Øving 21 - Game Expolit

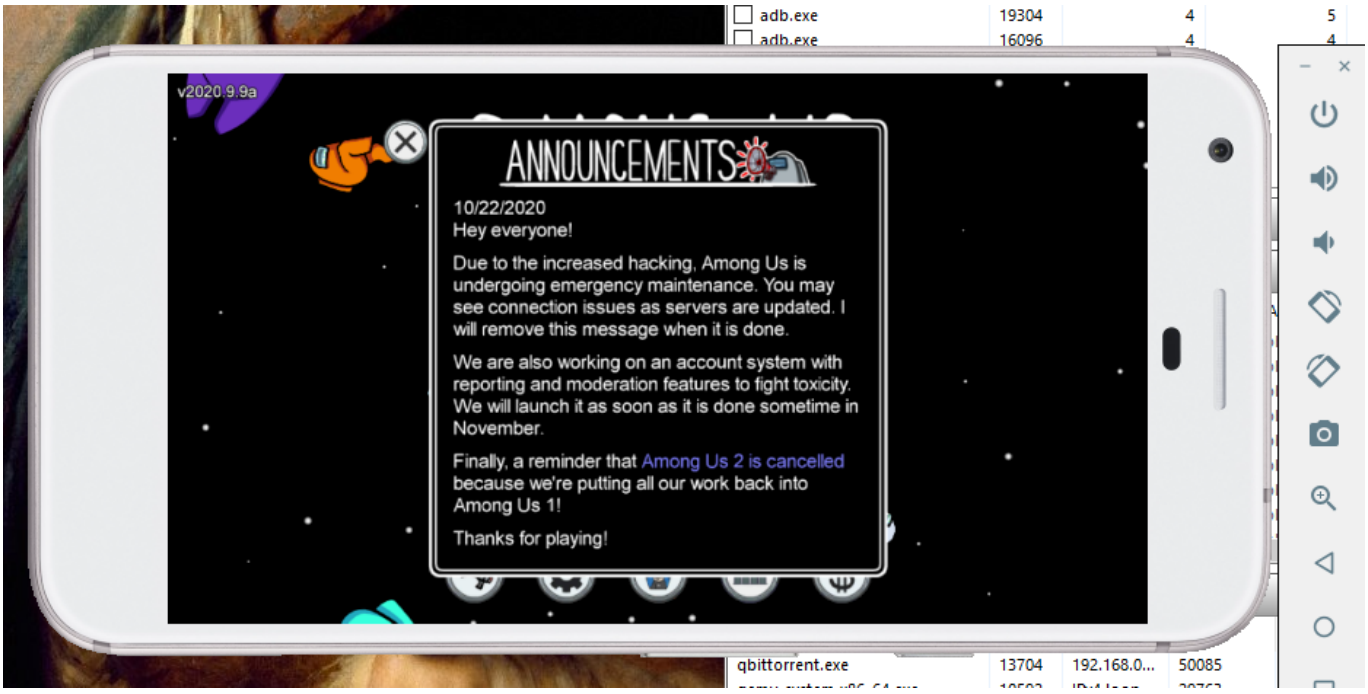
```
Finne mulige problemer i en fritt valgt nettverksprotokoll

Det er etterhvert mye programvare som kommuniserer over nett, ofte mot en sen-tral
server eller skytjeneste.

Bruk pakkesniffer, se om dere kan finne ut nok omen slik kommunikasjonsprotokoll
til å ihvertfall kunne foreslå hvordan den kantrikses med.Ta f.eks. et eller annet
mobil-spill.

Se på hva som overføres, se om dere finnernoe dere kjenner igjen fra spillet. Hvis
dere kunne endre kommunikasjonen fritt, kunne dere f.eks. skaffet fordeler i
spillet, eller jukset med highscore-lista?

Ser dere noe mottiltak?
```

Among Us

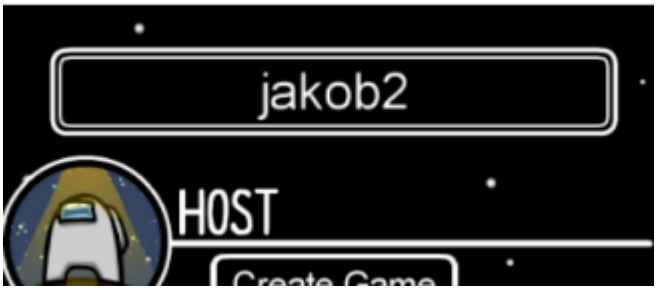
Starter en Virtuell Android Emulator.

