Forecast Modification for Better Performance

1.What we get from Volatility

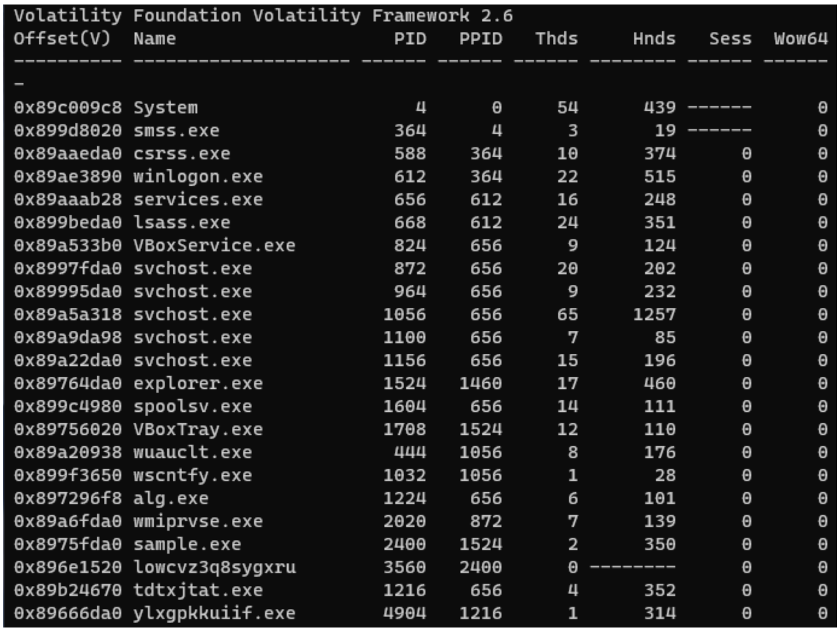
The malware sample used for this document is “Nivdort”. It’s a windows executable named “sample.exe” that pretends to help user downloading pictures from the internet while doing despicable activities in the background.

To begin with, let’s try to analyze the malware in Volatility. I ran sample.exe in a 32-bit Windows XP virtual machine, then got the virtual machine memory dump (named sample.bin), and then analyzed the dump file by Volatility standalone for Windows system.

First, we can run Volatility `pslist` plugin to see all processes running on the machine,

```
.\volatility_2.6_win64_standalone -f sample.bin --profile=WinXPSP3x86 pslist
```

we can get the result that is shown in the figure below.

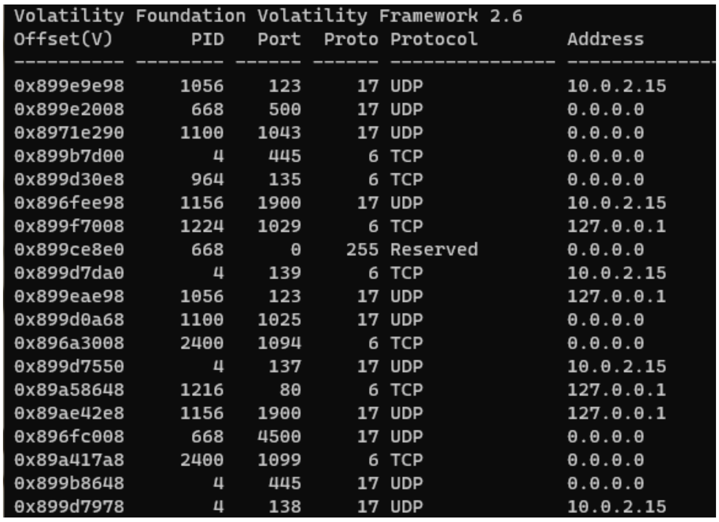


```
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64
---------- -------------------- ------ ------ ------ -------- ------ ------
-
0x89c009c8 System                    4      0     54      439 ------      0
0x899d8020 smss.exe                364      4      3       19 ------      0
0x89aaeda0 csrss.exe               588    364     10      374      0      0
0x89ae3890 winlogon.exe            612    364     22      515      0      0
0x89aaab28 services.exe            656    612     16      248      0      0
0x899beda0 lsass.exe               668    612     24      351      0      0
0x89a533b0 VBoxService.exe         824    656      9      124      0      0
0x8997fda0 svchost.exe             872    656     20      202      0      0
0x89995da0 svchost.exe             964    656      9      232      0      0
0x89a5a318 svchost.exe            1056    656     65     1257      0      0
0x89a9da98 svchost.exe            1100    656      7       85      0      0
0x89a22da0 svchost.exe            1156    656     15      196      0      0
0x89764da0 explorer.exe           1524   1460     17      460      0      0
0x899c4980 spoolsv.exe            1604    656     14      111      0      0
0x89756020 VBoxTray.exe           1708   1524     12      110      0      0
0x89a20938 wuauclt.exe             444   1056      8      176      0      0
0x899f3650 wscntfy.exe            1032   1056      1       28      0      0
0x897296f8 alg.exe                1224    656      6      101      0      0
0x89a6fda0 wmiprvse.exe           2020    872      7      139      0      0
0x8975fda0 sample.exe             2400   1524      2      350      0      0
0x896e1520 lowcvz3q8sygxru        3560   2400      0 --------      0      0
0x89b24670 tdtxjtat.exe           1216    656      4      352      0      0
0x89666da0 ylxgpkkuiif.exe        4904   1216      1      314      0      0
```

As we can see from the result, malware sample.exe has PID=2400, and “lowcvz3q8syqxru”, “tdtxjtat.exe” and “ylxgpkkuiif.exe” are all processes belonging to the malware. Our next step is to ask Volatility to print the list of all open sockets

```
.\volatility_2.6_win64_standalone -f sample.bin --profile=WinXPSP3x86 sockets
```

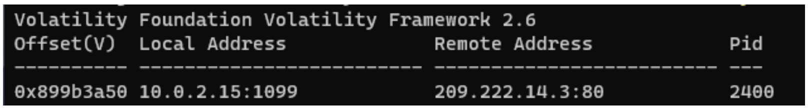
The result can be seen in the figure below. Among the entire list of open sockets, we can see that the malware executable “sample.exe”, whose PID is 2400, has established an open socket for communication.



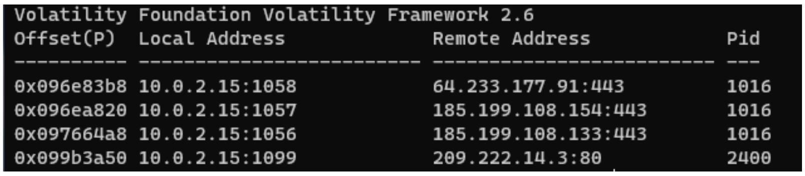
```
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address
---------- -------- ------ ------ --------------- -------------
0x899e9e98     1056    123     17 UDP             10.0.2.15
0x899e2008      668    500     17 UDP             0.0.0.0
0x8971e290     1100   1043     17 UDP             0.0.0.0
0x899b7d00        4    445      6 TCP             0.0.0.0
0x899d30e8      964    135      6 TCP             0.0.0.0
0x896fee98     1156   1900     17 UDP             10.0.2.15
0x899f7008     1224   1029      6 TCP             127.0.0.1
0x899ce8e0      668      0    255 Reserved        0.0.0.0
0x899d7da0        4    139      6 TCP             10.0.2.15
0x899eae98     1056    123     17 UDP             127.0.0.1
0x899d0a68     1100   1025     17 UDP             0.0.0.0
0x896a3008     2400   1094      6 TCP             0.0.0.0
0x899d7550        4    137     17 UDP             10.0.2.15
0x89a58648     1216     80      6 TCP             127.0.0.1
0x89ae42e8     1156   1900     17 UDP             127.0.0.1
0x896fc008      668   4500     17 UDP             0.0.0.0
0x89a417a8     2400   1099      6 TCP             0.0.0.0
0x899b8648        4    445     17 UDP             0.0.0.0
0x899d7978        4    138     17 UDP             10.0.2.15
```

To see the connection in detail we can use `connections` plugin and `connscan` plugin

```
.\volatility_2.6_win64_standalone -f sample.bin --profile=WinXPSP3x86 connections
.\volatility_2.6_win64_standalone -f sample.bin --profile=WinXPSP3x86 connscan
```



```
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x899b3a50 10.0.2.15:1099            209.222.14.3:80           2400
```



```
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x096e83b8 10.0.2.15:1058            64.233.177.91:443         1016
0x096ea820 10.0.2.15:1057            185.199.108.154:443       1016
0x097664a8 10.0.2.15:1056            185.199.108.133:443       1016
0x099b3a50 10.0.2.15:1099            209.222.14.3:80           2400
```

We can see that process with PID=2400 (sample.exe) is communicating via port 1099, with remote address 209.222.14.3. (Port=80 means they are communicating by http).

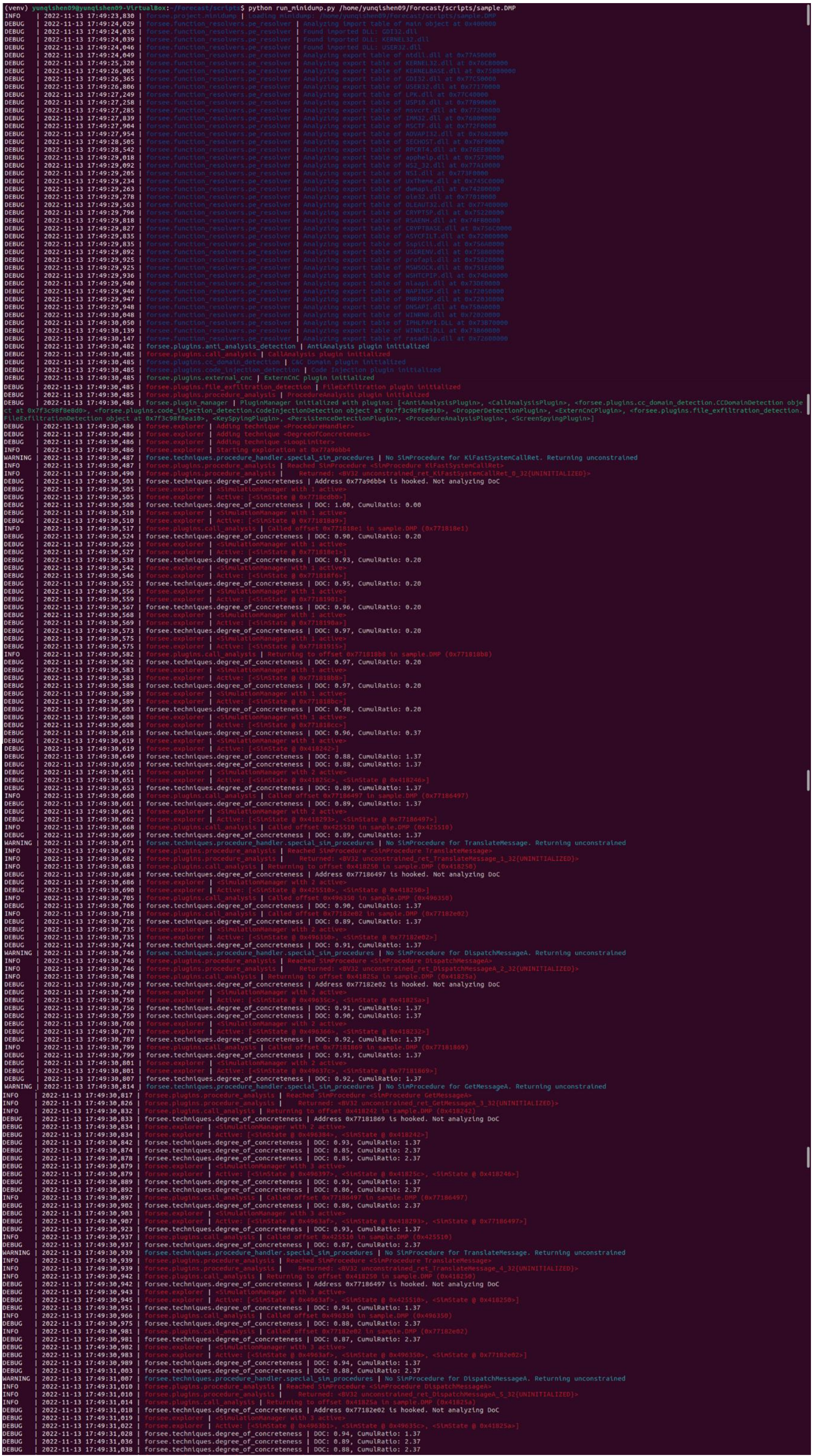
PS: I didn't use Windows 7 virtual machine in this part because Volatility doesn't support analyzing socket and connection of dump files from Windows 7 system.

