




# Dynamic instrumentation 101


Akshay Jain  
Nishaanth Guna



## Who are we?


Akshay Jain works at Phonepe as Security Engineer. He has reported vulnerabilities in Apple, Microsoft, Google and many fortune 500 companies.

Nishaanth Guna works at MDSec Consulting as a Security Consultant, pentesting web and mobile applications. Apart from application security, his other interests are red teaming and exploit development.



# Goals

- What is Dynamic Instrumentation?
- What is Frida?
- Modes of Frida
- Universal SSL Unpinning
- Hooking into Windows APIs
- Tracing API calls with in-build modules
- Some useful modules and references.



# Things that can be done in Frida

- Bypassing SSL Pinning and Root Detection in Mobile Applications
- Dumping in-memory keys such as passwords, private keys, application-specific secrets
- Analyzing Malware to understand the functionality
- Tracing a specific functionality to analyze the crash
- Bypass device level restrictions imposed on the target application.
- Hook into private API calls and dump the arguments, values.



# Dynamic Instrumentation

- Process of modifying or altering the instructions of the executable during runtime.
- Applications include various domains including reverse engineering, exploit development, software quality assurance, debugging etc.
- Instrumentation framework gets attached to the binary and can be used to debug the application when it is running.
- Methods, variables, arguments passed inside the application can be hooked to modify, print or alter the execution flow.
- Can be done on any executable running on any platform.



# Frida


- Frida instrumentation toolkit which allows you to inject snippets of JavaScript into native applications.
- Installing Frida is simple and supported on Node, Python, Swift, C and .NET. Has cross-platform support.
- Languages bindings also come in Node, Python, Swift etc.
- Needs an agent to be run on the device if it is run on embedded mode. For example, mobile devices need to run the frida-server and you can connect to the port from your local machine.





# Frida Tools

- Code coverage - lighthouse
- Fuzzing - libAFL
- Security - passionfruit, objection, fermion, house
- Frida internal tools
  - frida-ps
  - frida-discover
  - frida-kill
  - frida-trace
  - frida-ls-devices



# Modes of Operation

- Injection

It is a method which injects GUMJS into a shared library that injects into existing software.

- Embedded

Client-Server Model. Frida Gadget needs to be present in the device and the local instance can connect and run commands on it.

- PreLoad

Frida-gadget can be made to run on application using LD\_PRELOAD and DYLD\_INSERT\_LIBRARIES which makes the library attached to the process.





# Instrumentation of a process

- Find the PID of the application or attach Frida to the name of the process.
- Use -f flag to force Frida to start and run the process.
- Process.modules to extract information about the process.
- After we know which module to hook, we can use Module.functions to extract more information about the application.
- Command frida-trace can be used to generate a list of stubs and backtrace the API calls behind the executable.

```
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User> tasklist | Select-String "wsl"
```

