Formal

Monitoring and Constraining the Bananas 🍌 VS Code SSH Extension

Aditya Saligrama

Stanford Applied Cyber | May 16, 2025

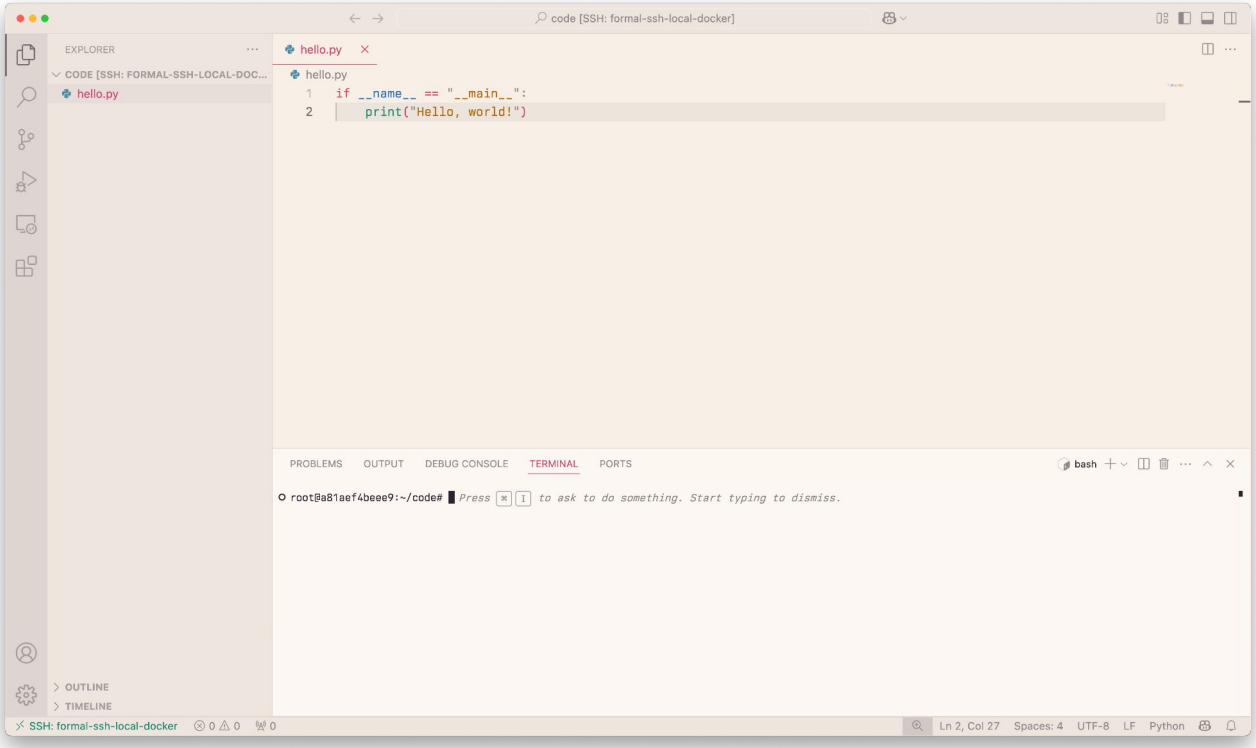
whoami

- Stanford ‘24 (B.S. Systems, M.S. Security)
- President of Applied Cyber ‘23-’25
- CCDC ‘21-’25 🥇🥉, CPTC ‘23-’24 🥈
- Now: Senior Software Engineer @ Formal

Motivation

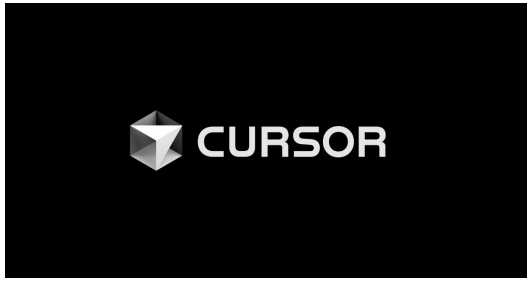
Remote development is becoming more popular

VS Code is very popular



"I even installed a separate SSH server on a Myth machine to make VS Code SSH work"
– a former Applied Cyber Competitions Lead

VS Code’s forks are growing in popularity



...but many security risks abound

BY THOMAS PTACEK — 3 MIN READ

VSCode's SSH Agent Is Bananas

We're interested in getting integrated into the flow VSCode uses to do remote editing over SSH, because everybody is using VSCode now,...

Read more →

February 7, 2025

The agent runs over port-forwarded SSH. It establishes a WebSockets connection back to your running VSCode front-end. The underlying protocol on that connection can:

- Wander around the filesystem
- Edit arbitrary files
- Launch its own shell PTY processes
- Persist itself

In security-world, there's a name for tools that work this way. I won't say it out loud, because that's not fair to VSCode, but let's just say the name is murid in nature.

Security Note

Using Remote-SSH opens a connection between your local machine and the remote. Only use Remote-SSH to connect to secure remote machines that you trust and that are owned by a party whom you trust. A compromised remote could use the VS Code Remote connection to execute code on your local machine.

