Billions of Blocks

This video of a Minecraft Java Edition world was briefly streamed online. We would like to recover the seed using only the little information we know. We know the world was generated with a string that starts with "S41NTC0N " and is followed by a lowercase English word. Can you crack the non-numeric seed used to generate this world?

Please note, you do not need to own Minecraft to solve this challenge.

For example, some possible answers include:

- "S41NTC0N password"
- "S41NTC0N banana"
- "S41NTC0N hypothetically"

So we are given a video of someone playing minecraft. We are asked to reverse engineer the seed from information gleaned from the video.

Fun fact, there are 2^64 (18,446,744,073,709,551,616) minecraft seeds.

So there are 2 problems.

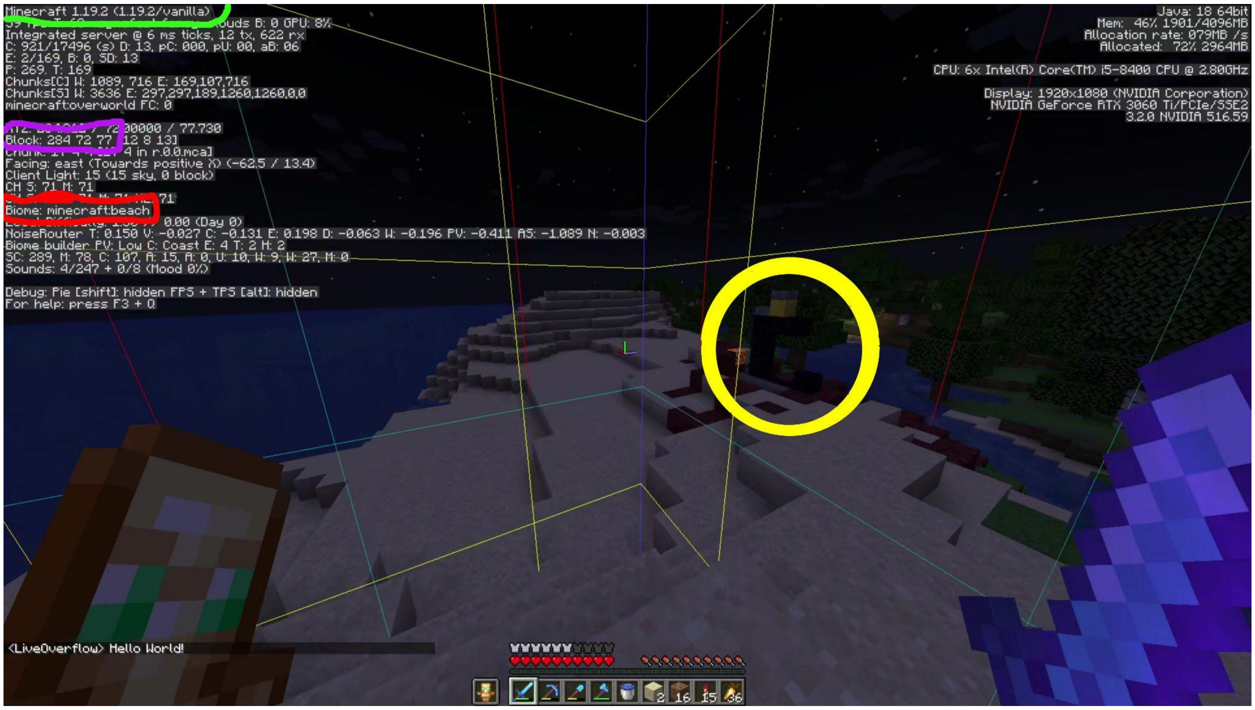
1. Identify the seed used.
2. Correlate the seed to the word.

One saving grace is that when you use a string to generate a world seed, it uses the java hashcode() function. hashcode() returns a 2^32 (4294967296) but it is signed. (−2,147,483,648 through 2,147,483,647)

So let’s take a look at what information we can get.

Let’s take a look at a frame from the video.

The player is running with the F3 debug screen on. It is also running with the F3-B showing the chunk borders.



```
Minecraft 1.19.2 (1.19.2/vanilla)
ouds B: 0 GPU: 8%
Integrated server @ 6 ms ticks, 12 tx, 622 rx
C: 921/17496 (s) D: 13, pC: 000, pU: 00, aB: 06
E: 2/169, B: 0, SD: 13
P: 269. T: 169
Chunks[C] W: 1089, 716 E: 169,107,716
Chunks[S] W: 3636 E: 297,297,189,1260,1260,0,0
minecraft:overworld FC: 0

00000 / 77.730
Block: 284 72 77 [12 8 13]
4 in r.0.0.mca]
Facing: east (Towards positive X) (-62.5 / 13.4)
Client Light: 15 (15 sky, 0 block)
CH S: 71 M: 71
71
Biome: minecraft:beach
0.00 (Day 0)
NoiseRouter T: 0.150 V: -0.027 C: -0.131 E: 0.198 D: -0.063 W: -0.196 PV: -0.411 AS: -1.089 N: -0.003
Biome builder PV: Low C: Coast E: 4 T: 2 H: 2
SC: 289, M: 78, C: 107, A: 15, A: 0, U: 10, W: 9, W: 27, M: 0
Sounds: 4/247 + 0/8 (Mood 0%)

Debug: Pie [shift]: hidden FPS + TPS [alt]: hidden
For help: press F3 + Q
```

```
                           Java: 18 64bit
                  Mem:  46% 1901/4096MB
               Allocation rate: 079MB /s
                    Allocated:  72% 2964MB

CPU: 6x Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz

     Display: 1920x1080 (NVIDIA Corporation)
      NVIDIA GeForce RTX 3060 Ti/PCIe/SSE2
                        3.2.0 NVIDIA 516.59
```

```
<LiveOverflow> Hello World!
```