wslhost.exe	18924 Console	1	6,268 K
wsl.exe	22632 Console	1	7,428 K
wslhost.exe	4232 Console	1	6,144 K

```
PS C:\Users\User> frida -f C:\Windows\System32\notepad.exe
```

```

┌───┐
│ C │
└───┘
> _
/_/_|_

Frida 15.1.14 - A world-class dynamic instrumentation toolkit

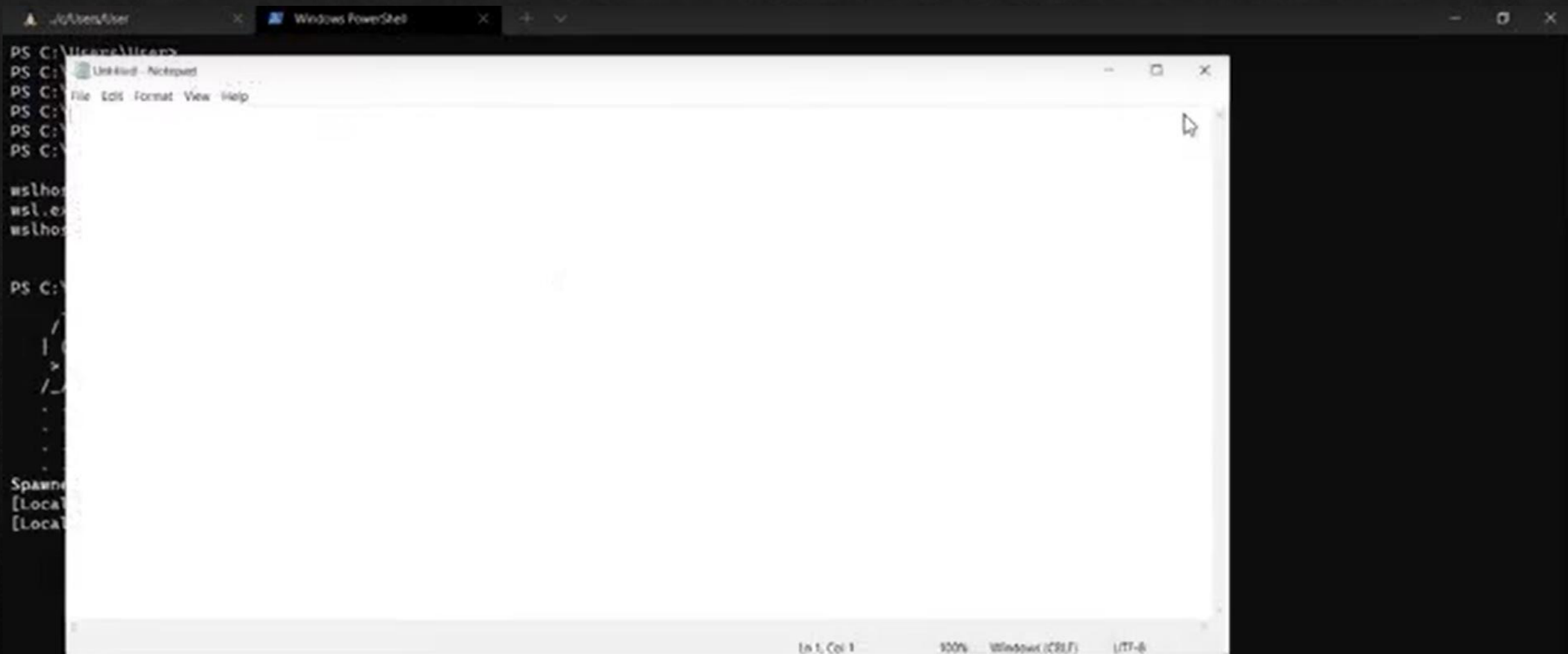
Commands:
  help      -> Displays the help system
  object?   -> Display information about 'object'
  exit/quit -> Exit

...
More info at https://frida.re/docs/home/
```

```
Spawned 'C:\Windows\System32\notepad.exe'. Use %resume to let the main thread start executing!
```

```
[Local::notepad.exe]-> %resume
```

```
[Local::notepad.exe]-> |
```



```
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User> tasklist | Select-String "wsl"
```

wslhost.exe	18924 Console	1	6,268 K
wsl.exe	22632 Console	1	7,428 K
wslhost.exe	4232 Console	1	6,144 K

```
PS C:\Users\User> frida -f C:\Windows\System32\notepad.exe
```

```

┌───┐
│ C │
└───┘
>
┌───┐
│ C │
└───┘
/./ |
...
...
...
More info at https://frida.re/docs/home/
Spawned 'C:\Windows\System32\notepad.exe'. Use %resume to let the main thread start executing!
[Local::notepad.exe]-> %resume
[Local::notepad.exe]-> Process terminated
[Local::notepad.exe]->

Thank you for using Frida!
PS C:\Users\User>
```

```

wslhost.exe      18924 Console      1      6,268 K
wsl.exe          22632 Console      1      7,428 K
wslhost.exe      4232 Console      1      6,144 K

```

PS C:\Users\User> frida -f C:\Windows\System32\notepad.exe

```

  ____
 /  _ \   Frida 15.1.14 - A world-class dynamic instrumentation toolkit
|  _ < |
>  _ < |
/_/  \_\_|

Commands:
  help      -> Displays the help system
  object?   -> Display information about 'object'
  exit/quit -> Exit

...
More info at https://frida.re/docs/home/

```

Spawned 'C:\Windows\System32\notepad.exe'. Use %resume to let the main thread start executing!

```

[Local::notepad.exe]-> %resume
[Local::notepad.exe]-> Process terminated
[Local::notepad.exe]->

```

Thank you for using Frida!