The two key threat models

- Rogue extension on a laptop compromises the remote host

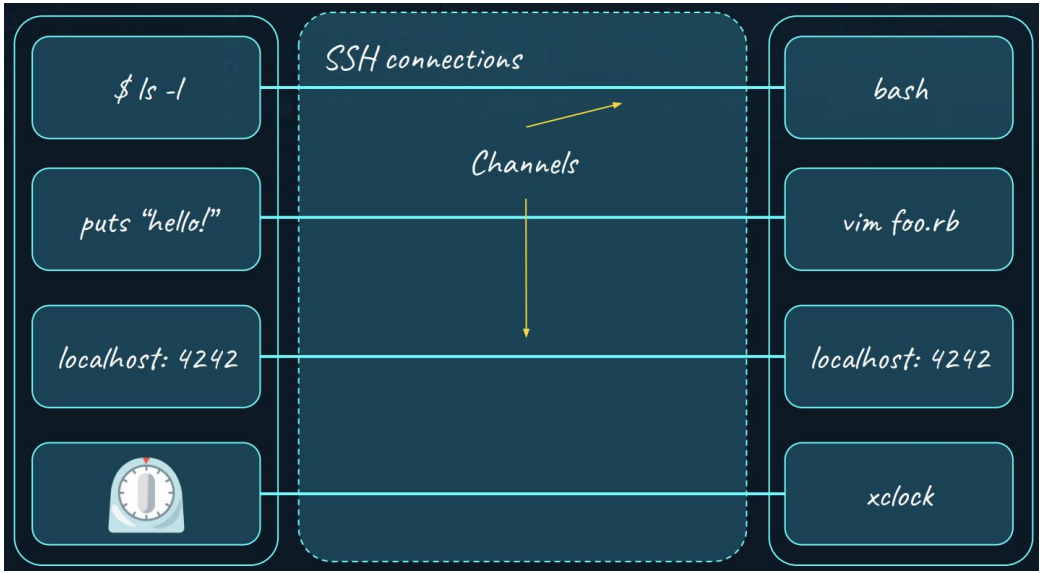
- Rogue remote host binary compromises the laptop

The VS Code SSH Protocol

SSH beyond shells

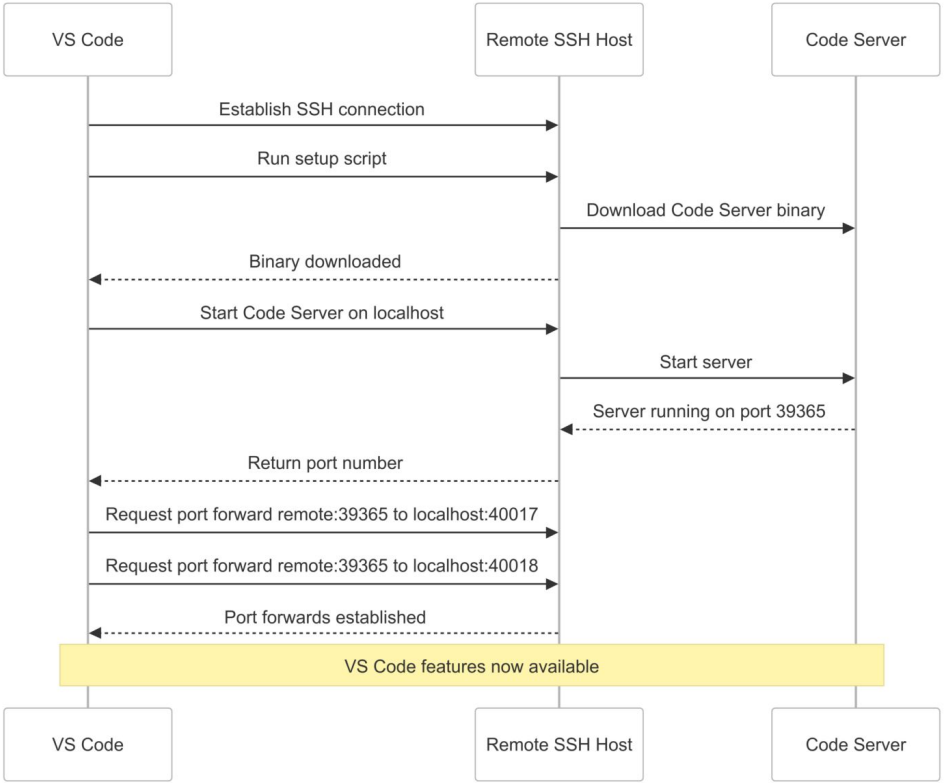
SSH is both encrypted transport (a la TLS) and application layer, supporting:

- Interactive shell sessions
- Command execution
- File transfer (SCP, SFTP)
- TCP port forwarding
- Unix socket forwarding
- Display forwarding
- SSH agent forwarding
- ...and more