Installerer Among Us APK

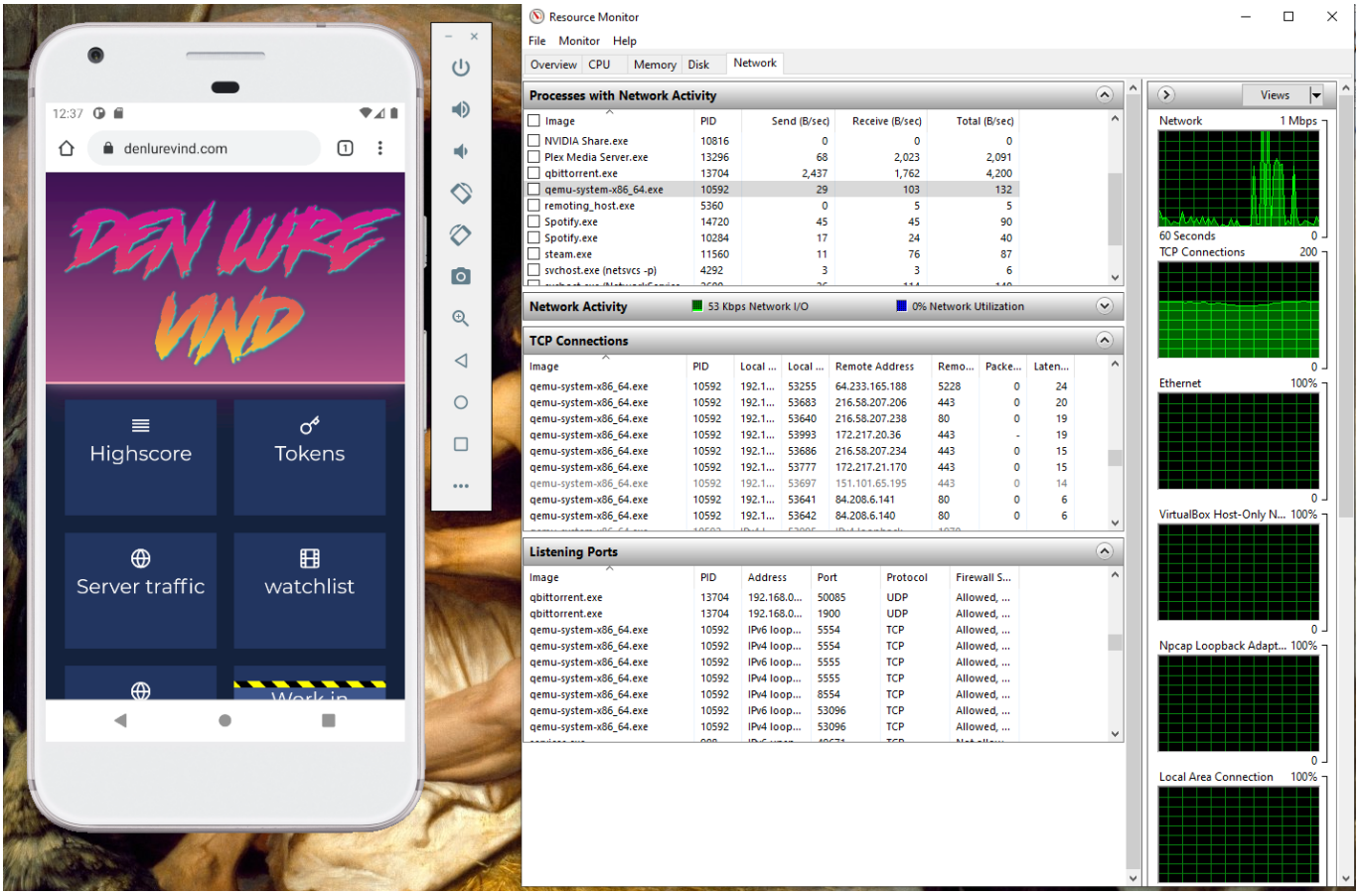
Da jeg starter spillet får jeg melding om at det er mange hackers som spiller...