PS C:\Users\User> frida -p 22632

```

  ____
 /  _ \   Frida 15.1.14 - A world-class dynamic instrumentation toolkit
|  _ < |
>  _ < |
/_/  \_\_|

Commands:
  help      -> Displays the help system
  object?   -> Display information about 'object'
  exit/quit -> Exit

...
More info at https://frida.re/docs/home/

```

[Local::PID::22632]-> Process.id

22632

[Local::PID::22632]-> Process.enumerateModulesSync()

```

AggregateError
ApiResolver
Array
ArrayBuffer
Backtracer
BigInt

```

```
[Local::PID::22632]-> Process.id
22632
[Local::PID::22632]-> Process.enumerateModulesSync()
[
  {
    "base": "0x7ff7184a0000",
    "name": "wsl.exe",
    "path": "C:\\Windows\\system32\\wsl.exe",
    "size": 135168
  },
  {
    "base": "0x7ff917730000",
    "name": "ntdll.dll",
    "path": "C:\\Windows\\SYSTEM32\\ntdll.dll",
    "size": 2052096
  },
  {
    "base": "0x7ff915dc0000",
    "name": "KERNEL32.DLL",
    "path": "C:\\Windows\\System32\\KERNEL32.DLL",
    "size": 778240
  },
  {
    "base": "0x7ff915370000",
    "name": "KERNELBASE.dll",
    "path": "C:\\Windows\\System32\\KERNELBASE.dll",
    "size": 2916352
  },
  {
    "base": "0x7ff9151e0000",
    "name": "ucrtbase.dll",
    "path": "C:\\Windows\\System32\\ucrtbase.dll",
    "size": 1048576
  },
  {
    "base": "0x7ff9167d0000",
    "name": "combase.dll",
    "path": "C:\\Windows\\System32\\combase.dll",
    "size": 3493888
  },
]
```



```
},
{
  "base": "0x7ff8f9960000",
  "name": "LxssManagerProxyStub.dll",
  "path": "C:\\Windows\\System32\\Lxss\\LxssManagerProxyStub.dll",
  "size": 36864
},
{
  "base": "0x7ff90f4d0000",
  "name": "wshhyperv.dll",
  "path": "C:\\Windows\\system32\\wshhyperv.dll",
  "size": 28672
},
{
  "base": "0x7ff915f40000",
  "name": "GDI32.dll",
  "path": "C:\\Windows\\System32\\GDI32.dll",
  "size": 176128
},
{
  "base": "0x7ff915740000",
  "name": "win32u.dll",
  "path": "C:\\Windows\\System32\\win32u.dll",
  "size": 139264
},
{
  "base": "0x7ff914ee0000",
  "name": "gdi32full.dll",
  "path": "C:\\Windows\\System32\\gdi32full.dll",
  "size": 1101824
},
{
  "base": "0x7ff9171b0000",
  "name": "USER32.dll",
  "path": "C:\\Windows\\System32\\USER32.dll",
  "size": 1788832
},
{
  "base": "0x7ff915150000",
  "name": "bcrypt.dll",
  "path": "C:\\Windows\\System32\\bcrypt.dll",
  "size": 159744
}
```

