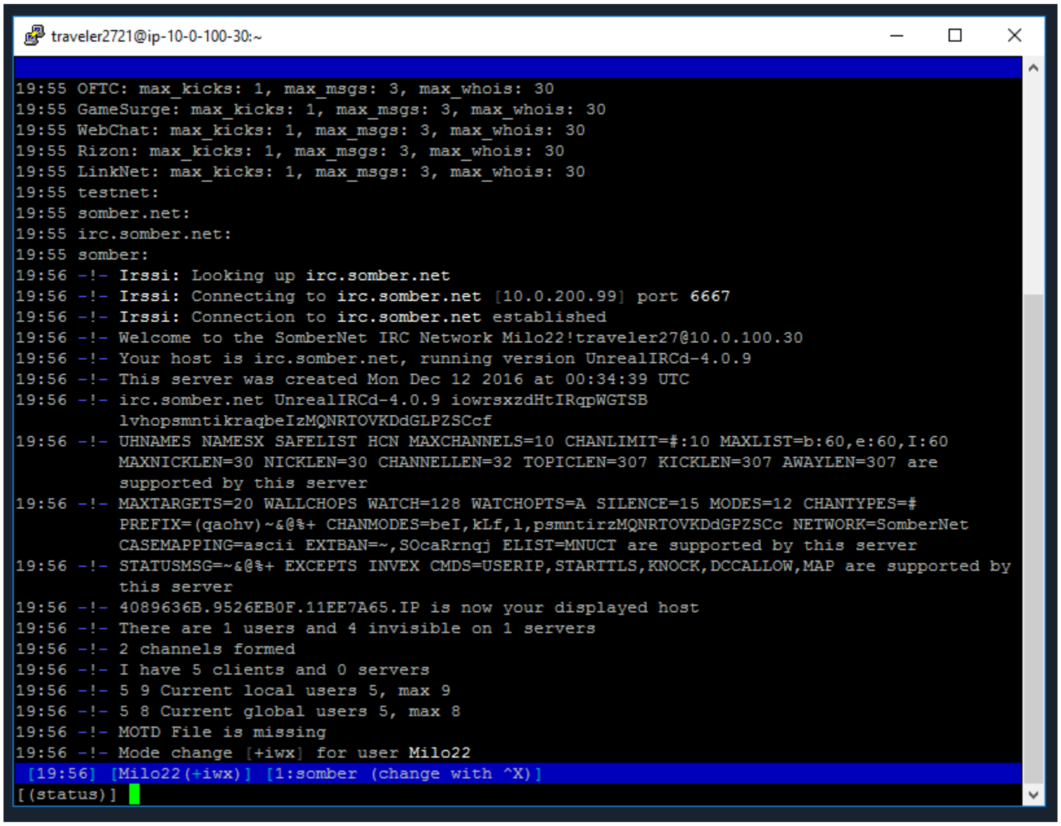
Connect somber



traveler2721@ip-10-0-100-30:~

```
19:54 [server]
19:54 nick = Milo22
19:55 Networks:
19:55 IRCnet: querychans: 5, max_kicks: 4, max_msgs: 5, max_whois: 4
19:55 EFNet: max_kicks: 4, max_msgs: 3, max_whois: 1
19:55 Undernet: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 DALnet: max_kicks: 4, max_msgs: 3, max_whois: 30
19:55 QuakeNet: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 OFTC: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 GameSurge: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 WebChat: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 Rizon: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 LinkNet: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 testnet:
19:55 somber.net:
19:55 irc.somber.net:
19:55 somber:

 [19:56] [] [1]
[(status)] /connect somber
```