Starter med å lage et brukernavn



Da jeg er på windows bruker jeg Resource Monitor til å se alle koblingene til emulator prosessen



Jeg tar dermed nslookup for å se om det er noen interresante ip'er

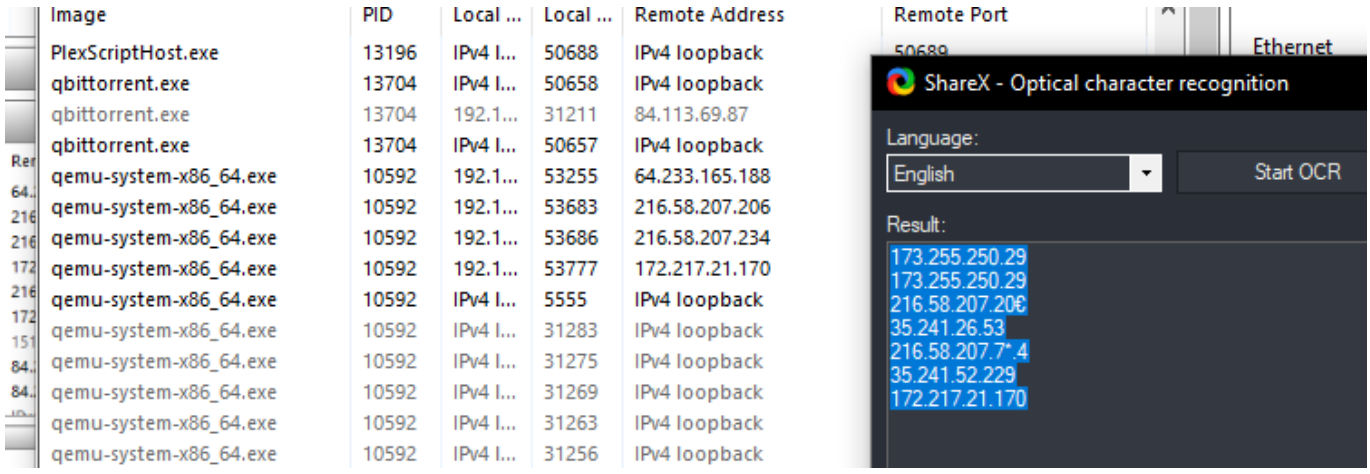


Image	PID	Local ...	Local ...	Remote Address	Remote Port
PlexScriptHost.exe	13196	IPv4 l...	50688	IPv4 loopback	
qbittorrent.exe	13704	IPv4 l...	50658	IPv4 loopback	
qbittorrent.exe	13704	192.1...	31211	84.113.69.87	
qbittorrent.exe	13704	IPv4 l...	50657	IPv4 loopback	
qemu-system-x86_64.exe	10592	192.1...	53255	64.233.165.188	
qemu-system-x86_64.exe	10592	192.1...	53683	216.58.207.206	
qemu-system-x86_64.exe	10592	192.1...	53686	216.58.207.234	
qemu-system-x86_64.exe	10592	192.1...	53777	172.217.21.170	
qemu-system-x86_64.exe	10592	IPv4 l...	5555	IPv4 loopback	
qemu-system-x86_64.exe	10592	IPv4 l...	31283	IPv4 loopback	
qemu-system-x86_64.exe	10592	IPv4 l...	31275	IPv4 loopback	
qemu-system-x86_64.exe	10592	IPv4 l...	31269	IPv4 loopback	
qemu-system-x86_64.exe	10592	IPv4 l...	31263	IPv4 loopback	
qemu-system-x86_64.exe	10592	IPv4 l...	31256	IPv4 loopback	

Ethernet

ShareX - Optical character recognition

Language:

English

Start OCR

Result:

173.255.250.29
173.255.250.29
216.58.207.20€
35.241.26.53
216.58.207.7*.4
35.241.52.229
172.217.21.170

```
C:\Users\Jakob>nslookup 173.255.250.29
Server:  dnscache01.get.no
Address:  84.208.20.110

Name:    li260-29.members.linode.com
Address:  173.255.250.29
```

