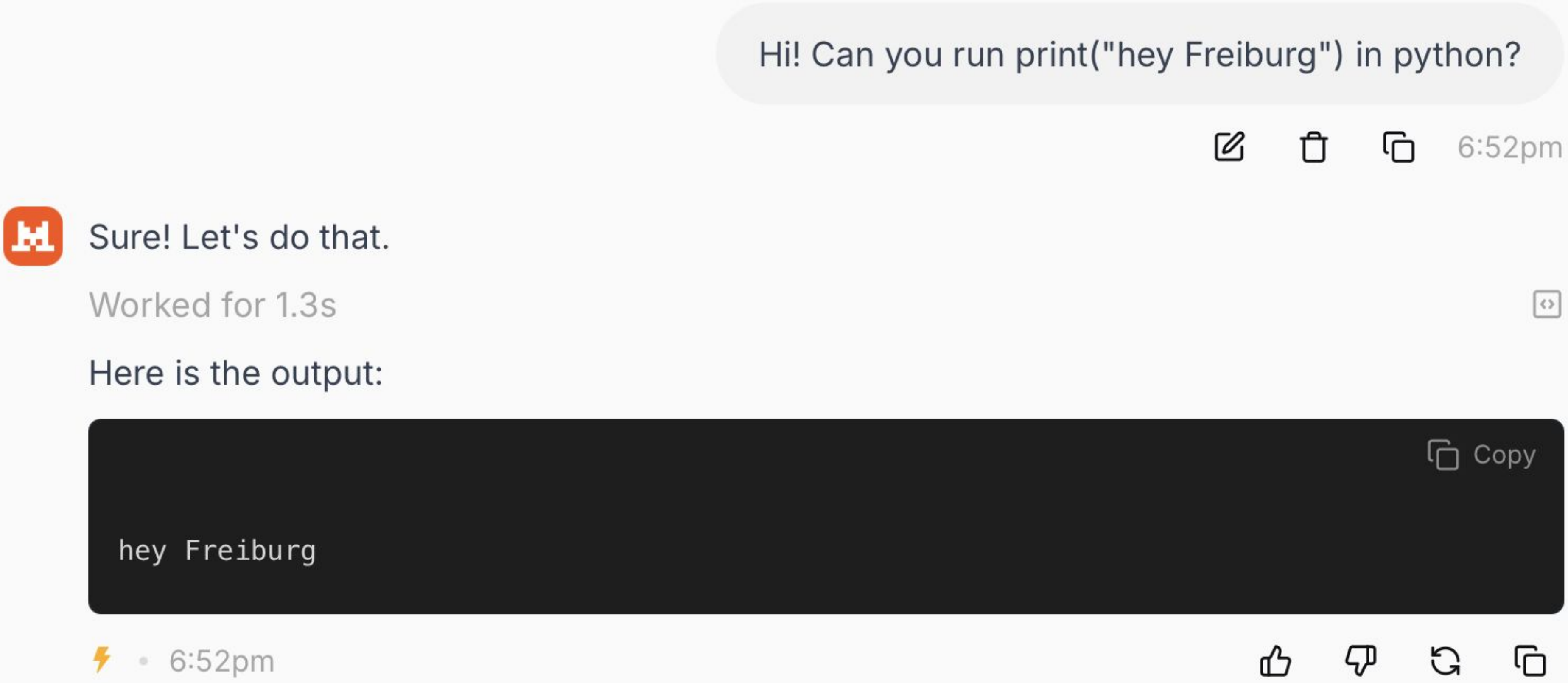
How to Crack Fire 🔥

and run untrusted code instantly without getting pwned 💀



Hi! Can you run print("hey Freiburg") in python?

6:52pm

Sure! Let's do that.