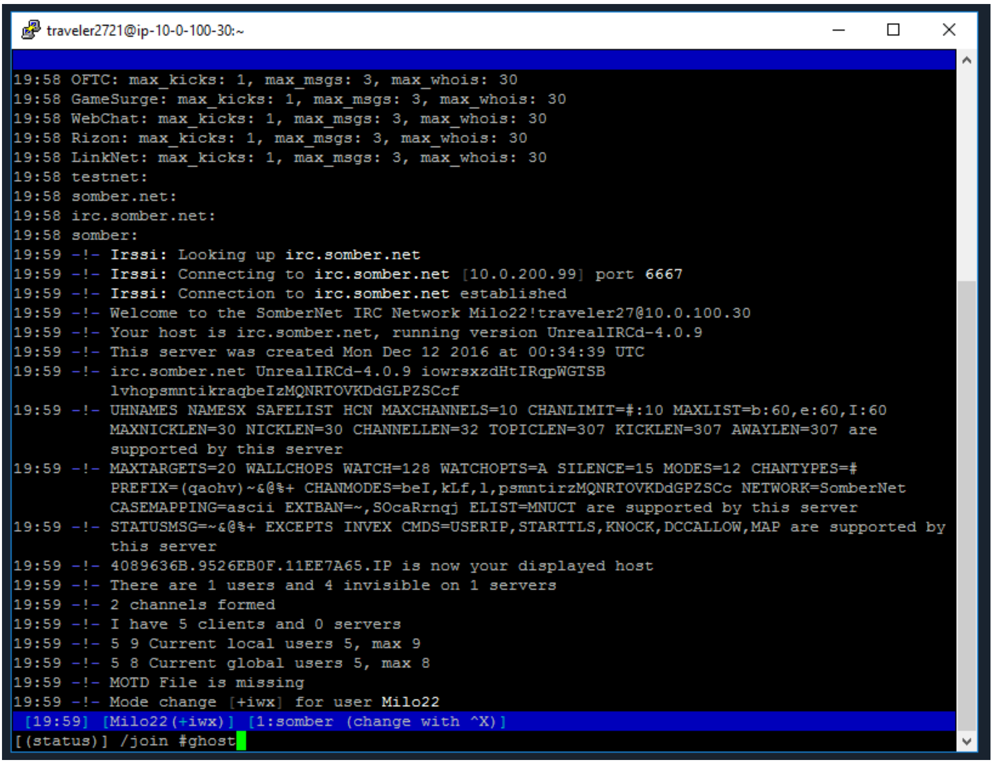
traveler2721@ip-10-0-100-30:~

```
19:55 OFTC: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 GameSurge: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 WebChat: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 Rizon: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 LinkNet: max_kicks: 1, max_msgs: 3, max_whois: 30
19:55 testnet:
19:55 somber.net:
19:55 irc.somber.net:
19:55 somber:
19:56 -!- Irssi: Looking up irc.somber.net
19:56 -!- Irssi: Connecting to irc.somber.net [10.0.200.99] port 6667
19:56 -!- Irssi: Connection to irc.somber.net established
19:56 -!- Welcome to the SomberNet IRC Network Milo22!traveler27@10.0.100.30
19:56 -!- Your host is irc.somber.net, running version UnrealIRCd-4.0.9
19:56 -!- This server was created Mon Dec 12 2016 at 00:34:39 UTC
19:56 -!- irc.somber.net UnrealIRCd-4.0.9 iowrsxzdHtIRqpWGTSB
          lvhopsmntikraqbeIzMQNRTOVKDdGLPZSCcf
19:56 -!- UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60
          MAXNICKLEN=30 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 are
          supported by this server
19:56 -!- MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=#
          PREFIX=(qaohv)~&@%+ CHANMODES=beI,kLf,l,psmntirzMQNRTOVKDdGPZSCc NETWORK=SomberNet
          CASEMAPPING=ascii EXTBAN=~,SOcaRrnqj ELIST=MNUCT are supported by this server
19:56 -!- STATUSMSG=~&@%+ EXCEPTS INVEX CMDS=USERIP,STARTTLS,KNOCK,DCCALLOW,MAP are supported by
          this server
19:56 -!- 4089636B.9526EB0F.11EE7A65.IP is now your displayed host
19:56 -!- There are 1 users and 4 invisible on 1 servers
19:56 -!- 2 channels formed
19:56 -!- I have 5 clients and 0 servers
19:56 -!- 5 9 Current local users 5, max 9
19:56 -!- 5 8 Current global users 5, max 8
19:56 -!- MOTD File is missing
19:56 -!- Mode change [+iwx] for user Milo22
 [19:56] [Milo22(+iwx)] [1:somber (change with ^X)]
[(status)]
```