2.Forecast failed to detect socket communication

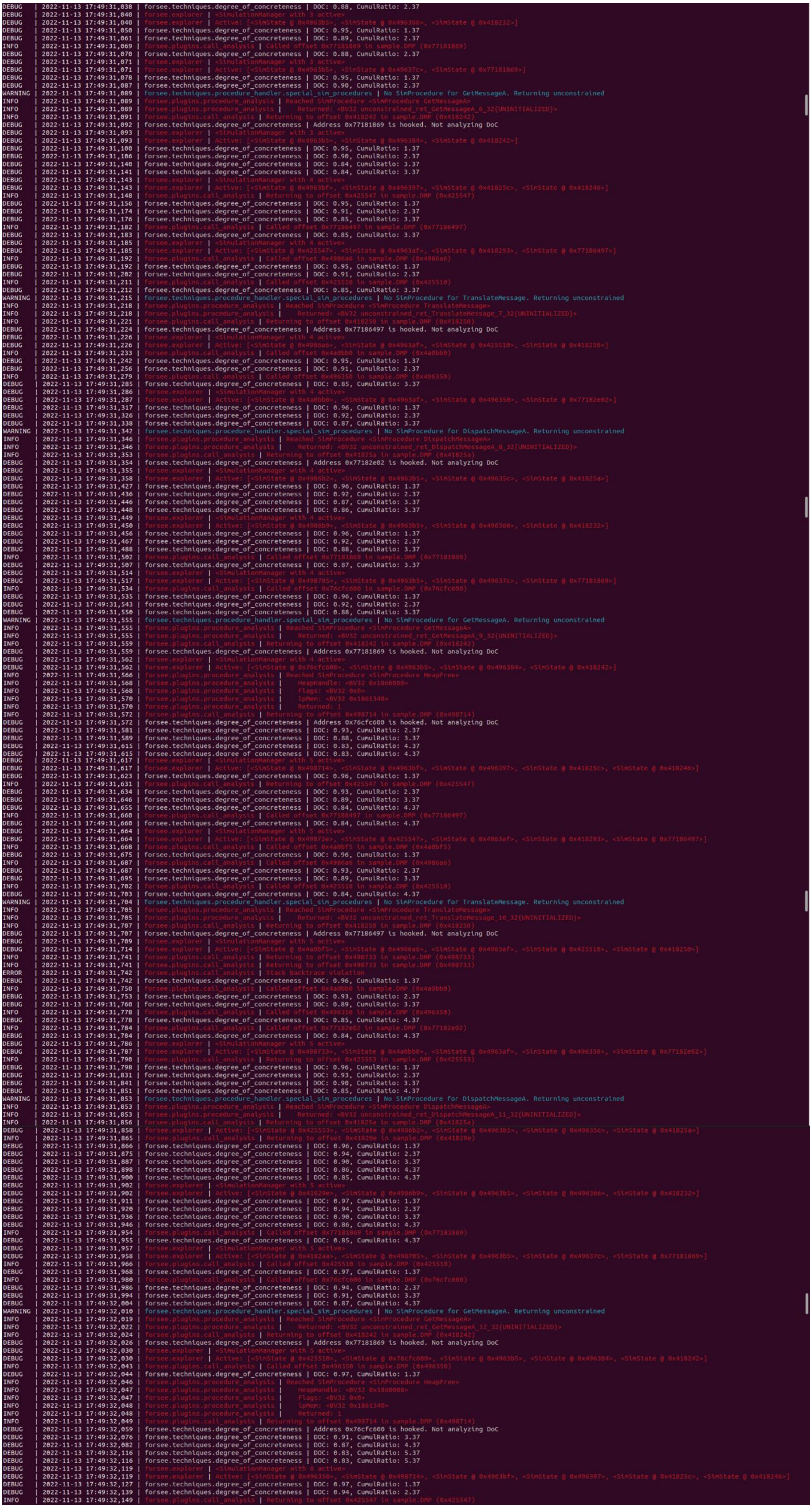
In this part, the malware was run on a 32-bit Windows 7 virtual machine, and the malware dump file was created by task manager of Windows system (and named as "sample.DMP"). After setting up Forecast and creating virtual environment in an Ubuntu 18.04 virtual machine, we can let Forecast to analyze the dump file

```
$ python run_minidump.py /home/yunqishen09/Forecast/scripts/sample.DMP
```

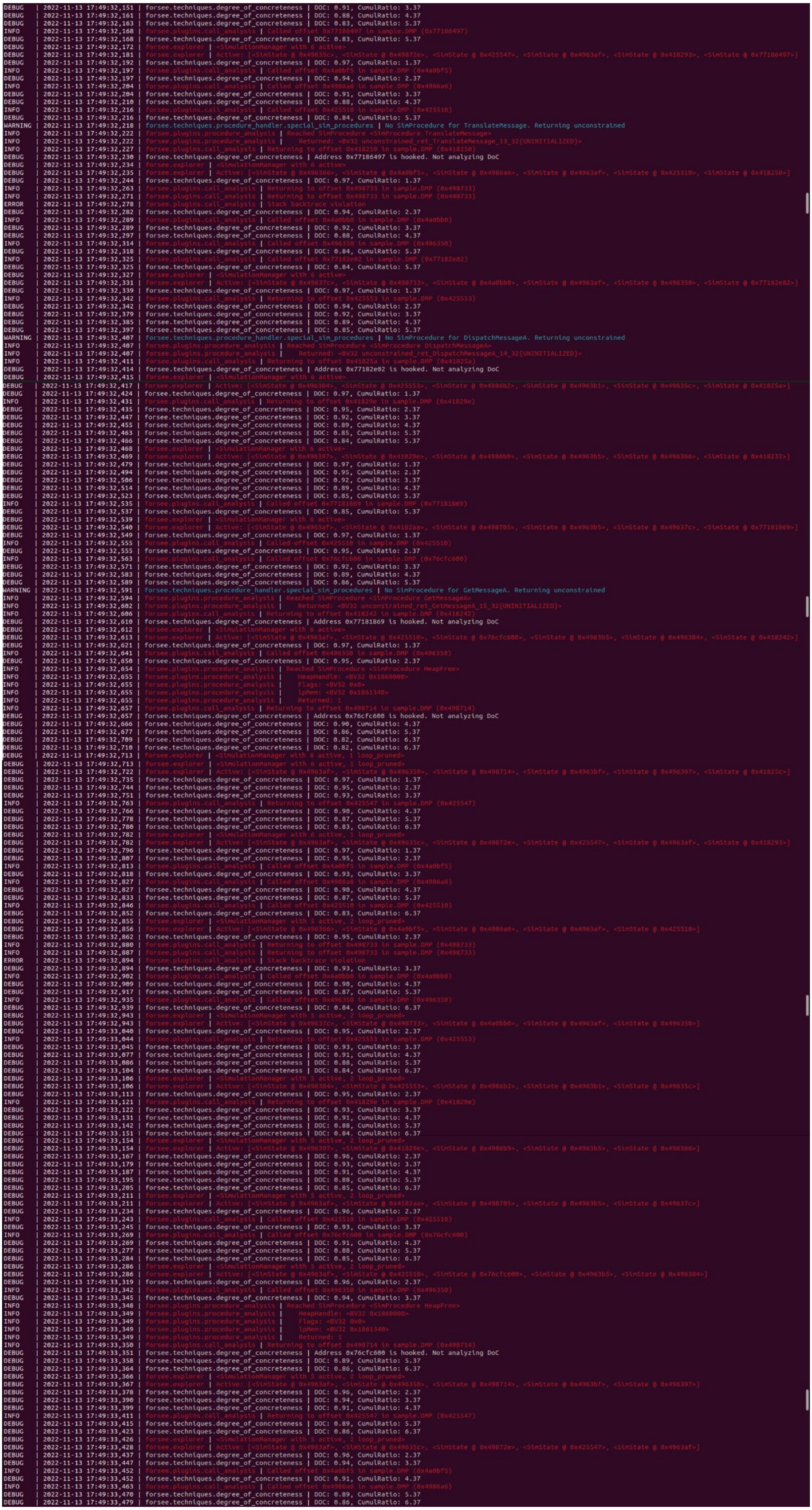
The result can be seen in pages below.