Worked for 1.3s

Here is the output:

```
hey Freiburg
```

6:52pm

About Me

Co-Founder - sliplane.io

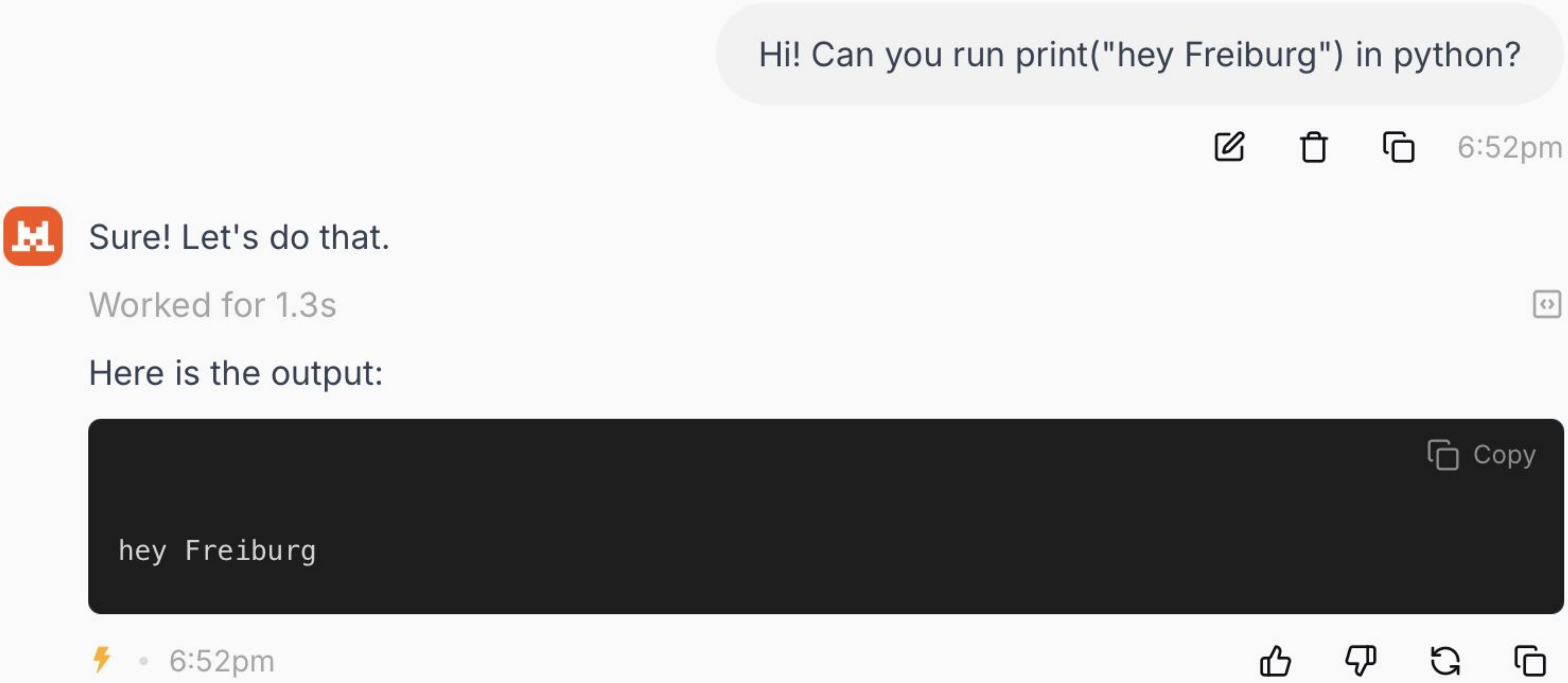
managed container hosting / PaaS

Contractor - e2b.dev

open-source runtime for executing AI-generated code

Docker Captain

container stuff



Hi! Can you run print("hey Freiburg") in python?