Analyze a Suspicious File

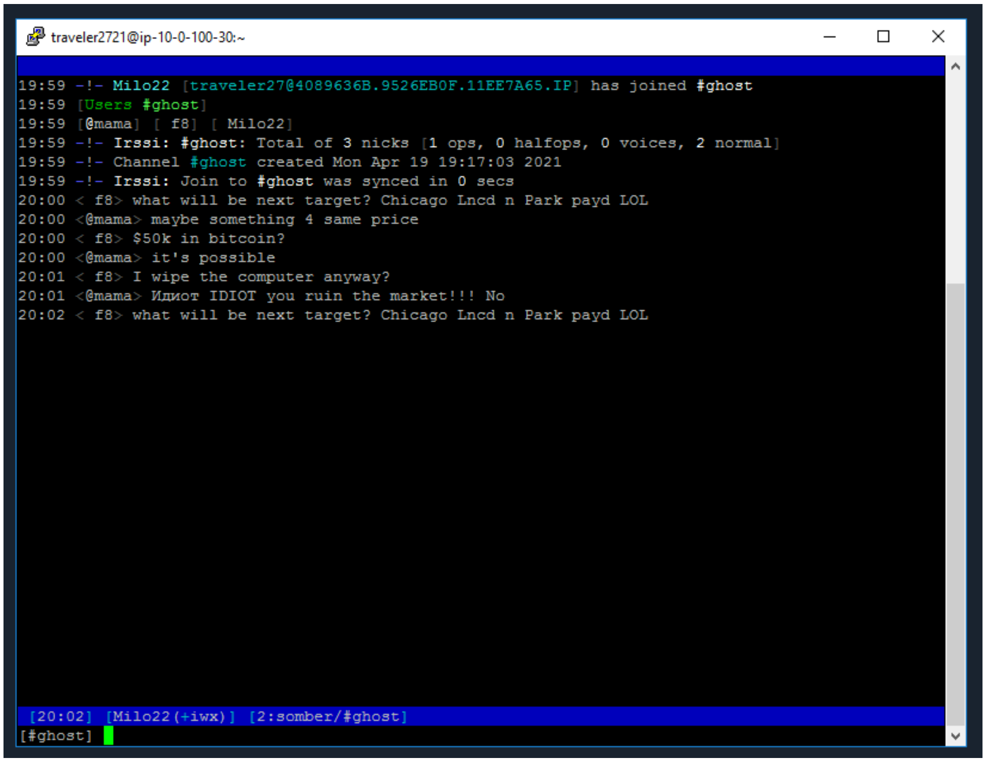
3.5 Join #ghost

join #ghost



```
19:58 OFTC: max_kicks: 1, max_msgs: 3, max_whois: 30
19:58 GameSurge: max_kicks: 1, max_msgs: 3, max_whois: 30
19:58 WebChat: max_kicks: 1, max_msgs: 3, max_whois: 30
19:58 Rizon: max_kicks: 1, max_msgs: 3, max_whois: 30
19:58 LinkNet: max_kicks: 1, max_msgs: 3, max_whois: 30
19:58 testnet:
19:58 somber.net:
19:58 irc.somber.net:
19:58 somber:
19:59 -!- Irssi: Looking up irc.somber.net
19:59 -!- Irssi: Connecting to irc.somber.net [10.0.200.99] port 6667
19:59 -!- Irssi: Connection to irc.somber.net established
19:59 -!- Welcome to the SomberNet IRC Network Milo22!traveler27@10.0.100.30
19:59 -!- Your host is irc.somber.net, running version UnrealIRCd-4.0.9
19:59 -!- This server was created Mon Dec 12 2016 at 00:34:39 UTC
19:59 -!- irc.somber.net UnrealIRCd-4.0.9 iowrsxzdHtIRqpWGTSB
          lvhopsmntikraqbeIzMQNRTOVKDdGLPZSCcf
19:59 -!- UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60
          MAXNICKLEN=30 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 are
          supported by this server
19:59 -!- MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=#
          PREFIX=(qaohv)~&@%+ CHANMODES=beI,kLf,l,psmntirzMQNRTOVKDdGPZSCc NETWORK=SomberNet
          CASEMAPPING=ascii EXTBAN=~,SOcaRrnqj ELIST=MNUCT are supported by this server