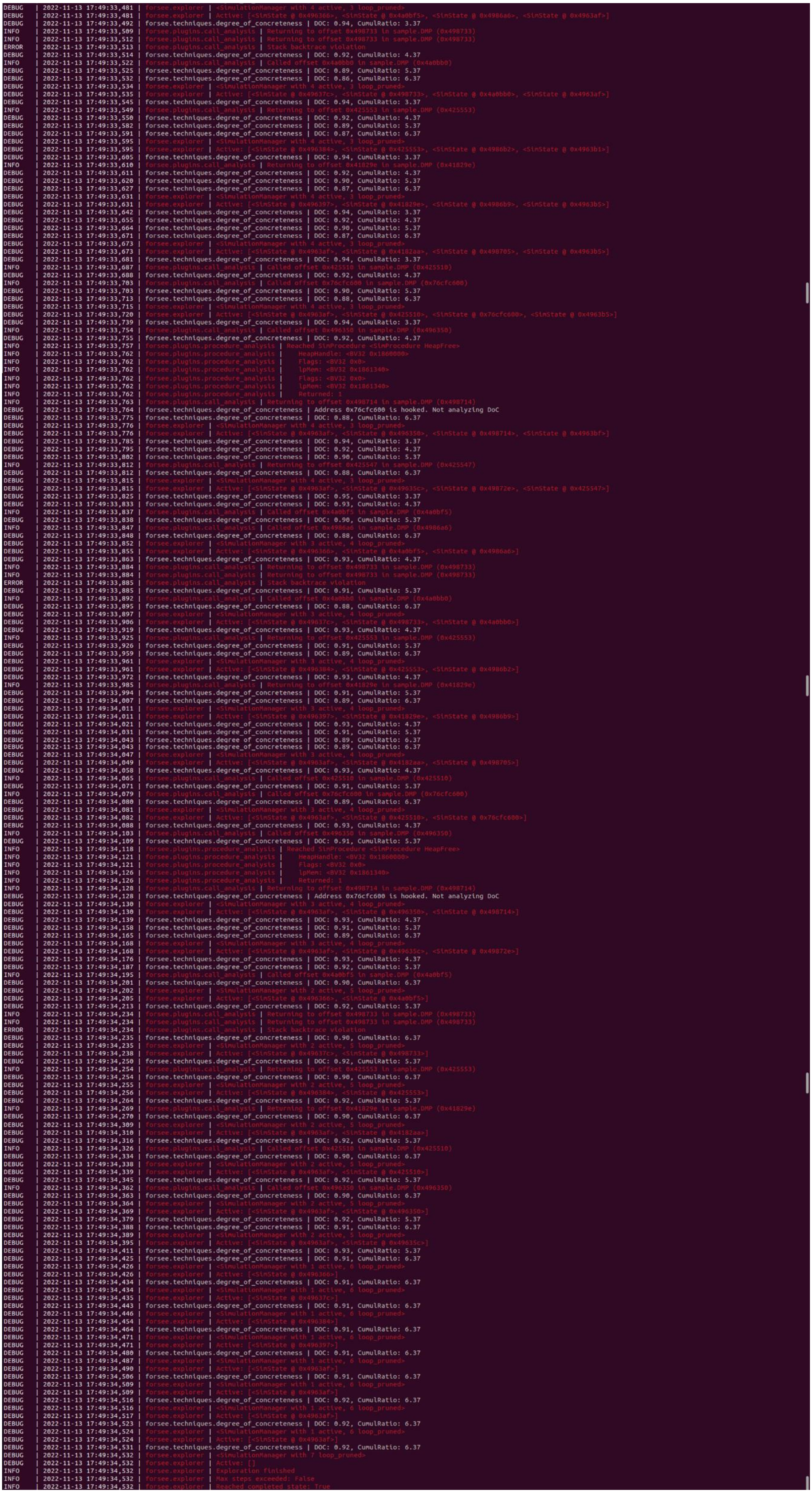
```
(venv) yunqishen09@yunqishen09-VirtualBox:~/Forecast/scripts$ python run_minidump.py /home/yunqishen09/Forecast/scripts/sample.DMP
INFO     | 2022-11-13 17:49:23,830 | forsee.project.minidump | Loading minidump: /home/yunqishen09/Forecast/scripts/sample.DMP
DEBUG    | 2022-11-13 17:49:24,029 | forsee.function_resolvers.pe_resolver | Analyzing import table of main object at 0x400000
DEBUG    | 2022-11-13 17:49:24,035 | forsee.function_resolvers.pe_resolver | Found imported DLL: GDI32.dll
DEBUG    | 2022-11-13 17:49:24,039 | forsee.function_resolvers.pe_resolver | Found imported DLL: KERNEL32.dll
DEBUG    | 2022-11-13 17:49:24,046 | forsee.function_resolvers.pe_resolver | Found imported DLL: USER32.dll
DEBUG    | 2022-11-13 17:49:24,049 | forsee.function_resolvers.pe_resolver | Analyzing export table of ntdll.dll at 0x77A50000
DEBUG    | 2022-11-13 17:49:25,320 | forsee.function_resolvers.pe_resolver | Analyzing export table of KERNEL32.dll at 0x76CB0000
DEBUG    | 2022-11-13 17:49:26,005 | forsee.function_resolvers.pe_resolver | Analyzing export table of KERNELBASE.dll at 0x75880000
DEBUG    | 2022-11-13 17:49:26,365 | forsee.function_resolvers.pe_resolver | Analyzing export table of GDI32.dll at 0x77C50000
DEBUG    | 2022-11-13 17:49:26,806 | forsee.function_resolvers.pe_resolver | Analyzing export table of USER32.dll at 0x77170000
DEBUG    | 2022-11-13 17:49:27,249 | forsee.function_resolvers.pe_resolver | Analyzing export table of LPK.dll at 0x77C40000
DEBUG    | 2022-11-13 17:49:27,258 | forsee.function_resolvers.pe_resolver | Analyzing export table of USP10.dll at 0x77890000
DEBUG    | 2022-11-13 17:49:27,285 | forsee.function_resolvers.pe_resolver | Analyzing export table of msvcrt.dll at 0x77240000
DEBUG    | 2022-11-13 17:49:27,839 | forsee.function_resolvers.pe_resolver | Analyzing export table of IMM32.dll at 0x76800000
DEBUG    | 2022-11-13 17:49:27,904 | forsee.function_resolvers.pe_resolver | Analyzing export table of MSCTF.dll at 0x772F0000
DEBUG    | 2022-11-13 17:49:27,954 | forsee.function_resolvers.pe_resolver | Analyzing export table of ADVAPI32.dll at 0x76820000
DEBUG    | 2022-11-13 17:49:28,505 | forsee.function_resolvers.pe_resolver | Analyzing export table of SECHOST.dll at 0x76F90000
DEBUG    | 2022-11-13 17:49:28,542 | forsee.function_resolvers.pe_resolver | Analyzing export table of RPCRT4.dll at 0x76EE0000
DEBUG    | 2022-11-13 17:49:29,018 | forsee.function_resolvers.pe_resolver | Analyzing export table of apphelp.dll at 0x75730000
DEBUG    | 2022-11-13 17:49:29,092 | forsee.function_resolvers.pe_resolver | Analyzing export table of WS2_32.dll at 0x77A10000
DEBUG    | 2022-11-13 17:49:29,205 | forsee.function_resolvers.pe_resolver | Analyzing export table of NSI.dll at 0x773F0000
DEBUG    | 2022-11-13 17:49:29,234 | forsee.function_resolvers.pe_resolver | Analyzing export table of UxTheme.dll at 0x745C0000
DEBUG    | 2022-11-13 17:49:29,263 | forsee.function_resolvers.pe_resolver | Analyzing export table of dwmapi.dll at 0x74280000
DEBUG    | 2022-11-13 17:49:29,278 | forsee.function_resolvers.pe_resolver | Analyzing export table of ole32.dll at 0x77010000
DEBUG    | 2022-11-13 17:49:29,563 | forsee.function_resolvers.pe_resolver | Analyzing export table of OLEAUT32.dll at 0x77400000
DEBUG    | 2022-11-13 17:49:29,796 | forsee.function_resolvers.pe_resolver | Analyzing export table of CRYPTSP.dll at 0x75220000
DEBUG    | 2022-11-13 17:49:29,818 | forsee.function_resolvers.pe_resolver | Analyzing export table of RSAENH.dll at 0x74FB0000
DEBUG    | 2022-11-13 17:49:29,827 | forsee.function_resolvers.pe_resolver | Analyzing export table of CRYPTBASE.dll at 0x756C0000
DEBUG    | 2022-11-13 17:49:29,835 | forsee.function_resolvers.pe_resolver | Analyzing export table of ASYCFILT.dll at 0x72000000
DEBUG    | 2022-11-13 17:49:29,835 | forsee.function_resolvers.pe_resolver | Analyzing export table of SspiCli.dll at 0x756A0000
DEBUG    | 2022-11-13 17:49:29,892 | forsee.function_resolvers.pe_resolver | Analyzing export table of USERENV.dll at 0x75880000
DEBUG    | 2022-11-13 17:49:29,925 | forsee.function_resolvers.pe_resolver | Analyzing export table of profapi.dll at 0x75820000
DEBUG    | 2022-11-13 17:49:29,925 | forsee.function_resolvers.pe_resolver | Analyzing export table of MSWSOCK.dll at 0x751E0000
DEBUG    | 2022-11-13 17:49:29,936 | forsee.function_resolvers.pe_resolver | Analyzing export table of WSHTCPIP.dll at 0x74D40000
DEBUG    | 2022-11-13 17:49:29,940 | forsee.function_resolvers.pe_resolver | Analyzing export table of nlaapi.dll at 0x730E0000
DEBUG    | 2022-11-13 17:49:29,946 | forsee.function_resolvers.pe_resolver | Analyzing export table of NAPINSP.dll at 0x72050000
DEBUG    | 2022-11-13 17:49:29,947 | forsee.function_resolvers.pe_resolver | Analyzing export table of PNRPNSP.dll at 0x72030000
DEBUG    | 2022-11-13 17:49:29,948 | forsee.function_resolvers.pe_resolver | Analyzing export table of DNSAPI.dll at 0x750A0000
DEBUG    | 2022-11-13 17:49:30,048 | forsee.function_resolvers.pe_resolver | Analyzing export table of WINRNR.dll at 0x72020000
DEBUG    | 2022-11-13 17:49:30,050 | forsee.function_resolvers.pe_resolver | Analyzing export table of IPHLPAPI.DLL at 0x73B70000
DEBUG    | 2022-11-13 17:49:30,139 | forsee.function_resolvers.pe_resolver | Analyzing export table of WINNSI.DLL at 0x73B60000
DEBUG    | 2022-11-13 17:49:30,147 | forsee.function_resolvers.pe_resolver | Analyzing export table of rasadhlp.dll at 0x72600000
DEBUG    | 2022-11-13 17:49:30,482 | forsee.plugins.anti_analysis_detection | AntiAnalysis plugin initialized
DEBUG    | 2022-11-13 17:49:30,485 | forsee.plugins.call_analysis | CallAnalysis plugin initialized
DEBUG    | 2022-11-13 17:49:30,485 | forsee.plugins.cc_domain_detection | C&C Domain plugin initialized
DEBUG    | 2022-11-13 17:49:30,485 | forsee.plugins.code_injection_detection | Code Injection plugin initialized
DEBUG    | 2022-11-13 17:49:30,485 | forsee.plugins.external_cnc | ExternCnC plugin initialized
DEBUG    | 2022-11-13 17:49:30,485 | forsee.plugins.file_exfiltration_detection | FileExfiltration plugin initialized
DEBUG    | 2022-11-13 17:49:30,485 | forsee.plugins.procedure_analysis | ProcedureAnalysis plugin initialized
DEBUG    | 2022-11-13 17:49:30,486 | forsee.plugin_manager | PluginManager initialized with plugins: [<AntiAnalysisPlugin>, <CallAnalysisPlugin>, <forsee.plugins.cc_domain_detection.CCDomainDetection obje
ct at 0x7f3c98f8e8d0>, <forsee.plugins.code_injection_detection.CodeInjectionDetection object at 0x7f3c98f8e910>, <DropperDetectionPlugin>, <ExternCnCPlugin>, <forsee.plugins.file_exfiltration_detection.
FileExfiltrationDetection object at 0x7f3c98f8ea10>, <KeySpyingPlugin>, <PersistenceDetectionPlugin>, <ProcedureAnalysisPlugin>, <ScreenSpyingPlugin>]
DEBUG    | 2022-11-13 17:49:30,486 | forsee.explorer | Adding technique <ProcedureHandler>
DEBUG    | 2022-11-13 17:49:30,486 | forsee.explorer | Adding technique <DegreeOfConcreteness>
DEBUG    | 2022-11-13 17:49:30,486 | forsee.explorer | Adding technique <LoopLimiter>
INFO     | 2022-11-13 17:49:30,486 | forsee.explorer | Starting exploration at 0x77a96bb4
WARNING  | 2022-11-13 17:49:30,487 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for KiFastSystemCallRet. Returning unconstrained
INFO     | 2022-11-13 17:49:30,487 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure KiFastSystemCallRet>
INFO     | 2022-11-13 17:49:30,490 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_KiFastSystemCallRet_0_32{UNINITIALIZED}>
DEBUG    | 2022-11-13 17:49:30,503 | forsee.techniques.degree_of_concreteness | Address 0x77a96bb4 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:30,505 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,505 | forsee.explorer | Active: [<SimState @ 0x7718cdb0>]
DEBUG    | 2022-11-13 17:49:30,508 | forsee.techniques.degree_of_concreteness | DOC: 1.00, CumulRatio: 0.00
DEBUG    | 2022-11-13 17:49:30,510 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,510 | forsee.explorer | Active: [<SimState @ 0x771818a9>]
INFO     | 2022-11-13 17:49:30,517 | forsee.plugins.call_analysis | Called offset 0x771818e1 in sample.DMP (0x771818e1)
DEBUG    | 2022-11-13 17:49:30,524 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 0.20
DEBUG    | 2022-11-13 17:49:30,526 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,527 | forsee.explorer | Active: [<SimState @ 0x771818e1>]
DEBUG    | 2022-11-13 17:49:30,538 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 0.20
DEBUG    | 2022-11-13 17:49:30,542 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,546 | forsee.explorer | Active: [<SimState @ 0x771818f6>]
DEBUG    | 2022-11-13 17:49:30,552 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 0.20
DEBUG    | 2022-11-13 17:49:30,556 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,559 | forsee.explorer | Active: [<SimState @ 0x77181901>]
DEBUG    | 2022-11-13 17:49:30,567 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 0.20
DEBUG    | 2022-11-13 17:49:30,568 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,569 | forsee.explorer | Active: [<SimState @ 0x7718190a>]
DEBUG    | 2022-11-13 17:49:30,573 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 0.20
DEBUG    | 2022-11-13 17:49:30,575 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,575 | forsee.explorer | Active: [<SimState @ 0x77181915>]
INFO     | 2022-11-13 17:49:30,582 | forsee.plugins.call_analysis | Returning to offset 0x771818b8 in sample.DMP (0x771818b8)
DEBUG    | 2022-11-13 17:49:30,582 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 0.20
DEBUG    | 2022-11-13 17:49:30,583 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,583 | forsee.explorer | Active: [<SimState @ 0x771818b8>]
DEBUG    | 2022-11-13 17:49:30,588 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 0.20
DEBUG    | 2022-11-13 17:49:30,589 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,589 | forsee.explorer | Active: [<SimState @ 0x771818bc>]
DEBUG    | 2022-11-13 17:49:30,603 | forsee.techniques.degree_of_concreteness | DOC: 0.98, CumulRatio: 0.20
DEBUG    | 2022-11-13 17:49:30,608 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,608 | forsee.explorer | Active: [<SimState @ 0x771818cc>]
DEBUG    | 2022-11-13 17:49:30,618 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 0.37
DEBUG    | 2022-11-13 17:49:30,619 | forsee.explorer | <SimulationManager with 1 active>
DEBUG    | 2022-11-13 17:49:30,619 | forsee.explorer | Active: [<SimState @ 0x418242>]
DEBUG    | 2022-11-13 17:49:30,649 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,650 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,651 | forsee.explorer | <SimulationManager with 2 active>
DEBUG    | 2022-11-13 17:49:30,651 | forsee.explorer | Active: [<SimState @ 0x41825c>, <SimState @ 0x418246>]
DEBUG    | 2022-11-13 17:49:30,653 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:30,660 | forsee.plugins.call_analysis | Called offset 0x77186497 in sample.DMP (0x77186497)
DEBUG    | 2022-11-13 17:49:30,661 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,661 | forsee.explorer | <SimulationManager with 2 active>
DEBUG    | 2022-11-13 17:49:30,662 | forsee.explorer | Active: [<SimState @ 0x418293>, <SimState @ 0x77186497>]
INFO     | 2022-11-13 17:49:30,668 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:30,669 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 1.37
WARNING  | 2022-11-13 17:49:30,671 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for TranslateMessage. Returning unconstrained
INFO     | 2022-11-13 17:49:30,679 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure TranslateMessage>
INFO     | 2022-11-13 17:49:30,682 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_TranslateMessage_1_32{UNINITIALIZED}>