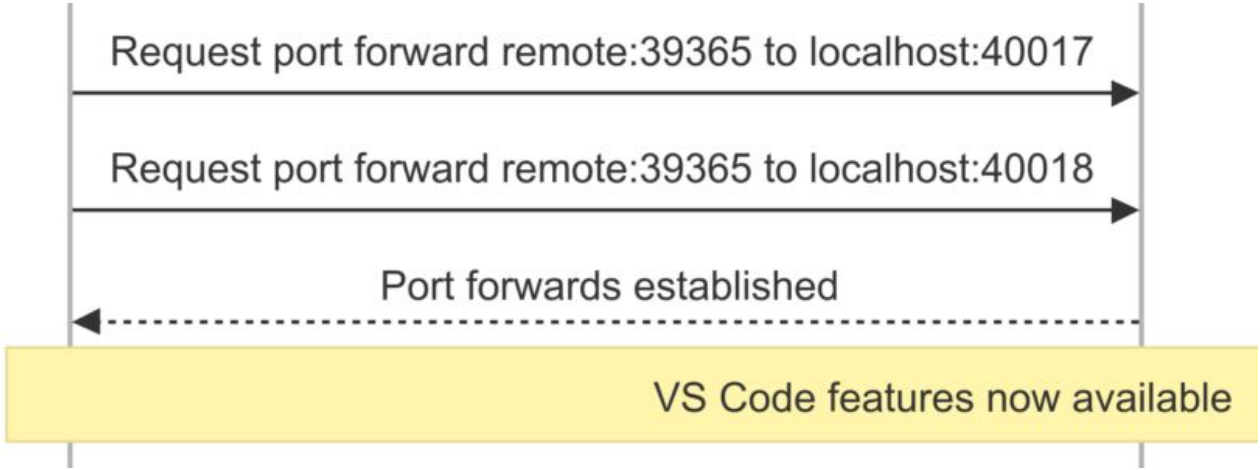


Adapted from H.D. Moore, "Charting the SSH Multiverse", BSidesSF 2025

Establishing a VS Code SSH Session

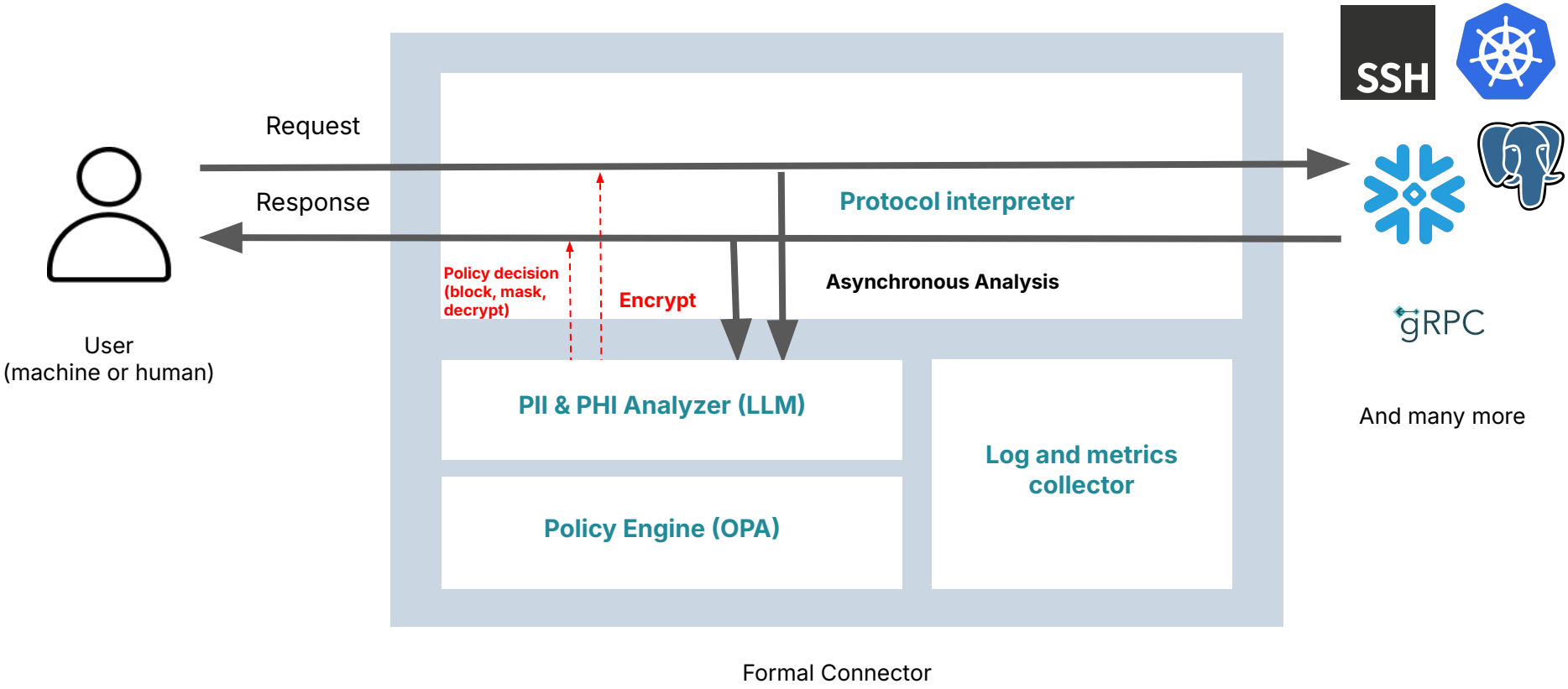


What actually happens here?



Proxying VS Code SSH

How Formal works



We also already support VS Code Remote SSH!