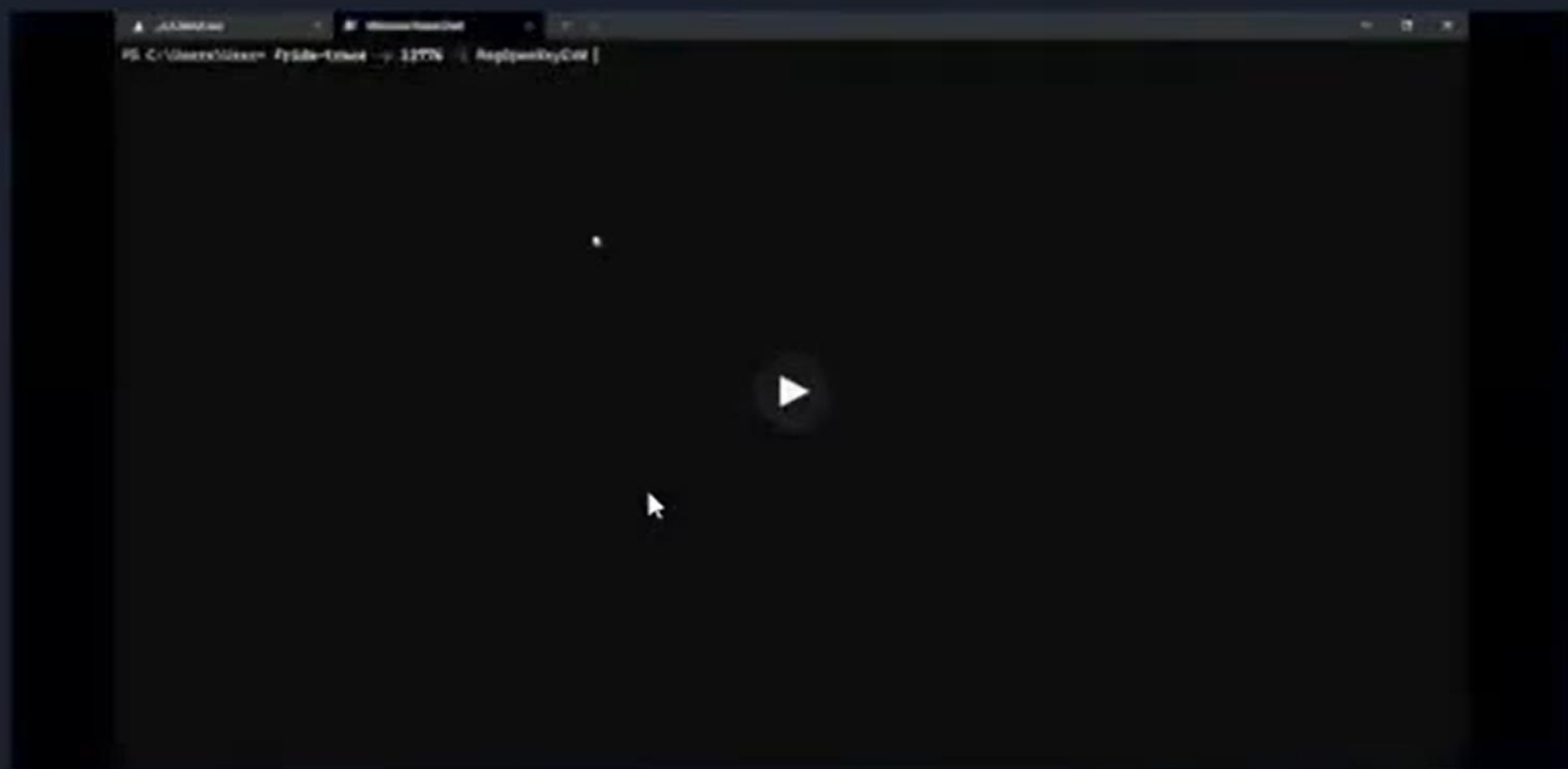
```
{
  "base": "0x7ff914ee0000",
  "name": "gdi32full.dll",
  "path": "C:\\Windows\\System32\\gdi32full.dll",
  "size": 1101824
},
{
  "base": "0x7ff9171b0000",
  "name": "USER32.dll",
  "path": "C:\\Windows\\System32\\USER32.dll",
  "size": 1700032
},
{
  "base": "0x7ff915150000",
  "name": "bcrypt.dll",
  "path": "C:\\Windows\\System32\\bcrypt.dll",
  "size": 159744
},
{
  "base": "0x7ff916c00000",
  "name": "IMM32.DLL",
  "path": "C:\\Windows\\System32\\IMM32.DLL",
  "size": 196608
},
{
  "base": "0x7ff87e730000",
  "name": "frida-agent.dll",
  "path": "C:\\Users\\User\\AppData\\Local\\Temp\\frida-1af5c2b5b22303e5e1b4d5a4c2ed4a21\\64\\frida-agent.dll",
  "size": 22425600
},
{
  "base": "0x7ff9175c0000",
  "name": "ole32.dll",
  "path": "C:\\Windows\\System32\\ole32.dll",
  "size": 1220608
},
{
  "base": "0x7ff915ee0000",
  "name": "SHLAPI.dll",
  "path": "C:\\Windows\\System32\\SHLAPI.dll",
  "size": 348160
},
}
```

```

    "size": 159744
  },
  {
    "base": "0x7ff915d10000",
    "name": "NSI.dll",
    "path": "C:\\Windows\\System32\\NSI.dll",
    "size": 32768
  }
]
[Local::PID::22632]-> Module.enumerateImportsSync("wsf.exe")
[
  {
    "address": "0x7ff9151fe4a0",
    "module": "api-ms-win-crt-runtime-l1-1-0.dll",
    "name": "_initterm_e",
    "type": "function"
  },
  {
    "address": "0x7ff915254650",
    "module": "api-ms-win-crt-runtime-l1-1-0.dll",
    "name": "_c_exit",
    "type": "function"
  },
  {
    "address": "0x7ff915254690",
    "module": "api-ms-win-crt-runtime-l1-1-0.dll",
    "name": "_register_thread_local_exe_atexit_callback",
    "type": "function"
  },
  {
    "address": "0x7ff9151fe430",
    "module": "api-ms-win-crt-runtime-l1-1-0.dll",
    "name": "_initterm",
    "type": "function"
  },
  {
    "address": "0x7ff915203620",
    "module": "api-ms-win-crt-private-l1-1-0.dll",
    "name": "_o__configthreadlocale",
    "type": "function"
  }
]