INFO     | 2022-11-13 17:49:30,683 | forsee.plugins.call_analysis | Returning to offset 0x418250 in sample.DMP (0x418250)
DEBUG    | 2022-11-13 17:49:30,684 | forsee.techniques.degree_of_concreteness | Address 0x77186497 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:30,686 | forsee.explorer | <SimulationManager with 2 active>
DEBUG    | 2022-11-13 17:49:30,690 | forsee.explorer | Active: [<SimState @ 0x425510>, <SimState @ 0x418250>]
INFO     | 2022-11-13 17:49:30,705 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:30,706 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:30,718 | forsee.plugins.call_analysis | Called offset 0x77182e02 in sample.DMP (0x77182e02)
DEBUG    | 2022-11-13 17:49:30,726 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,735 | forsee.explorer | <SimulationManager with 2 active>
DEBUG    | 2022-11-13 17:49:30,735 | forsee.explorer | Active: [<SimState @ 0x496350>, <SimState @ 0x77182e02>]
DEBUG    | 2022-11-13 17:49:30,744 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 1.37
WARNING  | 2022-11-13 17:49:30,746 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for DispatchMessageA. Returning unconstrained
INFO     | 2022-11-13 17:49:30,746 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure DispatchMessageA>
INFO     | 2022-11-13 17:49:30,746 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_DispatchMessageA_2_32{UNINITIALIZED}>
INFO     | 2022-11-13 17:49:30,748 | forsee.plugins.call_analysis | Returning to offset 0x41825a in sample.DMP (0x41825a)
DEBUG    | 2022-11-13 17:49:30,749 | forsee.techniques.degree_of_concreteness | Address 0x77182e02 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:30,749 | forsee.explorer | <SimulationManager with 2 active>
DEBUG    | 2022-11-13 17:49:30,750 | forsee.explorer | Active: [<SimState @ 0x49635c>, <SimState @ 0x41825a>]
DEBUG    | 2022-11-13 17:49:30,756 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,759 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,760 | forsee.explorer | <SimulationManager with 2 active>
DEBUG    | 2022-11-13 17:49:30,770 | forsee.explorer | Active: [<SimState @ 0x496366>, <SimState @ 0x418232>]
DEBUG    | 2022-11-13 17:49:30,787 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:30,799 | forsee.plugins.call_analysis | Called offset 0x77181869 in sample.DMP (0x77181869)
DEBUG    | 2022-11-13 17:49:30,799 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,801 | forsee.explorer | <SimulationManager with 2 active>
DEBUG    | 2022-11-13 17:49:30,801 | forsee.explorer | Active: [<SimState @ 0x49637c>, <SimState @ 0x77181869>]
DEBUG    | 2022-11-13 17:49:30,807 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 1.37
WARNING  | 2022-11-13 17:49:30,814 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for GetMessageA. Returning unconstrained
INFO     | 2022-11-13 17:49:30,817 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure GetMessageA>
INFO     | 2022-11-13 17:49:30,826 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_GetMessageA_3_32{UNINITIALIZED}>
INFO     | 2022-11-13 17:49:30,832 | forsee.plugins.call_analysis | Returning to offset 0x418242 in sample.DMP (0x418242)
DEBUG    | 2022-11-13 17:49:30,833 | forsee.techniques.degree_of_concreteness | Address 0x77181869 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:30,834 | forsee.explorer | <SimulationManager with 2 active>
DEBUG    | 2022-11-13 17:49:30,834 | forsee.explorer | Active: [<SimState @ 0x496384>, <SimState @ 0x418242>]
DEBUG    | 2022-11-13 17:49:30,842 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,874 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:30,878 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:30,879 | forsee.explorer | <SimulationManager with 3 active>
DEBUG    | 2022-11-13 17:49:30,879 | forsee.explorer | Active: [<SimState @ 0x496397>, <SimState @ 0x41825c>, <SimState @ 0x418246>]
DEBUG    | 2022-11-13 17:49:30,889 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:30,892 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:30,897 | forsee.plugins.call_analysis | Called offset 0x77186497 in sample.DMP (0x77186497)
DEBUG    | 2022-11-13 17:49:30,902 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:30,903 | forsee.explorer | <SimulationManager with 3 active>
DEBUG    | 2022-11-13 17:49:30,907 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x418293>, <SimState @ 0x77186497>]
DEBUG    | 2022-11-13 17:49:30,923 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:30,937 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:30,937 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 2.37
WARNING  | 2022-11-13 17:49:30,939 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for TranslateMessage. Returning unconstrained
INFO     | 2022-11-13 17:49:30,939 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure TranslateMessage>
INFO     | 2022-11-13 17:49:30,939 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_TranslateMessage_4_32{UNINITIALIZED}>
INFO     | 2022-11-13 17:49:30,942 | forsee.plugins.call_analysis | Returning to offset 0x418250 in sample.DMP (0x418250)
DEBUG    | 2022-11-13 17:49:30,942 | forsee.techniques.degree_of_concreteness | Address 0x77186497 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:30,943 | forsee.explorer | <SimulationManager with 3 active>
DEBUG    | 2022-11-13 17:49:30,945 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x425510>, <SimState @ 0x418250>]
DEBUG    | 2022-11-13 17:49:30,951 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:30,966 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:30,975 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:30,981 | forsee.plugins.call_analysis | Called offset 0x77182e02 in sample.DMP (0x77182e02)
DEBUG    | 2022-11-13 17:49:30,981 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:30,982 | forsee.explorer | <SimulationManager with 3 active>
DEBUG    | 2022-11-13 17:49:30,983 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x496350>, <SimState @ 0x77182e02>]
DEBUG    | 2022-11-13 17:49:30,989 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:31,003 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 2.37
WARNING  | 2022-11-13 17:49:31,007 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for DispatchMessageA. Returning unconstrained
INFO     | 2022-11-13 17:49:31,010 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure DispatchMessageA>
INFO     | 2022-11-13 17:49:31,010 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_DispatchMessageA_5_32{UNINITIALIZED}>
INFO     | 2022-11-13 17:49:31,014 | forsee.plugins.call_analysis | Returning to offset 0x41825a in sample.DMP (0x41825a)
DEBUG    | 2022-11-13 17:49:31,018 | forsee.techniques.degree_of_concreteness | Address 0x77182e02 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:31,019 | forsee.explorer | <SimulationManager with 3 active>
DEBUG    | 2022-11-13 17:49:31,022 | forsee.explorer | Active: [<SimState @ 0x4963b1>, <SimState @ 0x49635c>, <SimState @ 0x41825a>]
DEBUG    | 2022-11-13 17:49:31,028 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:31,036 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:31,038 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 2.37
```



```
DEBUG   | 2022-11-13 17:49:31,038 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,040 | forsee.explorer | <SimulationManager with 3 active>
DEBUG   | 2022-11-13 17:49:31,040 | forsee.explorer | Active: [<SimState @ 0x4963b5>, <SimState @ 0x496366>, <SimState @ 0x418232>]
DEBUG   | 2022-11-13 17:49:31,050 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,061 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 2.37
INFO    | 2022-11-13 17:49:31,069 | forsee.plugins.call_analysis | Called offset 0x77181869 in sample.DMP (0x77181869)
DEBUG   | 2022-11-13 17:49:31,070 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,071 | forsee.explorer | <SimulationManager with 3 active>
DEBUG   | 2022-11-13 17:49:31,071 | forsee.explorer | Active: [<SimState @ 0x4963b5>, <SimState @ 0x49637c>, <SimState @ 0x77181869>]
DEBUG   | 2022-11-13 17:49:31,078 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,087 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 2.37
WARNING | 2022-11-13 17:49:31,089 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for GetMessageA. Returning unconstrained
INFO    | 2022-11-13 17:49:31,089 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure GetMessageA>
INFO    | 2022-11-13 17:49:31,089 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_GetMessageA_6_32{UNINITIALIZED}>
INFO    | 2022-11-13 17:49:31,091 | forsee.plugins.call_analysis | Returning to offset 0x418242 in sample.DMP (0x418242)
DEBUG   | 2022-11-13 17:49:31,092 | forsee.techniques.degree_of_concreteness | Address 0x77181869 is hooked. Not analyzing DoC
DEBUG   | 2022-11-13 17:49:31,093 | forsee.explorer | <SimulationManager with 3 active>
DEBUG   | 2022-11-13 17:49:31,093 | forsee.explorer | Active: [<SimState @ 0x4963b5>, <SimState @ 0x496384>, <SimState @ 0x418242>]
DEBUG   | 2022-11-13 17:49:31,100 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,106 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,140 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,141 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,143 | forsee.explorer | <SimulationManager with 4 active>
DEBUG   | 2022-11-13 17:49:31,143 | forsee.explorer | Active: [<SimState @ 0x4963bf>, <SimState @ 0x496397>, <SimState @ 0x41825c>, <SimState @ 0x418246>]
INFO    | 2022-11-13 17:49:31,148 | forsee.plugins.call_analysis | Returning to offset 0x425547 in sample.DMP (0x425547)
DEBUG   | 2022-11-13 17:49:31,156 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,174 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,176 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 3.37
INFO    | 2022-11-13 17:49:31,182 | forsee.plugins.call_analysis | Called offset 0x77186497 in sample.DMP (0x77186497)
DEBUG   | 2022-11-13 17:49:31,183 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,185 | forsee.explorer | <SimulationManager with 4 active>
DEBUG   | 2022-11-13 17:49:31,185 | forsee.explorer | Active: [<SimState @ 0x425547>, <SimState @ 0x4963af>, <SimState @ 0x418293>, <SimState @ 0x77186497>]
INFO    | 2022-11-13 17:49:31,192 | forsee.plugins.call_analysis | Called offset 0x4986a6 in sample.DMP (0x4986a6)
DEBUG   | 2022-11-13 17:49:31,192 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,202 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 2.37
INFO    | 2022-11-13 17:49:31,211 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG   | 2022-11-13 17:49:31,212 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 3.37
WARNING | 2022-11-13 17:49:31,215 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for TranslateMessage. Returning unconstrained
INFO    | 2022-11-13 17:49:31,218 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure TranslateMessage>
INFO    | 2022-11-13 17:49:31,218 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_TranslateMessage_7_32{UNINITIALIZED}>
INFO    | 2022-11-13 17:49:31,221 | forsee.plugins.call_analysis | Returning to offset 0x418250 in sample.DMP (0x418250)
DEBUG   | 2022-11-13 17:49:31,224 | forsee.techniques.degree_of_concreteness | Address 0x77186497 is hooked. Not analyzing DoC
DEBUG   | 2022-11-13 17:49:31,226 | forsee.explorer | <SimulationManager with 4 active>
DEBUG   | 2022-11-13 17:49:31,226 | forsee.explorer | Active: [<SimState @ 0x4986a6>, <SimState @ 0x4963af>, <SimState @ 0x425510>, <SimState @ 0x418250>]
INFO    | 2022-11-13 17:49:31,233 | forsee.plugins.call_analysis | Called offset 0x4a0bb0 in sample.DMP (0x4a0bb0)
DEBUG   | 2022-11-13 17:49:31,242 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,256 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 2.37