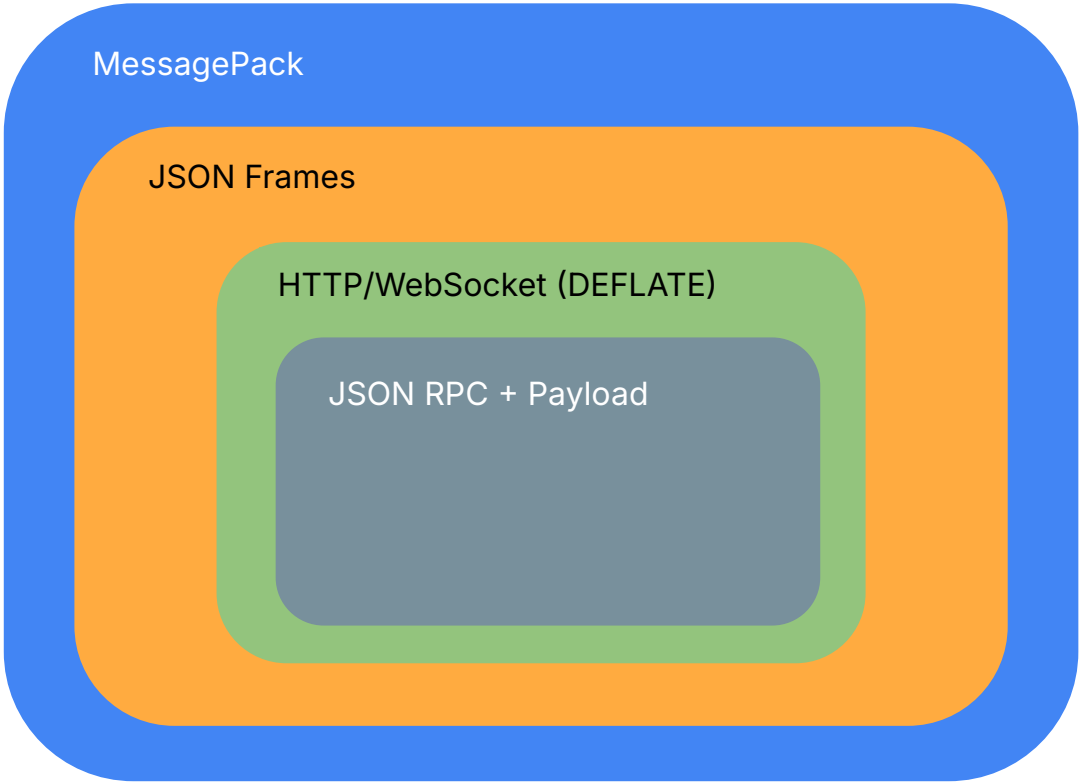
BLOG Feb 7, 2025

Down the rabbit hole: Implementing SSH port forwarding over AWS Session Manager

A technical quest through obscure SSH and AWS Session Manager features in service of enabling VS Code Remote SSH via the Formal Connector, culminating in forking and fixing several concurrency bugs in AWS's own reference library for connecting to compute instances using SSM.