```

# DEMO





PS C:\Users\User> frida-trace -p 22632 -s

Started tracing 0 functions. Press Ctrl+C to stop.

PS C:\Users\User> frida-trace -p 22632 -s

Instrumenting...

RpcBindingSetAuthInfoExA: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcBindingSetAuthInfoExA.js"  
NdrStubInitialize: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrStubInitialize.js"  
RpcBindingInqAuthInfoExA: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcBindingInqAuthInfoExA.js"  
pfnUnmarshalRoutines: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\pfnUnmarshalRoutines.js"  
NdrFixedArrayBufferSize: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrFixedArrayBufferSize.js"  
I\_RpcTransConnectionAllocatePacket: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\I\_RpcTransConnectionAllocatePacket.js"  
NdrConformantStructMemorySize: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrConformantStructMemorySize.js"  
RpcTestCancel: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcTestCancel.js"  
RpcBindingCreateW: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcBindingCreateW.js"  
NdrEncapsulatedUnionUnmarshal: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrEncapsulatedUnionUnmarshal.js"  
RpcBindingInqAuthClientW: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcBindingInqAuthClientW.js"  
Ndr64AsyncServerCallAll: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\Ndr64AsyncServerCallAll.js"  
I\_RpcGetCurrentCallHandle: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\I\_RpcGetCurrentCallHandle.js"  
NdrByteCountPointerMarshal: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrByteCountPointerMarshal.js"  
NdrWaitOrRepAsMarshal: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrWaitOrRepAsMarshal.js"  
RpcBindingVectorFree: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcBindingVectorFree.js"  
I\_RpcBindingInqLocalClientPID: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\I\_RpcBindingInqLocalClientPID.js"  
NdrMesTypeDecode2: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrMesTypeDecode2.js"  
I\_RpcServerCheckClientRestriction: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\I\_RpcServerCheckClientRestriction.js"  
NdrByteCountPointerBufferSize: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrByteCountPointerBufferSize.js"  
Ndr64AsyncServerCall64: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\Ndr64AsyncServerCall64.js"  
NdrGetSimpleTypeMemorySize: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrGetSimpleTypeMemorySize.js"  
NdrMesTypeDecoded: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrMesTypeDecoded.js"  
NdrOutInit: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrOutInit.js"  
DllGetClassObject: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\DllGetClassObject.js"  
NdrServerInitializeMarshal: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrServerInitializeMarshal.js"  
NdrFullPointerInsertRefId: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrFullPointerInsertRefId.js"  
NdrProxySendReceive: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrProxySendReceive.js"  
RpcBindingUnbind: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcBindingUnbind.js"  
RpcServerRegisterIfEx: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcServerRegisterIfEx.js"  
I\_RpcOpenClientProcess: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\I\_RpcOpenClientProcess.js"  
I\_RpcSystemFunction001: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\I\_RpcSystemFunction001.js"  
NdrEncapsulatedUnionMarshal: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrEncapsulatedUnionMarshal.js"  
NdrCorrelationFree: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\NdrCorrelationFree.js"  
RpcMgmtInqIfIds: Loaded handler at "C:\\Users\\User\\\_handlers\_\\RPCRT4.dll\\RpcMgmtInqIfIds.js"