INFO    | 2022-11-13 17:49:31,279 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG   | 2022-11-13 17:49:31,285 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,286 | forsee.explorer | <SimulationManager with 4 active>
DEBUG   | 2022-11-13 17:49:31,287 | forsee.explorer | Active: [<SimState @ 0x4a0bb0>, <SimState @ 0x4963af>, <SimState @ 0x496350>, <SimState @ 0x77182e02>]
DEBUG   | 2022-11-13 17:49:31,317 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,326 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,338 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 3.37
WARNING | 2022-11-13 17:49:31,342 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for DispatchMessageA. Returning unconstrained
INFO    | 2022-11-13 17:49:31,346 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure DispatchMessageA>
INFO    | 2022-11-13 17:49:31,346 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_DispatchMessageA_8_32{UNINITIALIZED}>
INFO    | 2022-11-13 17:49:31,353 | forsee.plugins.call_analysis | Returning to offset 0x41825a in sample.DMP (0x41825a)
DEBUG   | 2022-11-13 17:49:31,354 | forsee.techniques.degree_of_concreteness | Address 0x77182e02 is hooked. Not analyzing DoC
DEBUG   | 2022-11-13 17:49:31,355 | forsee.explorer | <SimulationManager with 4 active>
DEBUG   | 2022-11-13 17:49:31,358 | forsee.explorer | Active: [<SimState @ 0x4986b2>, <SimState @ 0x4963b1>, <SimState @ 0x49635c>, <SimState @ 0x41825a>]
DEBUG   | 2022-11-13 17:49:31,427 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,436 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,446 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,448 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,449 | forsee.explorer | <SimulationManager with 4 active>
DEBUG   | 2022-11-13 17:49:31,450 | forsee.explorer | Active: [<SimState @ 0x4986b9>, <SimState @ 0x4963b5>, <SimState @ 0x496366>, <SimState @ 0x418232>]
DEBUG   | 2022-11-13 17:49:31,456 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,467 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,488 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 3.37
INFO    | 2022-11-13 17:49:31,502 | forsee.plugins.call_analysis | Called offset 0x77181869 in sample.DMP (0x77181869)
DEBUG   | 2022-11-13 17:49:31,507 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,514 | forsee.explorer | <SimulationManager with 4 active>
DEBUG   | 2022-11-13 17:49:31,517 | forsee.explorer | Active: [<SimState @ 0x498705>, <SimState @ 0x4963b5>, <SimState @ 0x49637c>, <SimState @ 0x77181869>]
INFO    | 2022-11-13 17:49:31,534 | forsee.plugins.call_analysis | Called offset 0x76cfc600 in sample.DMP (0x76cfc600)
DEBUG   | 2022-11-13 17:49:31,535 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,543 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,550 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 3.37
WARNING | 2022-11-13 17:49:31,555 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for GetMessageA. Returning unconstrained
INFO    | 2022-11-13 17:49:31,555 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure GetMessageA>
INFO    | 2022-11-13 17:49:31,555 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_GetMessageA_9_32{UNINITIALIZED}>
INFO    | 2022-11-13 17:49:31,559 | forsee.plugins.call_analysis | Returning to offset 0x418242 in sample.DMP (0x418242)
DEBUG   | 2022-11-13 17:49:31,559 | forsee.techniques.degree_of_concreteness | Address 0x77181869 is hooked. Not analyzing DoC
DEBUG   | 2022-11-13 17:49:31,562 | forsee.explorer | <SimulationManager with 4 active>
DEBUG   | 2022-11-13 17:49:31,562 | forsee.explorer | Active: [<SimState @ 0x76cfc600>, <SimState @ 0x4963b5>, <SimState @ 0x496384>, <SimState @ 0x418242>]
INFO    | 2022-11-13 17:49:31,566 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure HeapFree>
INFO    | 2022-11-13 17:49:31,568 | forsee.plugins.procedure_analysis |     HeapHandle: <BV32 0x1860000>
INFO    | 2022-11-13 17:49:31,568 | forsee.plugins.procedure_analysis |     Flags: <BV32 0x0>
INFO    | 2022-11-13 17:49:31,570 | forsee.plugins.procedure_analysis |     lpMem: <BV32 0x1861340>
INFO    | 2022-11-13 17:49:31,570 | forsee.plugins.procedure_analysis |     Returned: 1
INFO    | 2022-11-13 17:49:31,572 | forsee.plugins.call_analysis | Returning to offset 0x498714 in sample.DMP (0x498714)
DEBUG   | 2022-11-13 17:49:31,572 | forsee.techniques.degree_of_concreteness | Address 0x76cfc600 is hooked. Not analyzing DoC
DEBUG   | 2022-11-13 17:49:31,581 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,589 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,615 | forsee.techniques.degree_of_concreteness | DOC: 0.83, CumulRatio: 4.37
DEBUG   | 2022-11-13 17:49:31,615 | forsee.techniques.degree_of_concreteness | DOC: 0.83, CumulRatio: 4.37
DEBUG   | 2022-11-13 17:49:31,617 | forsee.explorer | <SimulationManager with 5 active>
DEBUG   | 2022-11-13 17:49:31,617 | forsee.explorer | Active: [<SimState @ 0x498714>, <SimState @ 0x4963bf>, <SimState @ 0x496397>, <SimState @ 0x41825c>, <SimState @ 0x418246>]
DEBUG   | 2022-11-13 17:49:31,623 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
INFO    | 2022-11-13 17:49:31,631 | forsee.plugins.call_analysis | Returning to offset 0x425547 in sample.DMP (0x425547)
DEBUG   | 2022-11-13 17:49:31,634 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,646 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,655 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 4.37
INFO    | 2022-11-13 17:49:31,660 | forsee.plugins.call_analysis | Called offset 0x77186497 in sample.DMP (0x77186497)
DEBUG   | 2022-11-13 17:49:31,660 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 4.37
DEBUG   | 2022-11-13 17:49:31,664 | forsee.explorer | <SimulationManager with 5 active>
DEBUG   | 2022-11-13 17:49:31,664 | forsee.explorer | Active: [<SimState @ 0x49872e>, <SimState @ 0x425547>, <SimState @ 0x4963af>, <SimState @ 0x418293>, <SimState @ 0x77186497>]
INFO    | 2022-11-13 17:49:31,668 | forsee.plugins.call_analysis | Called offset 0x4a0bf5 in sample.DMP (0x4a0bf5)
DEBUG   | 2022-11-13 17:49:31,675 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
INFO    | 2022-11-13 17:49:31,687 | forsee.plugins.call_analysis | Called offset 0x4986a6 in sample.DMP (0x4986a6)
DEBUG   | 2022-11-13 17:49:31,687 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,695 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 3.37
INFO    | 2022-11-13 17:49:31,702 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG   | 2022-11-13 17:49:31,703 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 4.37
WARNING | 2022-11-13 17:49:31,704 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for TranslateMessage. Returning unconstrained
INFO    | 2022-11-13 17:49:31,705 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure TranslateMessage>
INFO    | 2022-11-13 17:49:31,705 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_TranslateMessage_10_32{UNINITIALIZED}>
INFO    | 2022-11-13 17:49:31,707 | forsee.plugins.call_analysis | Returning to offset 0x418250 in sample.DMP (0x418250)
DEBUG   | 2022-11-13 17:49:31,707 | forsee.techniques.degree_of_concreteness | Address 0x77186497 is hooked. Not analyzing DoC
DEBUG   | 2022-11-13 17:49:31,709 | forsee.explorer | <SimulationManager with 5 active>
DEBUG   | 2022-11-13 17:49:31,714 | forsee.explorer | Active: [<SimState @ 0x4a0bf5>, <SimState @ 0x4986a6>, <SimState @ 0x4963af>, <SimState @ 0x425510>, <SimState @ 0x418250>]
INFO    | 2022-11-13 17:49:31,741 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
INFO    | 2022-11-13 17:49:31,741 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
ERROR   | 2022-11-13 17:49:31,742 | forsee.plugins.call_analysis | Stack backtrace violation
DEBUG   | 2022-11-13 17:49:31,742 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
INFO    | 2022-11-13 17:49:31,750 | forsee.plugins.call_analysis | Called offset 0x4a0bb0 in sample.DMP (0x4a0bb0)
DEBUG   | 2022-11-13 17:49:31,753 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,760 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 3.37
INFO    | 2022-11-13 17:49:31,778 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG   | 2022-11-13 17:49:31,778 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 4.37
INFO    | 2022-11-13 17:49:31,784 | forsee.plugins.call_analysis | Called offset 0x77182e02 in sample.DMP (0x77182e02)
DEBUG   | 2022-11-13 17:49:31,784 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 4.37
DEBUG   | 2022-11-13 17:49:31,786 | forsee.explorer | <SimulationManager with 5 active>
DEBUG   | 2022-11-13 17:49:31,787 | forsee.explorer | Active: [<SimState @ 0x498733>, <SimState @ 0x4a0bb0>, <SimState @ 0x4963af>, <SimState @ 0x496350>, <SimState @ 0x77182e02>]
INFO    | 2022-11-13 17:49:31,790 | forsee.plugins.call_analysis | Returning to offset 0x425553 in sample.DMP (0x425553)
DEBUG   | 2022-11-13 17:49:31,798 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,831 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,841 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,851 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 4.37
WARNING | 2022-11-13 17:49:31,853 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for DispatchMessageA. Returning unconstrained
INFO    | 2022-11-13 17:49:31,853 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure DispatchMessageA>
INFO    | 2022-11-13 17:49:31,853 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_DispatchMessageA_11_32{UNINITIALIZED}>
INFO    | 2022-11-13 17:49:31,856 | forsee.plugins.call_analysis | Returning to offset 0x41825a in sample.DMP (0x41825a)
DEBUG   | 2022-11-13 17:49:31,858 | forsee.explorer | Active: [<SimState @ 0x425553>, <SimState @ 0x4986b2>, <SimState @ 0x4963b1>, <SimState @ 0x49635c>, <SimState @ 0x41825a>]
INFO    | 2022-11-13 17:49:31,865 | forsee.plugins.call_analysis | Returning to offset 0x41829e in sample.DMP (0x41829e)
DEBUG   | 2022-11-13 17:49:31,866 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,875 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,887 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,898 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 4.37
DEBUG   | 2022-11-13 17:49:31,900 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 4.37
DEBUG   | 2022-11-13 17:49:31,902 | forsee.explorer | <SimulationManager with 5 active>
DEBUG   | 2022-11-13 17:49:31,902 | forsee.explorer | Active: [<SimState @ 0x41829e>, <SimState @ 0x4986b9>, <SimState @ 0x4963b5>, <SimState @ 0x496366>, <SimState @ 0x418232>]
DEBUG   | 2022-11-13 17:49:31,911 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:31,920 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,936 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:31,946 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 4.37
INFO    | 2022-11-13 17:49:31,954 | forsee.plugins.call_analysis | Called offset 0x77181869 in sample.DMP (0x77181869)
DEBUG   | 2022-11-13 17:49:31,955 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 4.37
DEBUG   | 2022-11-13 17:49:31,957 | forsee.explorer | <SimulationManager with 5 active>
DEBUG   | 2022-11-13 17:49:31,958 | forsee.explorer | Active: [<SimState @ 0x4182aa>, <SimState @ 0x498705>, <SimState @ 0x4963b5>, <SimState @ 0x49637c>, <SimState @ 0x77181869>]
INFO    | 2022-11-13 17:49:31,966 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG   | 2022-11-13 17:49:31,968 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
INFO    | 2022-11-13 17:49:31,980 | forsee.plugins.call_analysis | Called offset 0x76cfc600 in sample.DMP (0x76cfc600)
DEBUG   | 2022-11-13 17:49:31,986 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 2.37
DEBUG   | 2022-11-13 17:49:31,994 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:32,004 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 4.37