Aditya Saligrama
SOFTWARE ENGINEER

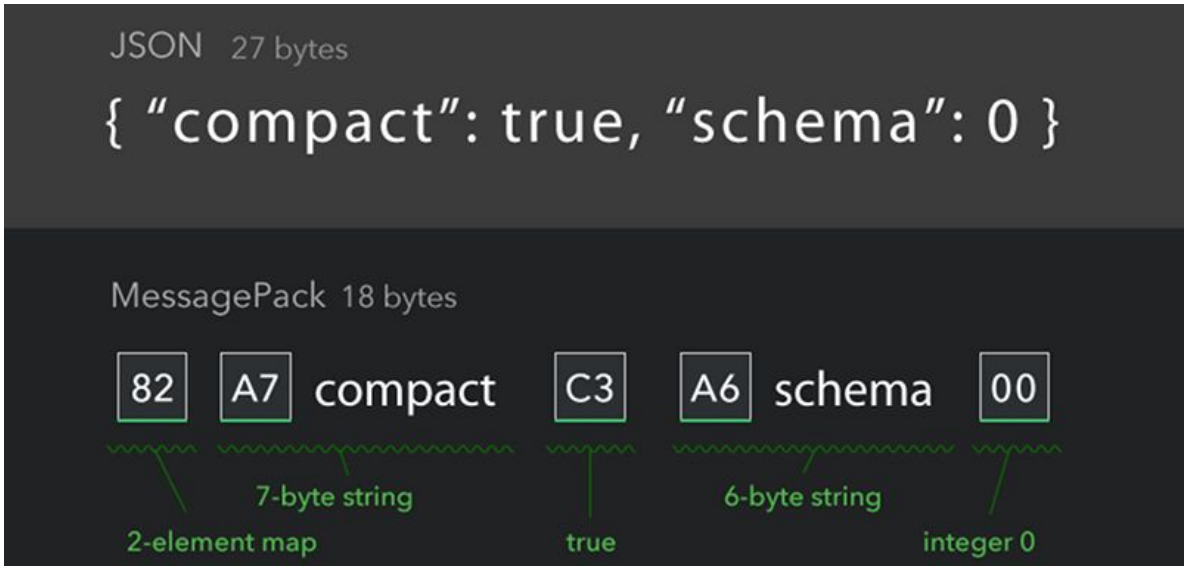
Encapsulation inception



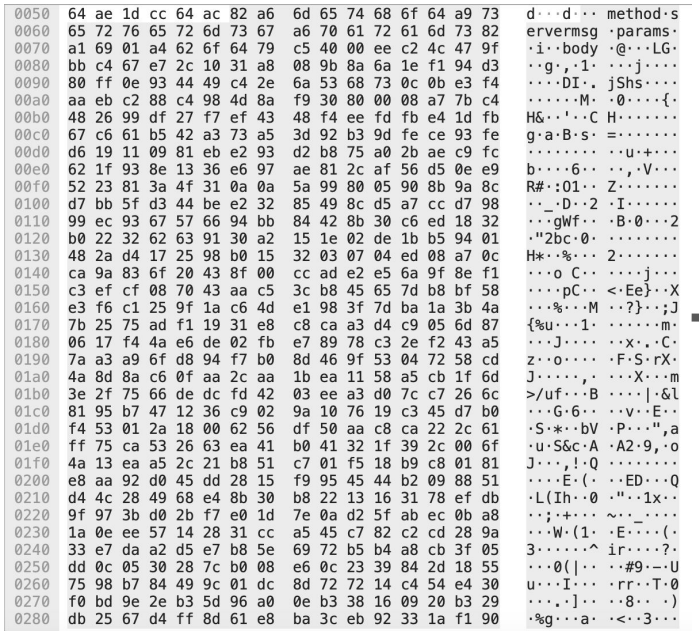
Introspecting JSON RPC and Payloads

1. Decode MessagePack
2. Inflate `servermsg` body
3. Decompress WebSocket RPC payload

Decoding MessagePack



Decoding MessagePack



```
0050  64 ae 1d cc 64 ac 82 a6  6d 65 74 68 6f 64 a9 73   d···d··· method·s
0060  65 72 76 65 72 6d 73 67  a6 70 61 72 61 6d 73 82   ervermsg ·params·
0070  a1 69 01 a4 62 6f 64 79  c5 40 00 ee c2 4c 47 9f   ·i··body ·@···LG·
0080  bb c4 67 e7 2c 10 31 a8  08 9b 8a 6a 1e f1 94 d3   ··g·,·1· ···j····
0090  80 ff 0e 93 44 49 c4 2e  6a 53 68 73 0c 0b e3 f4   ····DI·. jShs····
00a0  aa eb c2 88 c4 98 4d 8a  f9 30 80 00 08 a7 7b c4   ······M· ·0····{·
00b0  48 26 99 df 27 f7 ef 43  48 f4 ee fd fb e4 1d fb   H&··'··C H·······
00c0  67 c6 61 b5 42 a3 73 a5  3d 92 b3 9d fe ce 93 fe   g·a·B·s· =·······
00d0  d6 19 11 09 81 eb e2 93  d2 b8 75 a0 2b ae c9 fc   ········ ··u·+···
00e0  62 1f 93 8e 13 36 e6 97  ae 81 2c af 56 d5 0e e9   b····6·· ··,·V···
00f0  52 23 81 3a 4f 31 0a 0a  5a 99 80 05 90 8b 9a 8c   R#·:O1·· Z·······
0100  d7 bb 5f d3 44 be e2 32  85 49 8c d5 a7 cc d7 98   ··_·D··2 ·I······
0110  99 ec 93 67 57 66 94 bb  84 42 8b 30 c6 ed 18 32   ···gWf·· ·B·0···2
0120  b0 22 32 62 63 91 30 a2  15 1e 02 de 1b b5 94 01   ·"2bc·0· ········
0130  48 2a d4 17 25 98 b0 15  32 03 07 04 ed 08 a7 0c   H*··%··· 2·······
0140  ca 9a 83 6f 20 43 8f 00  cc ad e2 e5 6a 9f 8e f1   ···o C·· ····j···
0150  c3 ef cf 08 70 43 aa c5  3c b8 45 65 7d b8 bf 58   ····pC·· <·Ee}··X
0160  e3 f6 c1 25 9f 1a c6 4d  e1 98 3f 7d ba 1a 3b 4a   ···%···M ··?}··;J
0170  7b 25 75 ad f1 19 31 e8  c8 ca a3 d4 c9 05 6d 87   {%u···1· ····m·
0180  06 17 f4 4a e6 de 02 fb  e7 89 78 c3 2e f2 43 a5   ···J···· ··x·.·C·
0190  7a a3 a9 6f d8 94 f7 b0  8d 46 9f 53 04 72 58 cd   z··o···· ·F·S·rX·
01a0  4a 8d 8a c6 0f aa 2c aa  1b ea 11 58 a5 cb 1f 6d   J·····,· ···X···m
01b0  3e 2f 75 66 de dc fd 42  03 ee a3 d0 7c c7 26 6c   >/uf···B ····|·&l
01c0  81 95 b7 47 12 36 c9 02  9a 10 76 19 c3 45 d7 b0   ···G·6·· ··v··E··
01d0  f4 53 01 2a 18 00 62 56  df 50 aa c8 ca 22 2c 61   ·S·*··bV ·P···",a
01e0  ff 75 ca 53 26 63 ea 41  b0 41 32 1f 39 2c 00 6f   ·u·S&c·A ·A2·9,·o
01f0  4a 13 ea a5 2c 21 b8 51  c7 01 f5 18 b9 c8 01 81   J···,!·Q ········
0200  e8 aa 92 d0 45 dd 28 15  f9 95 45 44 b2 09 88 51   ····E·(· ··ED···Q
0210  d4 4c 28 49 68 e4 8b 30  b8 22 13 16 31 78 ef db   ·L(Ih··0 ·"··1x··
0220  9f 97 3b d0 2b f7 e0 1d  7e 0a d2 5f ab ec 0b a8   ··;·+··· ~··_····
0230  1a 0e ee 57 14 28 31 cc  a5 45 c7 82 c2 cd 28 9a   ···W·(1· ·E····(·
0240  33 e7 da a2 d5 e7 b8 5e  69 72 b5 b4 a8 cb 3f 05   3·····^ ir····?·
0250  dd 0c 05 30 28 7c b0 08  e6 0c 23 39 84 2d 18 55   ···0(|·· ··#9·-·U
0260  75 98 b7 84 49 9c 01 dc  8d 72 72 14 c4 54 e4 30   u···I··· ·rr··T·0
0270  f0 bd 9e 2e b3 5d 96 a0  0e b3 38 16 09 20 b3 29   ····.]·· ··8·· ·)
0280  db 25 67 d4 ff 8d 61 e8  ba 3c eb 92 33 1a f1 90   ·%g···a· ·<··3···
```