# DEMO

```
PS C:\Users\user> frida-trace -p 12776 -i RegOpenKeyExW
Instrumenting...
RegOpenKeyExW: Loaded handler at "C:\Users\user\...handlers...\X86\12776.dll\RegOpenKeyExW.js"
RegOpenKeyExW: Loaded handler at "C:\Users\user\...handlers...\X86\12776.dll\RegOpenKeyExW.js"
RegOpenKeyExW: Loaded handler at "C:\Users\user\...handlers...\X86\12776.dll\RegOpenKeyExW.js"
Started tracing 3 functions. Press Ctrl+C to stop.
/* 1TD 8x8b6 */
7936 m RegOpenKeyExW()
7937 m | RegOpenKeyExW()
7937 m | | RegOpenKeyExW()
7772 m RegOpenKeyExW()
7772 m | RegOpenKeyExW()
7772 m | | RegOpenKeyExW()
7772 m RegOpenKeyExW()
7772 m | RegOpenKeyExW()
7772 m | | RegOpenKeyExW()
7772 m RegOpenKeyExW()
7772 m | RegOpenKeyExW()
7772 m | | RegOpenKeyExW()
7772 m RegOpenKeyExW()
7772 m | RegOpenKeyExW()
7772 m | | RegOpenKeyExW()
11889 m RegOpenKeyExW()
11889 m | RegOpenKeyExW()
11889 m | | RegOpenKeyExW()
11921 m RegOpenKeyExW()
11921 m | RegOpenKeyExW()
11921 m | | RegOpenKeyExW()
12193 m RegOpenKeyExW()
12193 m | RegOpenKeyExW()
12193 m | | RegOpenKeyExW()
12796 m RegOpenKeyExW()
12796 m | RegOpenKeyExW()
12796 m | | RegOpenKeyExW()
13513 m RegOpenKeyExW()
13513 m | RegOpenKeyExW()
13513 m | | RegOpenKeyExW()
```



## DEMO-2

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\User> tasklist | Select-String "not"

notepad.exe                24568 Console                1      6,092 K
notepad.exe                5124 Console                1      6,732 K
notepad.exe                24160 Console                1      6,360 K

PS C:\Users\User> frida -p 5124

Frida 15.1.10 - A world-class dynamic instrumentation toolkit

Commands:
  help           -> Displays the help system
  object?       -> Display information about 'object'
  exit/quit     -> Exit

More info at https://frida.re/docs/home/

[local::PID::5124]-> var mod = Module.getExportByName(null, "ntkernel.dll");
Interceptor.attach(mod, {
  onEnter: function(args) {
    console.log("[*] [kernel] Console Dump: " + hexdump(args[1]));
  }
});
[local::PID::5124]->
```

## DEMO-2



## DEMO-2