WARNING | 2022-11-13 17:49:32,010 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for GetMessageA. Returning unconstrained
INFO    | 2022-11-13 17:49:32,019 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure GetMessageA>
INFO    | 2022-11-13 17:49:32,022 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_GetMessageA_12_32{UNINITIALIZED}>
INFO    | 2022-11-13 17:49:32,024 | forsee.plugins.call_analysis | Returning to offset 0x418242 in sample.DMP (0x418242)
DEBUG   | 2022-11-13 17:49:32,026 | forsee.techniques.degree_of_concreteness | Address 0x77181869 is hooked. Not analyzing DoC
DEBUG   | 2022-11-13 17:49:32,030 | forsee.explorer | <SimulationManager with 5 active>
DEBUG   | 2022-11-13 17:49:32,030 | forsee.explorer | Active: [<SimState @ 0x425510>, <SimState @ 0x76cfc600>, <SimState @ 0x4963b5>, <SimState @ 0x496384>, <SimState @ 0x418242>]
INFO    | 2022-11-13 17:49:32,043 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG   | 2022-11-13 17:49:32,044 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
INFO    | 2022-11-13 17:49:32,046 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure HeapFree>
INFO    | 2022-11-13 17:49:32,047 | forsee.plugins.procedure_analysis |     HeapHandle: <BV32 0x1860000>
INFO    | 2022-11-13 17:49:32,047 | forsee.plugins.procedure_analysis |     Flags: <BV32 0x0>
INFO    | 2022-11-13 17:49:32,048 | forsee.plugins.procedure_analysis |     lpMem: <BV32 0x1861340>
INFO    | 2022-11-13 17:49:32,048 | forsee.plugins.procedure_analysis |     Returned: 1
INFO    | 2022-11-13 17:49:32,049 | forsee.plugins.call_analysis | Returning to offset 0x498714 in sample.DMP (0x498714)
DEBUG   | 2022-11-13 17:49:32,059 | forsee.techniques.degree_of_concreteness | Address 0x76cfc600 is hooked. Not analyzing DoC
DEBUG   | 2022-11-13 17:49:32,076 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 3.37
DEBUG   | 2022-11-13 17:49:32,082 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 4.37
DEBUG   | 2022-11-13 17:49:32,116 | forsee.techniques.degree_of_concreteness | DOC: 0.83, CumulRatio: 5.37
DEBUG   | 2022-11-13 17:49:32,116 | forsee.techniques.degree_of_concreteness | DOC: 0.83, CumulRatio: 5.37
DEBUG   | 2022-11-13 17:49:32,119 | forsee.explorer | <SimulationManager with 6 active>
DEBUG   | 2022-11-13 17:49:32,119 | forsee.explorer | Active: [<SimState @ 0x496350>, <SimState @ 0x498714>, <SimState @ 0x4963bf>, <SimState @ 0x496397>, <SimState @ 0x41825c>, <SimState @ 0x418246>]
DEBUG   | 2022-11-13 17:49:32,127 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
DEBUG   | 2022-11-13 17:49:32,139 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 2.37
INFO    | 2022-11-13 17:49:32,149 | forsee.plugins.call_analysis | Returning to offset 0x425547 in sample.DMP (0x425547)
```



```
DEBUG    | 2022-11-13 17:49:32,151 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:32,161 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,163 | forsee.techniques.degree_of_concreteness | DOC: 0.83, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:32,168 | forsee.plugins.call_analysis | Called offset 0x77186497 in sample.DMP (0x77186497)
DEBUG    | 2022-11-13 17:49:32,168 | forsee.techniques.degree_of_concreteness | DOC: 0.83, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:32,172 | forsee.explorer | <SimulationManager with 6 active>
DEBUG    | 2022-11-13 17:49:32,181 | forsee.explorer | Active: [<SimState @ 0x49635c>, <SimState @ 0x49872e>, <SimState @ 0x425547>, <SimState @ 0x4963af>, <SimState @ 0x418293>, <SimState @ 0x77186497>]
DEBUG    | 2022-11-13 17:49:32,192 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:32,197 | forsee.plugins.call_analysis | Called offset 0x4a0bf5 in sample.DMP (0x4a0bf5)
DEBUG    | 2022-11-13 17:49:32,197 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:32,204 | forsee.plugins.call_analysis | Called offset 0x4986a6 in sample.DMP (0x4986a6)
DEBUG    | 2022-11-13 17:49:32,204 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:32,210 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:32,216 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:32,216 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 5.37
WARNING  | 2022-11-13 17:49:32,218 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for TranslateMessage. Returning unconstrained
INFO     | 2022-11-13 17:49:32,222 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure TranslateMessage>
INFO     | 2022-11-13 17:49:32,222 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_TranslateMessage_13_32{UNINITIALIZED}>
INFO     | 2022-11-13 17:49:32,227 | forsee.plugins.call_analysis | Returning to offset 0x418250 in sample.DMP (0x418250)
DEBUG    | 2022-11-13 17:49:32,230 | forsee.techniques.degree_of_concreteness | Address 0x77186497 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:32,234 | forsee.explorer | <SimulationManager with 6 active>
DEBUG    | 2022-11-13 17:49:32,235 | forsee.explorer | Active: [<SimState @ 0x496366>, <SimState @ 0x4a0bf5>, <SimState @ 0x4986a6>, <SimState @ 0x4963af>, <SimState @ 0x425510>, <SimState @ 0x418250>]
DEBUG    | 2022-11-13 17:49:32,244 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:32,263 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
INFO     | 2022-11-13 17:49:32,271 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
ERROR    | 2022-11-13 17:49:32,278 | forsee.plugins.call_analysis | Stack backtrace violation
DEBUG    | 2022-11-13 17:49:32,282 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:32,289 | forsee.plugins.call_analysis | Called offset 0x4a0bb0 in sample.DMP (0x4a0bb0)
DEBUG    | 2022-11-13 17:49:32,289 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:32,297 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:32,314 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:32,318 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:32,325 | forsee.plugins.call_analysis | Called offset 0x77182e02 in sample.DMP (0x77182e02)
DEBUG    | 2022-11-13 17:49:32,325 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:32,327 | forsee.explorer | <SimulationManager with 6 active>
DEBUG    | 2022-11-13 17:49:32,331 | forsee.explorer | Active: [<SimState @ 0x49637c>, <SimState @ 0x498733>, <SimState @ 0x4a0bb0>, <SimState @ 0x4963af>, <SimState @ 0x496350>, <SimState @ 0x77182e02>]
DEBUG    | 2022-11-13 17:49:32,339 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:32,342 | forsee.plugins.call_analysis | Returning to offset 0x425553 in sample.DMP (0x425553)
DEBUG    | 2022-11-13 17:49:32,342 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:32,379 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:32,385 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,397 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 5.37
WARNING  | 2022-11-13 17:49:32,407 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for DispatchMessageA. Returning unconstrained
INFO     | 2022-11-13 17:49:32,407 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure DispatchMessageA>
INFO     | 2022-11-13 17:49:32,407 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_DispatchMessageA_14_32{UNINITIALIZED}>
INFO     | 2022-11-13 17:49:32,411 | forsee.plugins.call_analysis | Returning to offset 0x41825a in sample.DMP (0x41825a)
DEBUG    | 2022-11-13 17:49:32,414 | forsee.techniques.degree_of_concreteness | Address 0x77182e02 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:32,415 | forsee.explorer | <SimulationManager with 6 active>
DEBUG    | 2022-11-13 17:49:32,417 | forsee.explorer | Active: [<SimState @ 0x496384>, <SimState @ 0x425553>, <SimState @ 0x4986b2>, <SimState @ 0x4963b1>, <SimState @ 0x49635c>, <SimState @ 0x41825a>]
DEBUG    | 2022-11-13 17:49:32,424 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:32,431 | forsee.plugins.call_analysis | Returning to offset 0x41829e in sample.DMP (0x41829e)
DEBUG    | 2022-11-13 17:49:32,435 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:32,447 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:32,455 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,463 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:32,466 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:32,468 | forsee.explorer | <SimulationManager with 6 active>
DEBUG    | 2022-11-13 17:49:32,469 | forsee.explorer | Active: [<SimState @ 0x496397>, <SimState @ 0x41829e>, <SimState @ 0x4986b9>, <SimState @ 0x4963b5>, <SimState @ 0x496366>, <SimState @ 0x418232>]
DEBUG    | 2022-11-13 17:49:32,479 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:32,494 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:32,506 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:32,514 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,523 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:32,535 | forsee.plugins.call_analysis | Called offset 0x77181869 in sample.DMP (0x77181869)
DEBUG    | 2022-11-13 17:49:32,537 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:32,539 | forsee.explorer | <SimulationManager with 6 active>
DEBUG    | 2022-11-13 17:49:32,540 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x4182aa>, <SimState @ 0x498705>, <SimState @ 0x4963b5>, <SimState @ 0x49637c>, <SimState @ 0x77181869>]
DEBUG    | 2022-11-13 17:49:32,549 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:32,555 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:32,555 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:32,563 | forsee.plugins.call_analysis | Called offset 0x76cfc600 in sample.DMP (0x76cfc600)
DEBUG    | 2022-11-13 17:49:32,571 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:32,583 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,589 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 5.37
WARNING  | 2022-11-13 17:49:32,591 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for GetMessageA. Returning unconstrained
INFO     | 2022-11-13 17:49:32,594 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure GetMessageA>
INFO     | 2022-11-13 17:49:32,602 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_GetMessageA_15_32{UNINITIALIZED}>
INFO     | 2022-11-13 17:49:32,606 | forsee.plugins.call_analysis | Returning to offset 0x418242 in sample.DMP (0x418242)
DEBUG    | 2022-11-13 17:49:32,610 | forsee.techniques.degree_of_concreteness | Address 0x77181869 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:32,612 | forsee.explorer | <SimulationManager with 6 active>
DEBUG    | 2022-11-13 17:49:32,613 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x425510>, <SimState @ 0x76cfc600>, <SimState @ 0x4963b5>, <SimState @ 0x496384>, <SimState @ 0x418242>]
DEBUG    | 2022-11-13 17:49:32,621 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
INFO     | 2022-11-13 17:49:32,641 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:32,650 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:32,654 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure HeapFree>
INFO     | 2022-11-13 17:49:32,655 | forsee.plugins.procedure_analysis |     HeapHandle: <BV32 0x1860000>
INFO     | 2022-11-13 17:49:32,655 | forsee.plugins.procedure_analysis |     Flags: <BV32 0x0>
INFO     | 2022-11-13 17:49:32,655 | forsee.plugins.procedure_analysis |     lpMem: <BV32 0x1861340>
INFO     | 2022-11-13 17:49:32,655 | forsee.plugins.procedure_analysis |     Returned: 1
INFO     | 2022-11-13 17:49:32,657 | forsee.plugins.call_analysis | Returning to offset 0x498714 in sample.DMP (0x498714)
DEBUG    | 2022-11-13 17:49:32,657 | forsee.techniques.degree_of_concreteness | Address 0x76cfc600 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:32,666 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,677 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:32,709 | forsee.techniques.degree_of_concreteness | DOC: 0.82, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:32,710 | forsee.techniques.degree_of_concreteness | DOC: 0.82, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:32,713 | forsee.explorer | <SimulationManager with 6 active, 1 loop_pruned>