File: `vscode_rpc.jsonl`

```
1  {"direction":"C → S","msg":{"id":0,"method":"challenge_issue","params":{"token":"3726d727-62a6-4416-b6a1-aaed0a3e70c5"}}}
2  {"direction":"S → C","msg":{"id":0,"result":{"challenge":"/THmTACBxxV49nObttIKjyU1McYKAThp0VrRjTV1MFA="}}}
3  {"direction":"C → S","msg":{"id":1,"method":"challenge_verify","params":{"response":"567weWW41CaM75U1xWsLztcLeQjjNv2TSP57Wwi/N5MepA="}}}
4  {"direction":"S → C","msg":{"id":1,"result":{}}}
5  {"direction":"C → S","msg":{"id":2,"method":"serve","params":{"archive_path":null,"commit_id":"17baf841131aa23349f217ca7c570c76ee87b957","compress":true,"connection_token":"remotessh","extensions":[],"quality":"stable","socket_id":0}}}
6  {"direction":"C → S","msg":{"id":3,"method":"serve","params":{"archive_path":null,"commit_id":"17baf841131aa23349f217ca7c570c76ee87b957","compress":true,"connection_token":"remotessh","extensions":[],"quality":"stable","socket_id":1}}}
7  {"direction":"S → C","msg":{"id":null,"method":"serverlog","params":{"level":2,"line":"Checking /root/.vscode-server/cli/servers/Stable-17baf841131aa23349f217ca7c570c76ee87b957/log.txt and /root/.vscode-server/cli/servers/Stable-17baf841131aa23349f217ca7c570c76ee87b957/pid.txt for a running server…"}}}
8  {"direction":"S → C","msg":{"id":null,"method":"serverlog","params":{"level":2,"line":"Found running server (pid=580)"}}}
9  {"direction":"S → C","msg":{"id":3,"result":{}}}
10 {"direction":"S → C","msg":{"id":2,"result":{}}}
11 {"direction":"S → C","msg":{"method":"servermsg","params":{"body":"TMxPS8MwGIDxeyHfoaddJGZv0zRtoQwd/kEvw1bc9U3ydo7WZjaRMj+9IDK8PZff83DXpUuohRi9xFHdhyhCRDMSB22wL3MACYiZlHnVZ6Ataqv02uqCqNSmUnozk/XTRDYe/dT5gaZGrnNE5xTXoAqegwSOReZ4ZRwpVUqntFn9Z02PY6BVGI6nNzKttwPF+xk/KDRx/qL0set2Aq6BJduLqdPX02FGRyz5izpdyIRfzJKWLL+8+DOd6zSctdx9+tuX/VWbfT9Ni2hvtoemYQlLfgAAAP//","i":1}}}
12 {"direction":"C → S","msg":{"method":"servermsg","params":{"body":"TMxBS8MwGIDhe6H/oafdYpc18UsLQZg4hSkozfD8Jf3SldZmNJHqvxdEhrf38ryPD6ZYY1OWU3A4nUNMZUxoJ2IcLHolOK844q6qRO13HByCk7B1cEukwNYS7hZyYZ7JpSHMJow0ayWtFMoR66AmJoQQzHromPLObztUskLa/Gfa4xRpE8fh8k62DW6kdFjwg6JOyycVT8a8lvyG59n91TTF6dIv2FGe/UVTrGTjL86zlhy7vtiRvpsi9cfDV2rtMK9v++cF+pdofK91nuXZDwAAAP//","i":0}}}
13 {"direction":"S → C","msg":{"id":null,"method":"servermsg","params":{"body":"8ggJCdA31DNUMDQwVAguzyxJzsjMS1cIKMovyU/Ozynm5QotSC9KTEm1UihPTSrOT85OLeHlcs7Py0tNLsnMz7NSgMrzcgWnJuuGpyYFg9XoOiYnpxaUAKW9SyP0U3IMTSrCXd1C883D3bz9XFwsSoosLGx5uXi5AAAAAP//","i":1}}}
14 {"direction":"C → S","msg":{"method":"servermsg","params":{"body":"YmJAgIhqpZLKglQlK6XE0pIMJR0IZaVUlJqbX5JaXAwSSkksSQQJuRWl+ARFBhgG6meGJmc55kU6VqR6F1e6V+rnGbrpZzq5GZsnpoUXpukX2yrVAgAAAP//","i":1}}}
15 {"direction":"S → C","msg":{"id":null,"method":"servermsg","params":{"body":"LMqxCsIwEADQPZB/uB+oNRaXgEOtAcGlmBbBzZ5HG9RcSA76+4I4v3cehr42GwNma8CvQXAJcYY+szDyu2g1pjk/nmRhpakwvki06jhGQgkcLfxdK09Y3Wjyv1O1iJTEQrmmj7uP5dhgk3bo9l129QkDXdqDVlp9AQAA//8=","i":0}}}
16 {"direction":"C → S","msg":{"method":"servermsg","params":{"body":"YmJAgIhqpZLKglQlK6XE0pIMJR0IZaVUlJqbX5JaXAwSSkksSVSyUjJwMi4wSfMNT3YOc/ZPK0nODtP3NMo1cvEKSCwqyHH2CM1N8UkNCkgOMbOwVaoFAAAA//8=","i":0}}}
17 {"direction":"S → C","msg":{"id":null,"method":"servermsg","params":{"body":"YmJAgJZqpZLKglQlK6XizPQ8JR2llMSSRCAvLT/JyCMyzFS/Ks232Cc/zzA1y8MitCKisNg5xL+s1DDHNCgzPNHfKyQt0haoC6Q5NcUFotfA0DjZL8Kl2N8pKtvEJdVS28utPDxTO8qlNMXMzDI/1S0t0cXfsTzFI9/b1zPfVqkWAAAA//8=","i":1}}}
18 {"direction":"C → S","msg":{"method":"servermsg","params":{"body":"jJG/DoIwHITf5eYOyqCxiZOyuOigpLpV+ktD7B9SQLCEl/VJDJoY3Fxv+b67m0KeX8hkvTFgyL21RQ2Ofy8AQ1VoR2r7sVotZrk8Z3sV29B1UsWlOMaLN8mhqR9xLtq03dlApRUizU7rsQ5VRSC1+VXhCYMMugLvYaTTjdSjMDkwXAPJG/j7OIbShxrcNcYwkLuD98MwvAAAAP//","i":1}}}
```