```
1fa5d3cf000 10 50 33 39 60 31 1b 50 33 39 60 32 1b 50 33 39 .[39m1.[39m2.[39
1fa5d3cf000 00 33 1b 50 33 39 60 22 3a 2f 60 60 70 2f 63 2f w3.[39m"/mnt/c/
1fa5d3cf000 55 73 65 72 73 2f 55 73 65 72 67 00 00 00 00 00 Users/User.....
1fa5d3cf000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Terminal Console Dump:
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
1fa5d3cf000 1b 50 32 1b 73 73 60 20 72 6f 6f 70 00 32 32 37 .[32;ash root@127
1fa5d3cf010 20 30 20 30 20 31 20 2f 50 20 22 50 61 73 73 40 .0.0.1 -P "Pass0
1fa5d3cf020 32 32 32 22 07 1b 50 31 30 72 6f 6f 70 00 32 32 223"...[1;root@12
1fa5d3cf030 37 20 30 20 30 20 31 07 33 39 60 20 1b 50 33 39 7.0.0.1.39m0.[39
1fa5d3cf040 60 20 1b 50 33 39 60 30 1b 50 33 39 60 20 1b 50 m..[39m0.[39m..[
1fa5d3cf050 33 39 60 31 1b 50 33 39 60 20 1b 50 33 39 60 20 39m1.[39m..[39m-
1fa5d3cf060 1b 50 33 39 60 30 1b 50 33 39 60 20 1b 50 33 39 .[39mP.[39m..[39
1fa5d3cf070 60 22 1b 50 33 39 60 50 1b 50 33 39 60 61 1b 50 w".[39mP.[39m..[39
1fa5d3cf080 33 39 60 73 1b 50 33 39 60 73 1b 50 33 39 60 40 39m..[39m..[39m0
1fa5d3cf090 1b 50 33 39 60 31 1b 50 33 39 60 32 1b 50 33 39 .[39m1.[39m2.[39
1fa5d3cf0a0 60 33 1b 50 33 39 60 22 3a 2f 60 60 70 2f 63 2f w3.[39m"/mnt/c/
1fa5d3cf0b0 55 73 65 72 73 2f 55 73 65 72 67 00 00 00 00 00 Users/User.....
1fa5d3cf0c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf0d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf0e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf0f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Terminal Console Dump:
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
1fa5d3cf000 73 73 65 3a 20 63 6f 60 60 65 63 70 20 70 6f 20 ash: connect to
1fa5d3cf010 00 0f 73 70 20 32 32 3a 20 4f 6f 60 60 65 63 70 69 host 127.0.0.1 p
1fa5d3cf020 0f 72 70 20 32 32 3a 20 4f 6f 60 60 65 63 70 69 rt 22: Connecti
1fa5d3cf030 0f 60 20 72 65 66 73 73 65 64 0d 0d 0a 5b 33 30 on refused...[39
1fa5d3cf040 60 20 1b 50 33 39 60 30 1b 50 33 39 60 20 1b 50 m..[39m0.[39m..[
1fa5d3cf050 33 39 60 31 1b 50 33 39 60 20 1b 50 33 39 60 20 39m1.[39m..[39m-
1fa5d3cf060 1b 50 33 39 60 30 1b 50 33 39 60 20 1b 50 33 39 .[39mP.[39m..[39
1fa5d3cf070 60 22 1b 50 33 39 60 50 1b 50 33 39 60 61 1b 50 w".[39mP.[39m..[39
1fa5d3cf080 33 39 60 73 1b 50 33 39 60 73 1b 50 33 39 60 40 39m..[39m..[39m0
1fa5d3cf090 1b 50 33 39 60 31 1b 50 33 39 60 32 1b 50 33 39 .[39m1.[39m2.[39
1fa5d3cf0a0 60 33 1b 50 33 39 60 22 3a 2f 60 60 70 2f 63 2f w3.[39m"/mnt/c/
1fa5d3cf0b0 55 73 65 72 73 2f 55 73 65 72 67 00 00 00 00 00 Users/User.....
1fa5d3cf0c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf0d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf0e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1fa5d3cf0f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

0.427 1.10
```



# Hooking WriteFile

```
var mod = Module.getExportByName(null, "WriteFile");  
Interceptor.attach(mod, {  
    onEnter: function(args)  
    {  
        console.log("\nTerminal Console Dump:\n" + hexdump(args[1]));  
    }  
});
```



# Installing Frida on Mobile Devices

Frida installation on android devices

Download frida-server from releases page

 <a href="#">frida-server-15.1.14-android-arm.xz</a>	6.54 MB
 <a href="#">frida-server-15.1.14-android-arm64.xz</a>	14 MB
 <a href="#">frida-server-15.1.14-android-x86.xz</a>	13.8 MB
 <a href="#">frida-server-15.1.14-android-x86_64.xz</a>	28 MB



# Installing Frida on Mobile Devices


```
$ adb root
```

```
$ adb push frida-server /data/local/tmp/
```


```
$ adb shell "chmod 755 /data/local/tmp/frida-server"
```

```
$ adb shell "/data/local/tmp/frida-server &"
```





```
try {  
    // Bypass Trustkit {}  
  
    const trustkit_Activity_1 =  
    Java.use('com.datatheorem.android.trustkit.pinning.OkHostnameVerifier');  
  
    trustkit_Activity_1.verify.overload('java.lang.String',  
    'javax.net.ssl.SSLSession').implementation = function (a, b) {  
  
        console.log(' --> Bypassing Trustkit OkHostnameVerifier(SSLSession): ' + a);  
  
        return true;  
  
    };  
  
    console.log('[+] Trustkit OkHostnameVerifier(SSLSession)');  
} catch (err) {  
  
    console.log('[ ] Trustkit OkHostnameVerifier(SSLSession)');  
  
}
```



## References

- <https://frida.re/docs/>
- <https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-writefile>
- <https://www.fuzzysecurity.com/tutorials/29.html>
- <https://www.ired.team/miscellaneous-reversing-forensics/windows-kernel-internals/installing-windows-apis-with-frida>
- <https://github.com/http Toolkit/frida-android-unpinning/blob/main/frida-script.js>
- :)