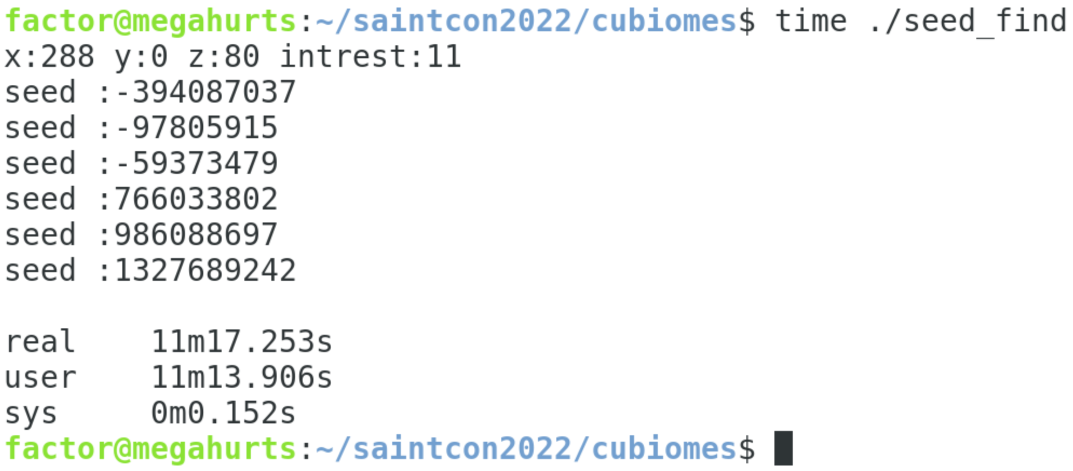
1st, in the green rectangle we see that it is running in version 1.19.2 . This is important because different versions of the game use different algorithms to generate the world.

2nd, in the yellow circle, there is a ruined portal. A ruined portal is generated during the world creation process. Portals are determined on a per chunk basis. This will be a structure that we will want to look at.

We can determine what chunk it is in. With just this knowledge we can limit it to 6871662 possible seeds or 0.16% of the keyspace. Still too many to work with.

3rd we are going to use the red and purple boxes which we can correlate a specific biome to specific blocks.

Let's add this first spot he is on. It reduces the amount of seeds to 165467.
Using a total of 7 spaces [(282,72,76,beach); (329,73,107,beach); (330,73,109,forest); (341,66,119,beach); (344,65,120,forest); (335,69,113,forest); (282,72,76,beach)] we reduce the seeds to 6.



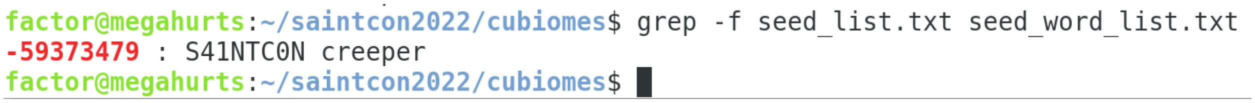
```
factor@megahurts:~/saintcon2022/cubiomes$ time ./seed_find
x:288 y:0 z:80 intrest:11
seed :-394087037
seed :-97805915
seed :-59373479
seed :766033802
seed :986088697
seed :1327689242

real	11m17.253s
user	11m13.906s
sys	0m0.152s
factor@megahurts:~/saintcon2022/cubiomes$ █
```

6 seeds we can validate by hand. (but for the sake of argument that we don't have minecraft installed we will pretend not to do that.)

So we have effectively solved the first problem. We have the seed for this world.

Now let's generate a list of possible solutions. We will concat "S41NTC0N " the contents of the file /usr/share/dict/american-english. We then run each of those though hashCode() and create a file full of hashes and strings. Note, I did sort by hash value.

-2147410947 : S41NTC0N Nootka's
-2147015982 : S41NTC0N clipboards
-2146919975 : S41NTC0N impolitic
.
.
.
2147474477 : S41NTC0N catacomb's
2147477636 : S41NTC0N trivets
2147480884 : S41NTC0N trivial



```
factor@megahurts:~/saintcon2022/cubiomes$ grep -f seed_list.txt seed_word_list.txt
-59373479 : S41NTC0N creeper
factor@megahurts:~/saintcon2022/cubiomes$ █
```

Links –
https://github.com/Cubitect/cubiomes // code used to locate biomes and structures
https://minecraft.fandom.com/wiki/Seed_(level_generation)#:~:text=Seed%20limit%20is%20now%2048%2Dbit.&text=World%20generator%20rewritten%20in%20a%20non%2Dbreaking%20way.&text=Replaced%20the%20random%20number%20generator,limit%20back%20to%2064%2Dbit. // info about world generation
They Cracked My Server!