

FRIDA TOOL:

Aakash R
CB.SC.P2CYS23011

Frida is a dynamic instrumentation toolkit designed for developers, reverse engineers, and security researchers. It allows you to inject scripts into running processes to inspect and modify their behaviour on the fly.

Use Cases

- **Security Testing:** Inspect and modify the behavior of applications to find vulnerabilities and test security mechanisms.
- **Reverse Engineering:** Understand how applications work internally by examining and modifying their runtime behavior.
- **Debugging:** Debug applications by injecting scripts to track down bugs and performance issues.
- **Bypassing Restrictions:** Modify app behavior to bypass certain restrictions or implement additional features.

Frida uses an injector to load a shared library into the target process. This library provides a JavaScript runtime environment where user scripts are executed. The scripts can hook into various functions, manipulate memory, and interact with the app in real-time.

```
Collecting frida-tools
  Downloading frida-tools-12.4.3.tar.gz (200 kB)
    200.9/200.9 kB 1.4 MB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Installing backend dependencies ... done
  Preparing metadata (pyproject.toml) ... done
Collecting colorama<1.0.0,>=0.2.7 (from frida-tools)
  Downloading colorama-0.4.6-py3-none-any.whl.metadata (17 kB)
Collecting frida<17.0.0,>=16.2.2 (from frida-tools)
  Downloading frida-16.3.1-cp37-abi3-win32.whl.metadata (2.1 kB)
Collecting prompt_toolkit<4.0.0,>=2.0.0 (from frida-tools)
  Downloading prompt_toolkit-3.0.45-py3-none-any.whl.metadata (6.4 kB)
Collecting pygments<3.0.0,>=2.0.2 (from frida-tools)
  Downloading pygments-2.18.0-py3-none-any.whl.metadata (2.5 kB)
Collecting typing_extensions (from frida<17.0.0,>=16.2.2->frida-tools)
  Downloading typing_extensions-4.12.1-py3-none-any.whl.metadata (3.0 kB)
Collecting wcwidth (from prompt_toolkit<4.0.0,>=2.0.0->frida-tools)
  Downloading wcwidth-0.2.13-py2.py3-none-any.whl.metadata (14 kB)
Downloaded colorama-0.4.6-py3-none-any.whl (25 kB)
Downloaded frida-16.3.1-cp37-abi3-win32.whl (19.9 MB)
    19.9/19.9 MB 3.3 MB/s eta 0:00:00
Downloaded prompt_toolkit-3.0.45-py3-none-any.whl (386 kB)
    386.1/386.1 kB 3.0 MB/s eta 0:00:00
Downloaded pygments-2.18.0-py3-none-any.whl (1.2 MB)
    1.2/1.2 MB 3.3 MB/s eta 0:00:00
Downloaded typing_extensions-4.12.1-py3-none-any.whl (37 kB)
Downloaded wcwidth-0.2.13-py2.py3-none-any.whl (34 kB)
Building wheels for collected packages: frida-tools
  Building wheel for frida-tools (pyproject.toml) ... done
  Created wheel for frida-tools: filename=frida_tools-12.4.3-py3-none-any.whl size=209691 sha256=ed5bb2a57ccddc70f25583e35d566235037e84852c41e0ade5135786b02
```

```

D:\Mtech Course\Sem 3\Android Assignments\frida_tools>emulator -list-avds
INFO | Storing crashdata in: C:\Temps\AndroidEmulator\emu-crash-34.2.14.db, detection is enabled for process: 10760
Pixel_3_API_19
Pixel_4_XL_API_30

D:\Mtech Course\Sem 3\Android Assignments\frida_tools>emulator -avd

D:\Mtech Course\Sem 3\Android Assignments\frida_tools>emulator -avd Pixel_3_API_19
INFO | Storing crashdata in: C:\Temps\AndroidEmulator\emu-crash-34.2.14.db, detection is enabled for process: 11000
INFO | Android emulator version 34.2.14.0 (build_id 11834374) (CL:N/A)
INFO | Found systemPath C:\Users\Jay Shah\AppData\Local\Android\Sdk\system-images\android-19\default\x86\
INFO | Storing crashdata in: C:\Temps\AndroidEmulator\emu-crash-34.2.14.db, detection is enabled for process: 9936
INFO | Duplicate loglines will be removed, if you wish to see each individual line launch with the -log-nofilter flag

INFO | IPv4 server found: 192.168.1.1
INFO | Ignore IPv6 address: 857:1567:b02:0:6051:1567:b02:0
INFO | Ignore IPv6 address: 857:1567:b02:0:6051:1567:b02:0 (2x)
INFO | Ignore IPv6 address: 205d:1567:b02:0:6051:1567:b02:0
INFO | Ignore IPv6 address: 205d:1567:b02:0:6051:1567:b02:0 (2x)
INFO | Ignore IPv6 address: 4063:1567:b02:0:6051:1567:b02:0
INFO | Ignore IPv6 address: 4063:1567:b02:0:6051:1567:b02:0 (2x)

```

```

PS D:\Mtech Course\Sem 3\Android Assignments\frida_tools> adb push frida-server /data/local/tmp
frida-server: 1 file pushed, 0 skipped. 23.2 MB/s (56532312 bytes in 2.320s)
PS D:\Mtech Course\Sem 3\Android Assignments\frida_tools> adb shell

```

```

PS D:\Mtech Course\Sem 3\Android Assignments\frida_tools> adb push frida-server /data/local/tmp
frida-server: 1 file pushed, 0 skipped. 23.2 MB/s (56532312 bytes in 2.320s)
PS D:\Mtech Course\Sem 3\Android Assignments\frida_tools> adb shell
root@generic_x86:/ # cd /data/local/tmp
root@generic_x86:/data/local/tmp # ls
frida-server
hmod 777 frida-server
root@generic_x86:/data/local/tmp # chmod 777 frida-server
root@generic_x86:/data/local/tmp #

```

With Burp Suite:

AndroidWifi

Metered

Detect automatically

Proxy

Manual

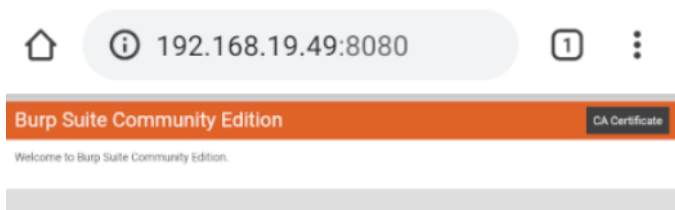
The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname

10.11.138.225

Proxy port

8081



Search for CA Certificate