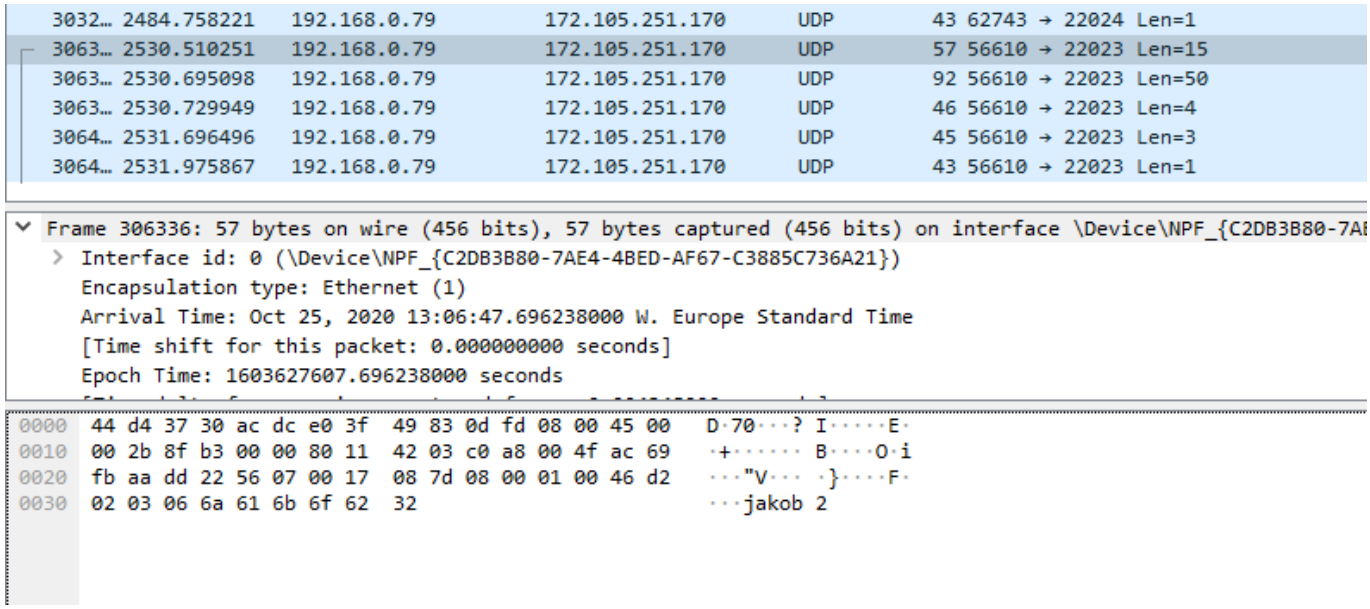
En Ip skiller seg ut da dette er hosten til en populær spill side

> li260-29.members.linode.com

Da jeg starter wireshark interface med filter:

> ip.dst == 172.105.251.170 || ip.src == 172.105.251.170

Finner jeg en pakke som inneholder mitt navn

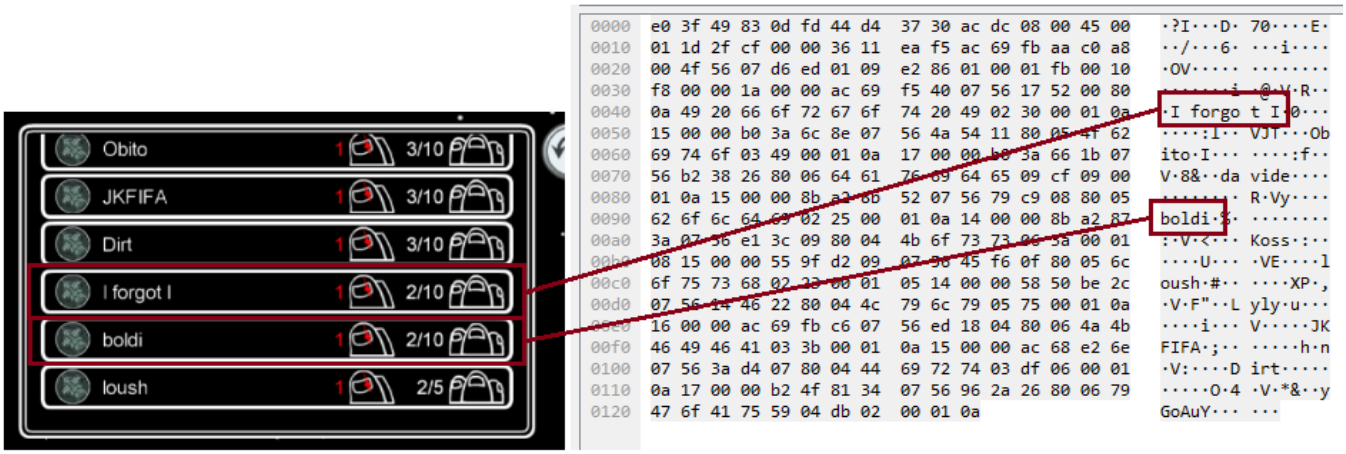


3032…	2484.758221	192.168.0.79	172.105.251.170	UDP	43 62743 → 22024 Len=1
3063…	2530.510251	192.168.0.79	172.105.251.170	UDP	57 56610 → 22023 Len=15
3063…	2530.695098	192.168.0.79	172.105.251.170	UDP	92 56610 → 22023 Len=50
3063…	2530.729949	192.168.0.79	172.105.251.170	UDP	46 56610 → 22023 Len=4
3064…	2531.696496	192.168.0.79	172.105.251.170	UDP	45 56610 → 22023 Len=3
3064…	2531.975867	192.168.0.79	172.105.251.170	UDP	43 56610 → 22023 Len=1

```
Frame 306336: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_{C2DB3B80-7AE
  Interface id: 0 (\Device\NPF_{C2DB3B80-7AE4-4BED-AF67-C3885C736A21})
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 25, 2020 13:06:47.696238000 W. Europe Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1603627607.696238000 seconds
```

```
0000  44 d4 37 30 ac dc e0 3f  49 83 0d fd 08 00 45 00   D·70···? I·····E·
0010  00 2b 8f b3 00 00 80 11  42 03 c0 a8 00 4f ac 69   ·+······ B····O·i
0020  fb aa dd 22 56 07 00 17  08 7d 08 00 01 00 46 d2   ···"V··· ·}····F·
0030  02 03 06 6a 61 6b 6f 62  32                       ···jakob 2
```

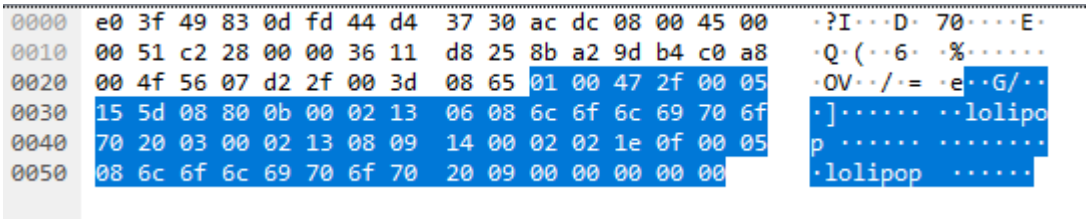
Da jeg åpner server lista får jeg også en plaintext pakke med alle instances.



Men da jeg kobler til en server slutter all trafikken, selve spillet anvender en annen server enn lobbyen.

Da jeg joiner en server holder jeg øye på hvilke nye Ip'er som dukker opp i Resource manager.

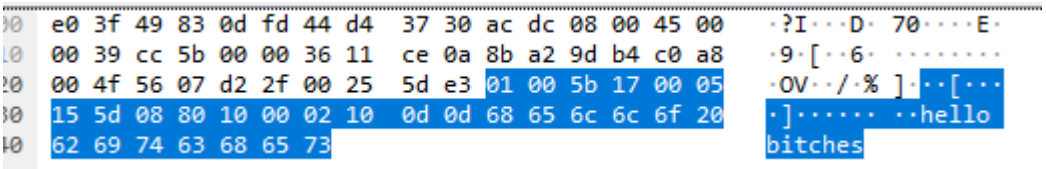
Inne i lobbyen er det andre spillere som kommer inn fortløpende, jeg fant igjen en pakke med navnet til en ny spiller.



Vi ser her at navnet `lolipop` er på vei inn.

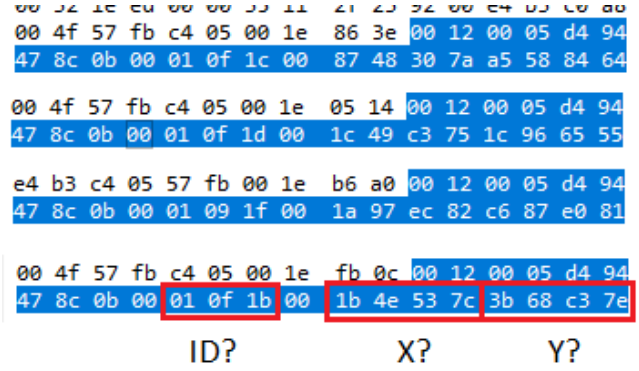
Ikke lenge etter dukker det opp en spiller med det navnet.

Vi har også tilgang til å chatte med hverandre via ingame chat.



Etter å analysere pakkene ser det ut som spillet bruker "ticks", posisjonen til alle spillerene blir oppdatert på et gitt interval. Ved å se på alle pakkene ser vi et klart mønster. De inneholder antaglivis spiller id og posisjon.