DEBUG    | 2022-11-13 17:49:32,713 | forsee.explorer | <SimulationManager with 6 active, 1 loop_pruned>
DEBUG    | 2022-11-13 17:49:32,722 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x496350>, <SimState @ 0x498714>, <SimState @ 0x4963bf>, <SimState @ 0x496397>, <SimState @ 0x41825c>]
DEBUG    | 2022-11-13 17:49:32,735 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:32,744 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:32,751 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:32,763 | forsee.plugins.call_analysis | Returning to offset 0x425547 in sample.DMP (0x425547)
DEBUG    | 2022-11-13 17:49:32,766 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,778 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:32,780 | forsee.techniques.degree_of_concreteness | DOC: 0.83, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:32,782 | forsee.explorer | <SimulationManager with 6 active, 1 loop_pruned>
DEBUG    | 2022-11-13 17:49:32,782 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x49635c>, <SimState @ 0x49872e>, <SimState @ 0x425547>, <SimState @ 0x4963af>, <SimState @ 0x418293>]
DEBUG    | 2022-11-13 17:49:32,796 | forsee.techniques.degree_of_concreteness | DOC: 0.97, CumulRatio: 1.37
DEBUG    | 2022-11-13 17:49:32,807 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:32,813 | forsee.plugins.call_analysis | Called offset 0x4a0bf5 in sample.DMP (0x4a0bf5)
DEBUG    | 2022-11-13 17:49:32,818 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:32,827 | forsee.plugins.call_analysis | Called offset 0x4986a6 in sample.DMP (0x4986a6)
DEBUG    | 2022-11-13 17:49:32,827 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,833 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:32,846 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:32,852 | forsee.techniques.degree_of_concreteness | DOC: 0.83, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:32,855 | forsee.explorer | <SimulationManager with 5 active, 2 loop_pruned>
DEBUG    | 2022-11-13 17:49:32,856 | forsee.explorer | Active: [<SimState @ 0x496366>, <SimState @ 0x4a0bf5>, <SimState @ 0x4986a6>, <SimState @ 0x4963af>, <SimState @ 0x425510>]
DEBUG    | 2022-11-13 17:49:32,862 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:32,880 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
INFO     | 2022-11-13 17:49:32,887 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
ERROR    | 2022-11-13 17:49:32,894 | forsee.plugins.call_analysis | Stack backtrace violation
DEBUG    | 2022-11-13 17:49:32,894 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:32,902 | forsee.plugins.call_analysis | Called offset 0x4a0bb0 in sample.DMP (0x4a0bb0)
DEBUG    | 2022-11-13 17:49:32,909 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:32,917 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:32,935 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:32,939 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:32,943 | forsee.explorer | <SimulationManager with 5 active, 2 loop_pruned>
DEBUG    | 2022-11-13 17:49:32,943 | forsee.explorer | Active: [<SimState @ 0x49637c>, <SimState @ 0x498733>, <SimState @ 0x4a0bb0>, <SimState @ 0x4963af>, <SimState @ 0x496350>]
DEBUG    | 2022-11-13 17:49:33,040 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:33,044 | forsee.plugins.call_analysis | Returning to offset 0x425553 in sample.DMP (0x425553)
DEBUG    | 2022-11-13 17:49:33,045 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:33,077 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:33,086 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,104 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,106 | forsee.explorer | <SimulationManager with 5 active, 2 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,106 | forsee.explorer | Active: [<SimState @ 0x496384>, <SimState @ 0x425553>, <SimState @ 0x4986b2>, <SimState @ 0x4963b1>, <SimState @ 0x49635c>]
DEBUG    | 2022-11-13 17:49:33,113 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:33,121 | forsee.plugins.call_analysis | Returning to offset 0x41829e in sample.DMP (0x41829e)
DEBUG    | 2022-11-13 17:49:33,122 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:33,131 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:33,142 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,151 | forsee.techniques.degree_of_concreteness | DOC: 0.84, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,154 | forsee.explorer | <SimulationManager with 5 active, 2 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,154 | forsee.explorer | Active: [<SimState @ 0x496397>, <SimState @ 0x41829e>, <SimState @ 0x4986b9>, <SimState @ 0x4963b5>, <SimState @ 0x496366>]
DEBUG    | 2022-11-13 17:49:33,167 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:33,179 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:33,187 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:33,195 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,205 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,211 | forsee.explorer | <SimulationManager with 5 active, 2 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,211 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x4182aa>, <SimState @ 0x498705>, <SimState @ 0x4963b5>, <SimState @ 0x49637c>]
DEBUG    | 2022-11-13 17:49:33,234 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:33,243 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:33,245 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:33,269 | forsee.plugins.call_analysis | Called offset 0x76cfc600 in sample.DMP (0x76cfc600)
DEBUG    | 2022-11-13 17:49:33,269 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:33,277 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,284 | forsee.techniques.degree_of_concreteness | DOC: 0.85, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,286 | forsee.explorer | <SimulationManager with 5 active, 2 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,286 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x425510>, <SimState @ 0x76cfc600>, <SimState @ 0x4963b5>, <SimState @ 0x496384>]
DEBUG    | 2022-11-13 17:49:33,319 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 2.37
INFO     | 2022-11-13 17:49:33,342 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:33,345 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:33,348 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure HeapFree>
INFO     | 2022-11-13 17:49:33,349 | forsee.plugins.procedure_analysis |     HeapHandle: <BV32 0x1860000>
INFO     | 2022-11-13 17:49:33,349 | forsee.plugins.procedure_analysis |     Flags: <BV32 0x0>
INFO     | 2022-11-13 17:49:33,349 | forsee.plugins.procedure_analysis |     lpMem: <BV32 0x1861340>
INFO     | 2022-11-13 17:49:33,349 | forsee.plugins.procedure_analysis |     Returned: 1
INFO     | 2022-11-13 17:49:33,350 | forsee.plugins.call_analysis | Returning to offset 0x498714 in sample.DMP (0x498714)
DEBUG    | 2022-11-13 17:49:33,351 | forsee.techniques.degree_of_concreteness | Address 0x76cfc600 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:33,358 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,364 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,366 | forsee.explorer | <SimulationManager with 5 active, 2 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,367 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x496350>, <SimState @ 0x498714>, <SimState @ 0x4963bf>, <SimState @ 0x496397>]
DEBUG    | 2022-11-13 17:49:33,378 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:33,390 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:33,399 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,411 | forsee.plugins.call_analysis | Returning to offset 0x425547 in sample.DMP (0x425547)
DEBUG    | 2022-11-13 17:49:33,415 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,423 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,426 | forsee.explorer | <SimulationManager with 5 active, 2 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,428 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x49635c>, <SimState @ 0x49872e>, <SimState @ 0x425547>, <SimState @ 0x4963af>]
DEBUG    | 2022-11-13 17:49:33,437 | forsee.techniques.degree_of_concreteness | DOC: 0.96, CumulRatio: 2.37
DEBUG    | 2022-11-13 17:49:33,447 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:33,452 | forsee.plugins.call_analysis | Called offset 0x4a0bf5 in sample.DMP (0x4a0bf5)
DEBUG    | 2022-11-13 17:49:33,452 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,463 | forsee.plugins.call_analysis | Called offset 0x4986a6 in sample.DMP (0x4986a6)
DEBUG    | 2022-11-13 17:49:33,470 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,479 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 6.37
```



```
DEBUG    | 2022-11-13 17:49:33,481 | forsee.explorer | <SimulationManager with 4 active, 3 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,481 | forsee.explorer | Active: [<SimState @ 0x496366>, <SimState @ 0x4a0bf5>, <SimState @ 0x4986a6>, <SimState @ 0x4963af>]
DEBUG    | 2022-11-13 17:49:33,492 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:33,509 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
INFO     | 2022-11-13 17:49:33,512 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
ERROR    | 2022-11-13 17:49:33,513 | forsee.plugins.call_analysis | Stack backtrace violation
DEBUG    | 2022-11-13 17:49:33,514 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,522 | forsee.plugins.call_analysis | Called offset 0x4a0bb0 in sample.DMP (0x4a0bb0)
DEBUG    | 2022-11-13 17:49:33,525 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,532 | forsee.techniques.degree_of_concreteness | DOC: 0.86, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,534 | forsee.explorer | <SimulationManager with 4 active, 3 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,535 | forsee.explorer | Active: [<SimState @ 0x49637c>, <SimState @ 0x498733>, <SimState @ 0x4a0bb0>, <SimState @ 0x4963af>]
DEBUG    | 2022-11-13 17:49:33,545 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:33,549 | forsee.plugins.call_analysis | Returning to offset 0x425553 in sample.DMP (0x425553)
DEBUG    | 2022-11-13 17:49:33,550 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:33,582 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,591 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,595 | forsee.explorer | <SimulationManager with 4 active, 3 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,595 | forsee.explorer | Active: [<SimState @ 0x496384>, <SimState @ 0x425553>, <SimState @ 0x4986b2>, <SimState @ 0x4963b1>]
DEBUG    | 2022-11-13 17:49:33,605 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:33,610 | forsee.plugins.call_analysis | Returning to offset 0x41829e in sample.DMP (0x41829e)
DEBUG    | 2022-11-13 17:49:33,611 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:33,620 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,627 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,631 | forsee.explorer | <SimulationManager with 4 active, 3 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,631 | forsee.explorer | Active: [<SimState @ 0x496397>, <SimState @ 0x41829e>, <SimState @ 0x4986b9>, <SimState @ 0x4963b5>]
DEBUG    | 2022-11-13 17:49:33,642 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:33,655 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:33,664 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,671 | forsee.techniques.degree_of_concreteness | DOC: 0.87, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,673 | forsee.explorer | <SimulationManager with 4 active, 3 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,673 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x4182aa>, <SimState @ 0x498705>, <SimState @ 0x4963b5>]