19:59 -!- STATUSMSG=~&@%+ EXCEPTS INVEX CMDS=USERIP,STARTTLS,KNOCK,DCCALLOW,MAP are supported by
          this server
19:59 -!- 4089636B.9526EB0F.11EE7A65.IP is now your displayed host
19:59 -!- There are 1 users and 4 invisible on 1 servers
19:59 -!- 2 channels formed
19:59 -!- I have 5 clients and 0 servers
19:59 -!- 5 9 Current local users 5, max 9
19:59 -!- 5 8 Current global users 5, max 8
19:59 -!- MOTD File is missing
19:59 -!- Mode change [+iwx] for user Milo22
 [19:59] [Milo22(+iwx)] [1:somber (change with ^X)]
[(status)] /join #ghost
```

3.6 Observe conversation



```
19:59 -!- Milo22 [traveler27@4089636B.9526EB0F.11EE7A65.IP] has joined #ghost
19:59 [Users #ghost]
19:59 [@mama] [ f8] [ Milo22]
19:59 -!- Irssi: #ghost: Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2 normal]
19:59 -!- Channel #ghost created Mon Apr 19 19:17:03 2021
19:59 -!- Irssi: Join to #ghost was synced in 0 secs
20:00 < f8> what will be next target? Chicago Lncd n Park payd LOL
20:00 <@mama> maybe something 4 same price
20:00 < f8> $50k in bitcoin?
20:00 <@mama> it's possible
20:01 < f8> I wipe the computer anyway?
20:01 <@mama> Идиот IDIOT you ruin the market!!! No
20:02 < f8> what will be next target? Chicago Lncd n Park payd LOL













 [20:02] [Milo22(+iwx)] [2:somber/#ghost]
[#ghost]
```