Dersom vi gjør hex dataen om til tall før vi noe som kan se ut som x og y verdier.




```
pos = [[0x8748307a, 0xa5588464],
       [0x1c49c375, 0x1c966555],
       [0x1a97ec82, 0xc687e081],
       [0x1b4e537c, 0x3b68c37e]]

ids = [0x0f1c,
       0x0f1d,
       0x091f,
       0x0f1b]
```

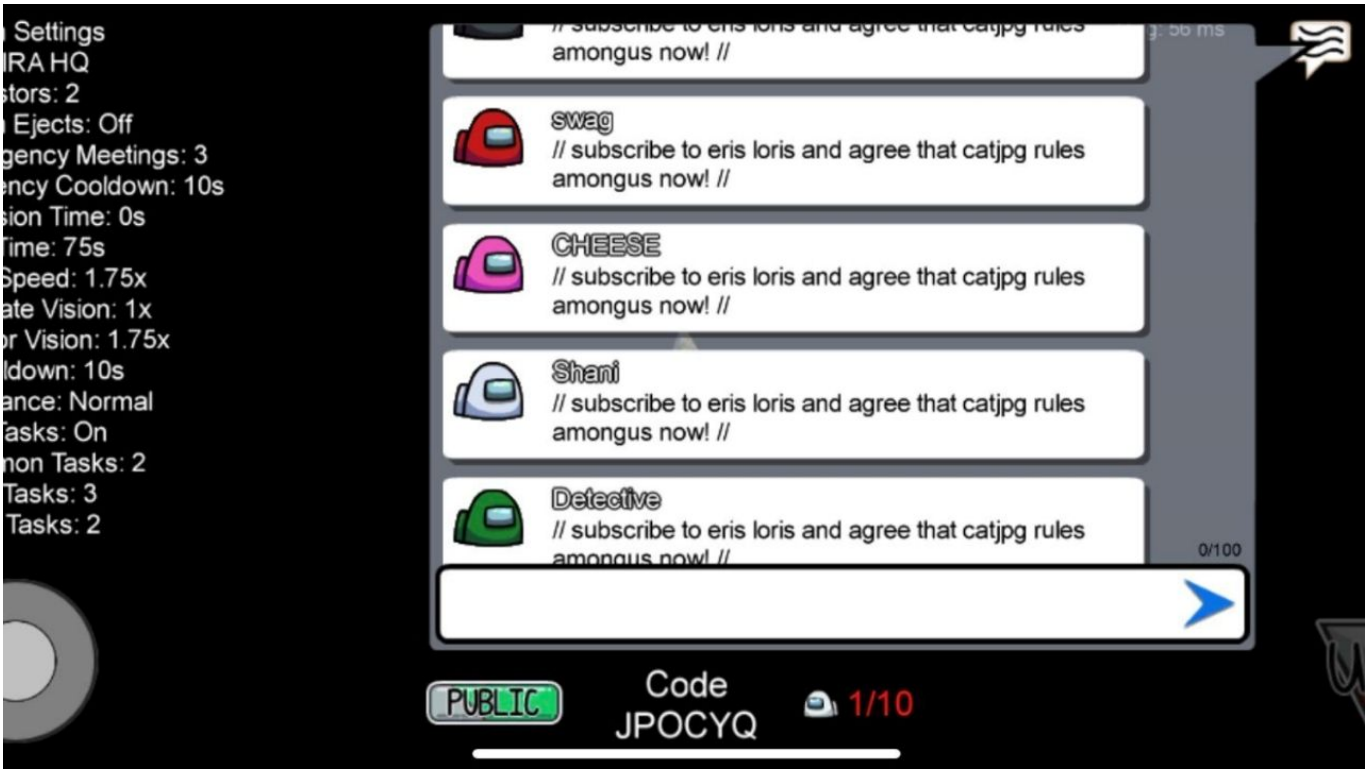
```
3868
x 2269655162
y 2774041700

3869
x 474596213
y 479618389

2335
x 446164098
y 3330793601

3867
x 458118012
y 996721534
```

Hvis serveren ikke autentiserer denne informasjonen kan man i teorien teleportere rundt på kartet. En fiks på dette hadde vært å sjekke ny posisjon mot gammel posisjon, dersom det ikke er mulig å komme seg fra A til B på en gitt tid kan man si at spilleren jukser.

Konklusjon

Dersom dette spillet har økt i popularitet har de økt fokuset på å sikre serverside autentisering slik at det er vanskelig for en klient å påvirke spillet.

Men man kan se flere eksempler på dette i det siste hvor noen har klart å få andre i spillet til å sende meldinger.




jakob2 was The Impostor.