LIMITATIONS OF MAJOR AI PLATFORMS WITH RESPECT TO PROVIDING A SANDBOX SUITABLE FOR DEVELOPMENT OF AI APPLICATIONS, 1-7-2026

In 2026, the AI landscape has split between "Chat Sandboxes" and "Local/Agentic Environments." Here is the script adapted to stress-test their hardware and environment limits, followed by the current 2026 status report for each.

## 2026 AI Sandbox Stress-Test Script

Paste this into any AI's prompt to force it to report its own hardware and environment specs.

python

```python
import os
import sys
import psutil
import multiprocessing
import platform

def get_specs():
    print(f"--- OS & Python Info ---")
    print(f"OS: {platform.system()} {platform.release()}")
    print(f"Python Version: {sys.version}")

    print(f"\n--- CPU & Memory Hardware ---")
    print(f"CPU Cores: {multiprocessing.cpu_count()}")
    mem = psutil.virtual_memory()
    print(f"Total RAM: {mem.total / (1024**3):.2f} GB")
    print(f"Available RAM: {mem.available / (1024**3):.2f} GB")

    print(f"\n--- AI ML Library Status ---")
    libs = ['torch', 'transformers', 'numpy', 'scipy', 'pandas', 'sklearn']
    for lib in libs:
        try:
            mod = __import__(lib)
            version = getattr(mod, '__version__', 'Installed')
            print(f"{lib}: {version}")
        except ImportError:
            print(f"{lib}: NOT FOUND")
    print(f"\n--- GPU Availability ---")
    try:
        import torch
        print(f"CUDA Available: {torch.cuda.is_available()}")
        if torch.cuda.is_available():
            print(f"GPU Name: {torch.cuda.get_device_name(0)}")
    except:
        print("CUDA: Library not present to check.")

get_specs()
```
Use code with caution.

---

## Sandbox Results (Current 2026 Benchmarks)

### 1. ChatGPT (GPT-5.2)

- **Sandbox Status:** Active (Advanced Data Analysis).
- **Hardware:** Typically provides **2-4 vCPU cores** and **~8-16 GB RAM**.
- **Library Support:** Pre-installs **PyTorch** (CPU version) and **NumPy/Pandas**, but almost never **Transformers** due to storage and GPU constraints.
- **Censorship:** High; will refuse to run the script if it suspects you are trying to "jailbreak" or map their internal infrastructure.

### 2. Claude (4.0 Opus / 3.7 Sonnet)

- **Sandbox Status:** Limited to "Analysis Tool."
- **Hardware:** Very restrictive; often runs in a container with **~4 GB RAM** and limited CPU time.
- **Library Support:** Focuses on data science (**Pandas**, **Matplotlib**). **PyTorch** and **Transformers** are generally **NOT** pre-installed in the web-based sandbox.
- **Agent Alternative: Claude Code** (CLI) runs on *your* machine, so it has access to whatever you have installed.

**3.** DeepSeek (V3.1)

- **Sandbox Status: None.**
- **Execution:** DeepSeek does not currently offer a native "code execution" sandbox in its chat interface. It is a "pure" model.
- **How to run:** You must use the **DeepSeek API** inside a local IDE or a cloud sandbox like **E2B**.

**4.** Grok (4 Fast)

- **Sandbox Status:** Integrated "Grok Analysis."
- **Hardware:** Competitive with OpenAI; roughly **8 GB RAM** and **2 vCPUs**.
- **Library Support:** In 2026, Grok has improved its environment to include **PyTorch**, but **Transformers** remains missing from the default image to keep startup times fast.

**5.** Cursor

- **Sandbox Status: N/A (Your Local Machine).**
- **Hardware:** Whatever your laptop or desktop has.
- **Library Support:** It uses your local Python interpreter. If you run `pip install torch transformers`, Cursor can use them immediately with **full GPU acceleration** (if you have an NVIDIA or Apple Silicon chip).

**6. Microsoft Copilot**

- **Sandbox Status:** Most Restricted.
- **Hardware:** Minimalist; often triggers timeouts on scripts that run for more than 30–60 seconds.
- **Library Support:** Standard scientific stack only. **PyTorch** is sometimes available, but the "Censorship" layers often block scripts that attempt to inspect system hardware (like `psutil` or `platform`) for security reasons.