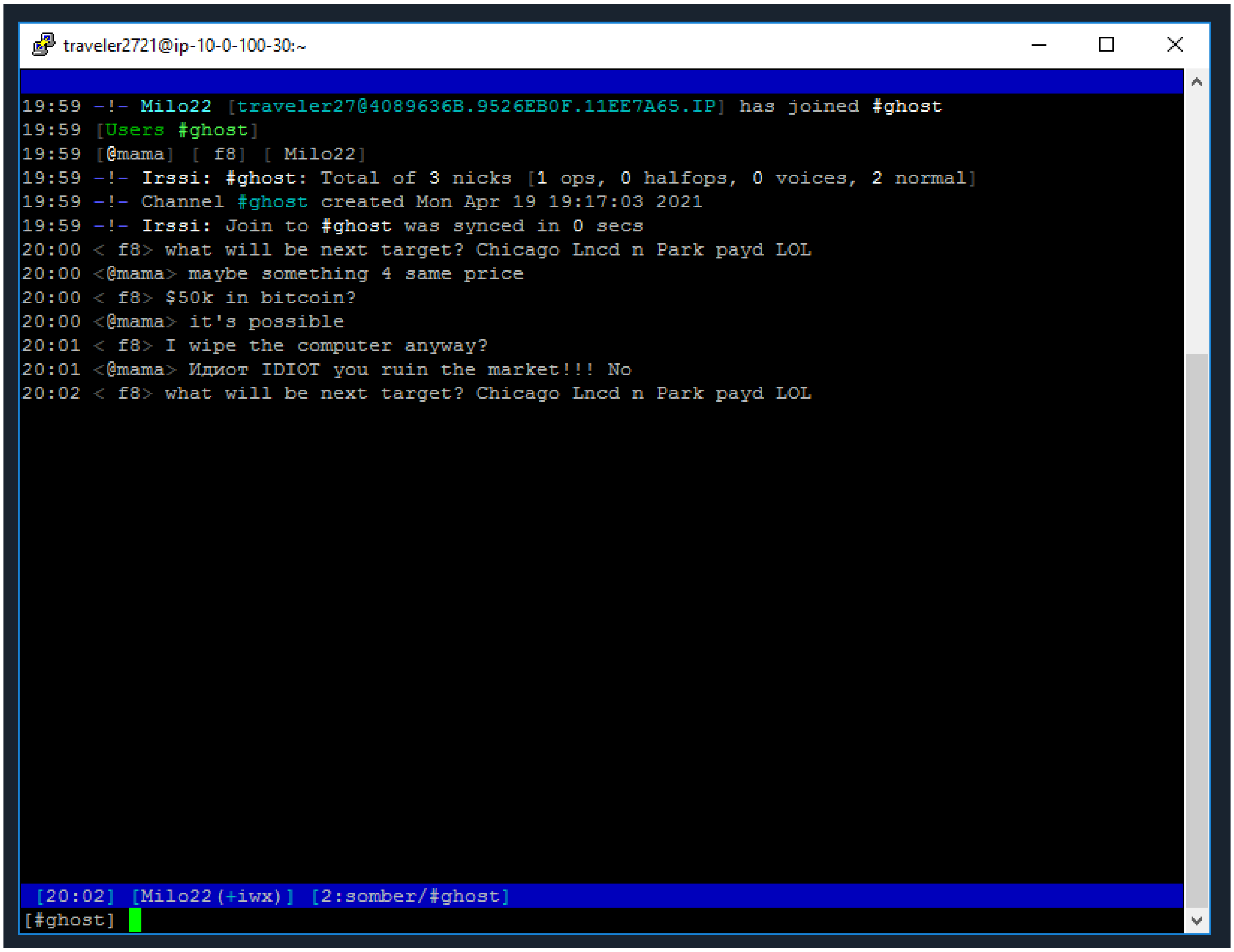
See who the players are:
Other players noted are @mama and f8

3.7 Eavesdrop on the IRC channel

irc.somber.net #ghost

This appears to be 2x Russians that have done a ransomware on Chicago Land and Parks for $50k in bitcoin.
The one player, f8 wanted to wipe their computers anyway even after collecting the ransom but the second player @mama said no as it would harm the market…if you wipe them anyway, then future victims won't pay…

I would suggest continuing to monitor them as they are talking about who's next, but haven't said yet…



```
19:59 -!- Milo22 [traveler27@4089636B.9526EB0F.11EE7A65.IP] has joined #ghost
19:59 [Users #ghost]
19:59 [@mama] [ f8] [ Milo22]
19:59 -!- Irssi: #ghost: Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2 normal]
19:59 -!- Channel #ghost created Mon Apr 19 19:17:03 2021
19:59 -!- Irssi: Join to #ghost was synced in 0 secs
20:00 < f8> what will be next target? Chicago Lncd n Park payd LOL
20:00 <@mama> maybe something 4 same price
20:00 < f8> $50k in bitcoin?
20:00 <@mama> it's possible
20:01 < f8> I wipe the computer anyway?
20:01 <@mama> Идиот IDIOT you ruin the market!!! No
20:02 < f8> what will be next target? Chicago Lncd n Park payd LOL











 [20:02] [Milo22(+iwx)] [2:somber/#ghost]
[#ghost]
```