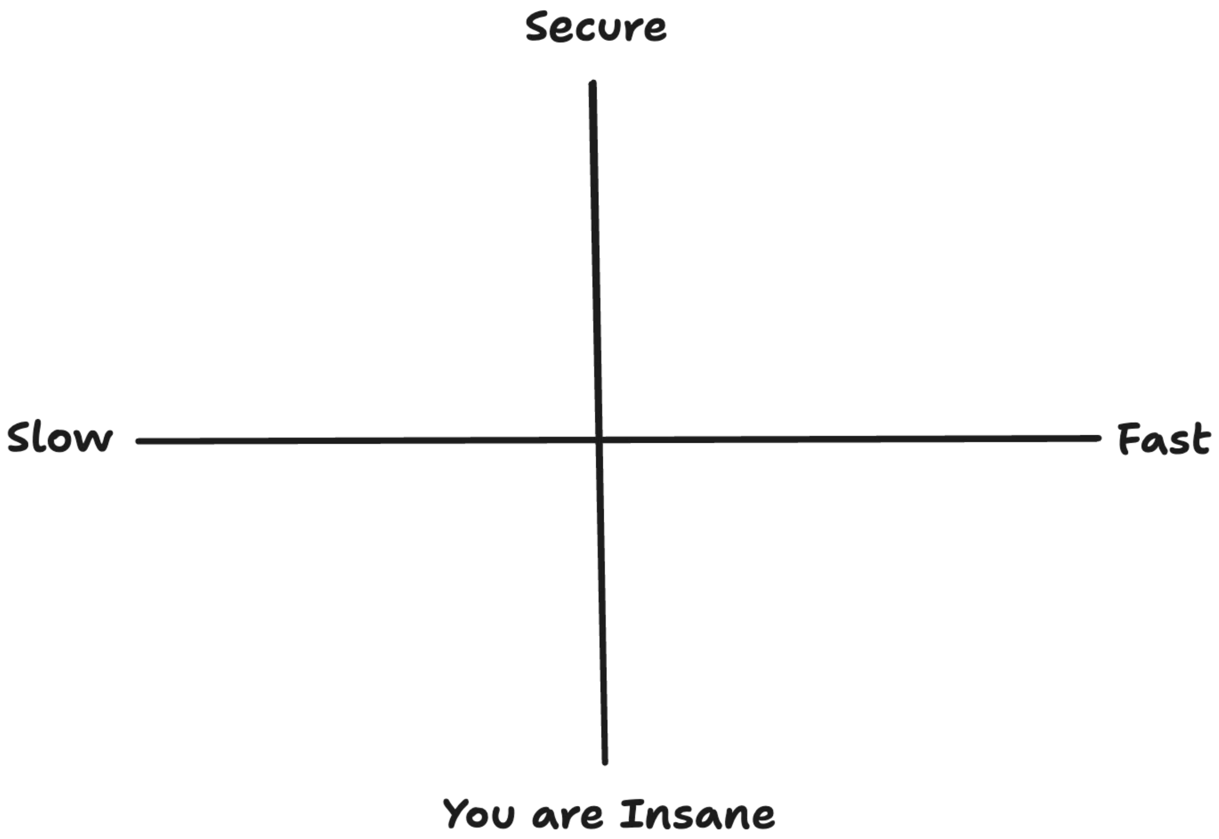
Sure! Let's do that.

Here is the output:

```
hey Freiburg
```

“Running Untrusted Code is a Solved Problem”

… right?



Secure

Slow

Fast

You are Insane

Firecracker

- Minimalist KVM-based VMM by AWS for running “microVMs”
- Ideal for serverless and multi-tenant workloads
- Stronger isolation than containers via hardware virtualization (KVM)
- Can boot in **<150ms**
- Low memory/cpu overhead
  - **<= 5 MiB per VM**
  - 95% compute-only guest cpu performance

Sliplane AWS Fargate aws Lambda

E2B Koyeb Open Nebula katacontainers Northflank

DEMO TIME

DO NOT RUN THIS IN PRODUCTION

- Use a Jailer
- Limit resources with cgroups (memory, network, storage, ..)
- Mitigate hardware vulnerabilities (rowhammer, side channel attacks etc)
- Don’t trust anything inside the guest :)

https://github.com/e2b-dev/infra

https://github.com/firecracker-microvm/firecracker/blob/main/docs/prod-host-setup.md

Conclusion

- Firecracker is cool (but not the only way to achieve this)

- Check out E2B for sandboxing!
- Check out Sliplane for hosting your Docker applications!

- Repo with slides + setup steps:

  http://github.com/code42cate/talks