Inflating servermsg's

```
TMxPS8MwGIDxeyHfoaddJGZv0zRtoQwd/kEvw1bc9U3ydo7WZjaRMj+9IDK8PZff83DXpUuohRi9xfHdhyhCR
DMSB22wL3MACYiZlHnVZ6Ataqv02uqCqNSmUnozk/XTRDYe/dT5gaZGrnNE5xTXoAqegwSOReZ4ZRwpVUqntF
n9Z02PY6BVGI6nNzKttwPF+xk/KDRx/qL0set2Aq6BJduLqdPX02FGRyz5izpdyIRfzJKWLL+8+DOd6zSctdx
9+tuX/VWbfT9Ni2hvtoemYQlLfgAAAP//
```

```
GET ws://localhost/stable-17baf841131aa23349f217ca7c570c76ee87b957?reconnectionToken=
304aadd5-7156-4131-a62d-9bde5583d57b&reconnection=false&skipWebSocketFrames=true
HTTP/1.1
Connection: Upgrade
Upgrade: websocket
Sec-WebSocket-Key: sy73PqoBRX+S2zJnw/SACg==
```

Behavioral Analysis

MCP server autodiscovery


```
{
  "method": "Filesystem.readFile",
  "params": {
    "path": "/root/.cursor/mcp.json",
    "scheme": "vscode",
    "uri": "vscode://ssh-remote+formal-ssh:/root/.cursor/mcp.json"
  }
}
```

What other RPC APIs are available?

```
override async installFromGallery(extension: IGalleryExtension, installOptions: InstallOptions = {}): Promise<ILocalExtension> {
        if (isUndefined(installOptions.donotVerifySignature)) {
                const value = this.configurationService.getValue(VerifyExtensionSignatureConfigKey);
                installOptions.donotVerifySignature = isBoolean(value) ? !value : undefined;
        }
        const local = await this.doInstallFromGallery(extension, installOptions);
        await this.installUIDependenciesAndPackedExtensions(local);
        return local;
}
```

- `"extensionKind": ["ui"]` — Indicates the extension **must** run close to the UI because it requires access to local assets, devices, or capabilities or because low latency is required. In the case of VS Code for the Web with Codespaces, where no local extension host is available, such an extension can not load, unless it is also a web extension. It will then be loaded in the web extension host with a limitation that it cannot instantiate a web worker.

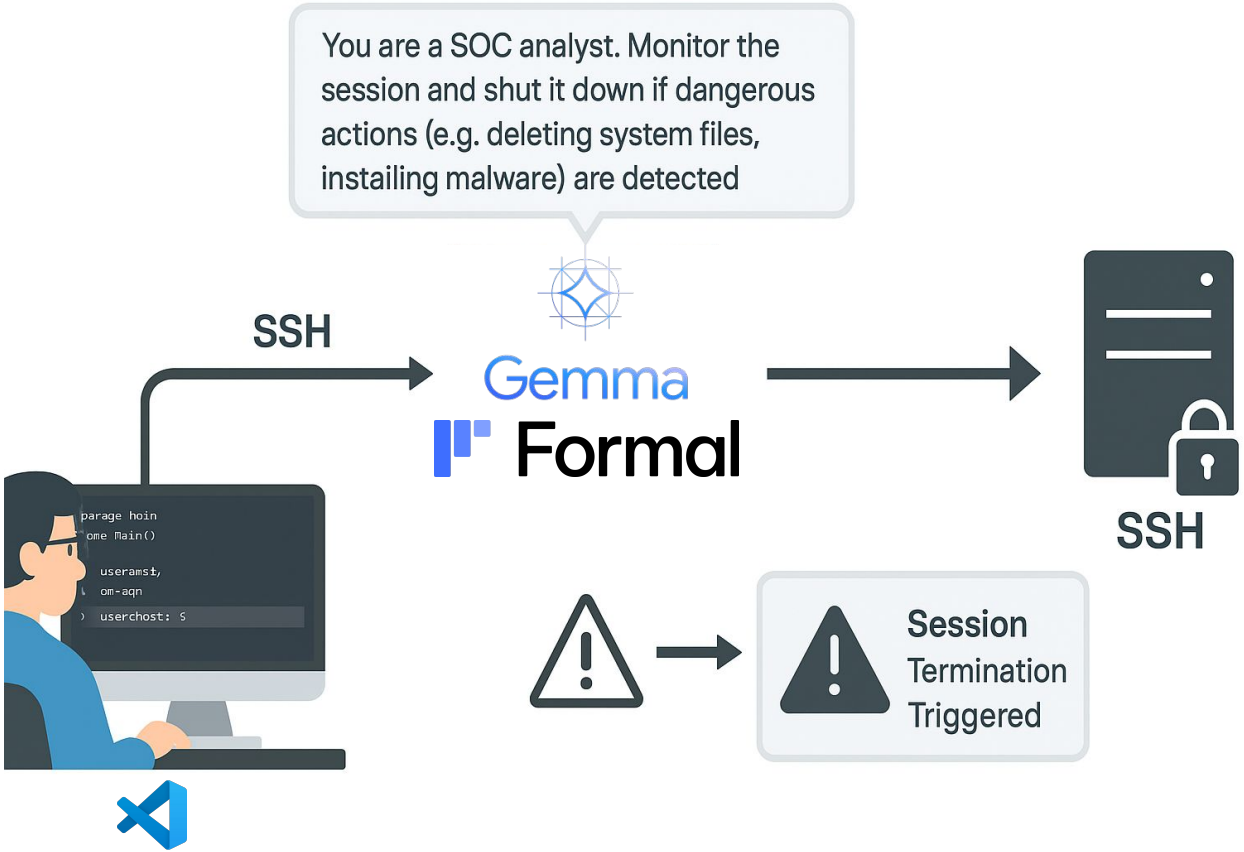
Constraining VS Code SSH

Introspecting JSON RPC and Payloads

- To block the extension threat: use Formal to end the connection if `installFromGallery` is called
  - Potentially only with specific non-allowlisted extensions

- But many more attack vectors remain
  - Potentially arbitrary: e.g. how do we decide which files on the remote are sensitive?

Formal with (more) LLMs



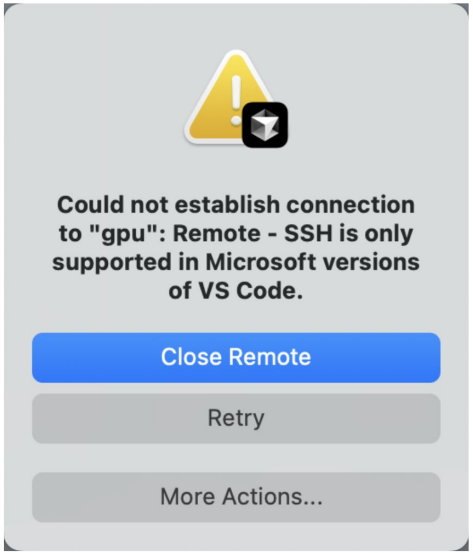
A note on VS Code forks

Remote - SSH is only supported in Microsoft versions of VS Code

Bug Reports

stephengineer Oct 2024

I am trying to use Cursor to connect VM, but I received the following error. However, I can connect VM via VS Code with the same config. Anyone knows how to fix it?



bekit Feb 11

You can get it to work by installing a version from before when Microsoft began blocking its use on third party apps. `v0.113.1` is the latest version I was able to get working, which can be downloaded from here: https://marketplace.visualstudio.com/_apis/public/gallery/publishers/ms-vscode-remote/vsextensions/remote-ssh/0.113.1/vspackage 171

Formal is hiring!

Engineering

Senior Software Engineer | Backend

Engineering • San Francisco • Full time • On-site

Software Engineer | Backend

Engineering • San Francisco • Full time • On-site

Software Engineer | Fullstack

Engineering • San Francisco • Full time • On-site

Solutions Engineer

Engineering • San Francisco • Full time

Marketing & Design

Founding Designer

Marketing & Design • San Francisco • Full time • On-site

Founding Marketer

Marketing & Design • San Francisco • Full time • On-site

Sales

Account Executive

Sales • San Francisco • Full time

Operations

Sales • San Francisco • Full time • On-site

Questions?

✉️ aditya@joinformal.com