DEBUG    | 2022-11-13 17:49:33,681 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:33,687 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:33,688 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,703 | forsee.plugins.call_analysis | Called offset 0x76cfc600 in sample.DMP (0x76cfc600)
DEBUG    | 2022-11-13 17:49:33,703 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,713 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,715 | forsee.explorer | <SimulationManager with 4 active, 3 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,720 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x425510>, <SimState @ 0x76cfc600>, <SimState @ 0x4963b5>]
DEBUG    | 2022-11-13 17:49:33,739 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
INFO     | 2022-11-13 17:49:33,754 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:33,755 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,757 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure HeapFree>
INFO     | 2022-11-13 17:49:33,762 | forsee.plugins.procedure_analysis |     HeapHandle: <BV32 0x1860000>
INFO     | 2022-11-13 17:49:33,762 | forsee.plugins.procedure_analysis |     Flags: <BV32 0x0>
INFO     | 2022-11-13 17:49:33,762 | forsee.plugins.procedure_analysis |     lpMem: <BV32 0x1861340>
INFO     | 2022-11-13 17:49:33,762 | forsee.plugins.procedure_analysis |     Flags: <BV32 0x0>
INFO     | 2022-11-13 17:49:33,762 | forsee.plugins.procedure_analysis |     lpMem: <BV32 0x1861340>
INFO     | 2022-11-13 17:49:33,762 | forsee.plugins.procedure_analysis |     Returned: 1
INFO     | 2022-11-13 17:49:33,763 | forsee.plugins.call_analysis | Returning to offset 0x498714 in sample.DMP (0x498714)
DEBUG    | 2022-11-13 17:49:33,764 | forsee.techniques.degree_of_concreteness | Address 0x76cfc600 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:33,775 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,776 | forsee.explorer | <SimulationManager with 4 active, 3 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,776 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x496350>, <SimState @ 0x498714>, <SimState @ 0x4963bf>]
DEBUG    | 2022-11-13 17:49:33,785 | forsee.techniques.degree_of_concreteness | DOC: 0.94, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:33,795 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:33,802 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:33,812 | forsee.plugins.call_analysis | Returning to offset 0x425547 in sample.DMP (0x425547)
DEBUG    | 2022-11-13 17:49:33,812 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,815 | forsee.explorer | <SimulationManager with 4 active, 3 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,815 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x49635c>, <SimState @ 0x49872e>, <SimState @ 0x425547>]
DEBUG    | 2022-11-13 17:49:33,825 | forsee.techniques.degree_of_concreteness | DOC: 0.95, CumulRatio: 3.37
DEBUG    | 2022-11-13 17:49:33,833 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,837 | forsee.plugins.call_analysis | Called offset 0x4a0bf5 in sample.DMP (0x4a0bf5)
DEBUG    | 2022-11-13 17:49:33,838 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:33,847 | forsee.plugins.call_analysis | Called offset 0x4986a6 in sample.DMP (0x4986a6)
DEBUG    | 2022-11-13 17:49:33,848 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,852 | forsee.explorer | <SimulationManager with 3 active, 4 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,855 | forsee.explorer | Active: [<SimState @ 0x496366>, <SimState @ 0x4a0bf5>, <SimState @ 0x4986a6>]
DEBUG    | 2022-11-13 17:49:33,863 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,884 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
INFO     | 2022-11-13 17:49:33,884 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
ERROR    | 2022-11-13 17:49:33,885 | forsee.plugins.call_analysis | Stack backtrace violation
DEBUG    | 2022-11-13 17:49:33,885 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:33,892 | forsee.plugins.call_analysis | Called offset 0x4a0bb0 in sample.DMP (0x4a0bb0)
DEBUG    | 2022-11-13 17:49:33,895 | forsee.techniques.degree_of_concreteness | DOC: 0.88, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,897 | forsee.explorer | <SimulationManager with 3 active, 4 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,906 | forsee.explorer | Active: [<SimState @ 0x49637c>, <SimState @ 0x498733>, <SimState @ 0x4a0bb0>]
DEBUG    | 2022-11-13 17:49:33,919 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,925 | forsee.plugins.call_analysis | Returning to offset 0x425553 in sample.DMP (0x425553)
DEBUG    | 2022-11-13 17:49:33,926 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:33,959 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:33,961 | forsee.explorer | <SimulationManager with 3 active, 4 loop_pruned>
DEBUG    | 2022-11-13 17:49:33,961 | forsee.explorer | Active: [<SimState @ 0x496384>, <SimState @ 0x425553>, <SimState @ 0x4986b2>]
DEBUG    | 2022-11-13 17:49:33,972 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:33,985 | forsee.plugins.call_analysis | Returning to offset 0x41829e in sample.DMP (0x41829e)
DEBUG    | 2022-11-13 17:49:33,994 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:34,007 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,011 | forsee.explorer | <SimulationManager with 3 active, 4 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,011 | forsee.explorer | Active: [<SimState @ 0x496397>, <SimState @ 0x41829e>, <SimState @ 0x4986b9>]
DEBUG    | 2022-11-13 17:49:34,021 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:34,031 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:34,043 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,043 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,047 | forsee.explorer | <SimulationManager with 3 active, 4 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,049 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x4182aa>, <SimState @ 0x498705>]
DEBUG    | 2022-11-13 17:49:34,058 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:34,065 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:34,071 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:34,079 | forsee.plugins.call_analysis | Called offset 0x76cfc600 in sample.DMP (0x76cfc600)
DEBUG    | 2022-11-13 17:49:34,080 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,081 | forsee.explorer | <SimulationManager with 3 active, 4 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,082 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x425510>, <SimState @ 0x76cfc600>]
DEBUG    | 2022-11-13 17:49:34,088 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
INFO     | 2022-11-13 17:49:34,103 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:34,109 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:34,118 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure HeapFree>
INFO     | 2022-11-13 17:49:34,121 | forsee.plugins.procedure_analysis |     HeapHandle: <BV32 0x1860000>
INFO     | 2022-11-13 17:49:34,121 | forsee.plugins.procedure_analysis |     Flags: <BV32 0x0>
INFO     | 2022-11-13 17:49:34,126 | forsee.plugins.procedure_analysis |     lpMem: <BV32 0x1861340>
INFO     | 2022-11-13 17:49:34,126 | forsee.plugins.procedure_analysis |     Returned: 1
INFO     | 2022-11-13 17:49:34,128 | forsee.plugins.call_analysis | Returning to offset 0x498714 in sample.DMP (0x498714)
DEBUG    | 2022-11-13 17:49:34,128 | forsee.techniques.degree_of_concreteness | Address 0x76cfc600 is hooked. Not analyzing DoC
DEBUG    | 2022-11-13 17:49:34,130 | forsee.explorer | <SimulationManager with 3 active, 4 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,130 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x496350>, <SimState @ 0x498714>]
DEBUG    | 2022-11-13 17:49:34,139 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:34,158 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:34,165 | forsee.techniques.degree_of_concreteness | DOC: 0.89, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,168 | forsee.explorer | <SimulationManager with 3 active, 4 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,168 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x49635c>, <SimState @ 0x49872e>]
DEBUG    | 2022-11-13 17:49:34,176 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 4.37
DEBUG    | 2022-11-13 17:49:34,187 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:34,195 | forsee.plugins.call_analysis | Called offset 0x4a0bf5 in sample.DMP (0x4a0bf5)
DEBUG    | 2022-11-13 17:49:34,201 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,202 | forsee.explorer | <SimulationManager with 2 active, 5 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,205 | forsee.explorer | Active: [<SimState @ 0x496366>, <SimState @ 0x4a0bf5>]
DEBUG    | 2022-11-13 17:49:34,213 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:34,234 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
INFO     | 2022-11-13 17:49:34,234 | forsee.plugins.call_analysis | Returning to offset 0x498733 in sample.DMP (0x498733)
ERROR    | 2022-11-13 17:49:34,234 | forsee.plugins.call_analysis | Stack backtrace violation
DEBUG    | 2022-11-13 17:49:34,235 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,235 | forsee.explorer | <SimulationManager with 2 active, 5 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,238 | forsee.explorer | Active: [<SimState @ 0x49637c>, <SimState @ 0x498733>]
DEBUG    | 2022-11-13 17:49:34,250 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:34,254 | forsee.plugins.call_analysis | Returning to offset 0x425553 in sample.DMP (0x425553)
DEBUG    | 2022-11-13 17:49:34,254 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,255 | forsee.explorer | <SimulationManager with 2 active, 5 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,256 | forsee.explorer | Active: [<SimState @ 0x496384>, <SimState @ 0x425553>]
DEBUG    | 2022-11-13 17:49:34,264 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:34,269 | forsee.plugins.call_analysis | Returning to offset 0x41829e in sample.DMP (0x41829e)
DEBUG    | 2022-11-13 17:49:34,270 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,309 | forsee.explorer | <SimulationManager with 2 active, 5 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,310 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x4182aa>]
DEBUG    | 2022-11-13 17:49:34,316 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:34,326 | forsee.plugins.call_analysis | Called offset 0x425510 in sample.DMP (0x425510)
DEBUG    | 2022-11-13 17:49:34,334 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,338 | forsee.explorer | <SimulationManager with 2 active, 5 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,339 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x425510>]
DEBUG    | 2022-11-13 17:49:34,345 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 5.37
INFO     | 2022-11-13 17:49:34,362 | forsee.plugins.call_analysis | Called offset 0x496350 in sample.DMP (0x496350)
DEBUG    | 2022-11-13 17:49:34,363 | forsee.techniques.degree_of_concreteness | DOC: 0.90, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,364 | forsee.explorer | <SimulationManager with 2 active, 5 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,369 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x496350>]
DEBUG    | 2022-11-13 17:49:34,379 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:34,388 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,389 | forsee.explorer | <SimulationManager with 2 active, 5 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,395 | forsee.explorer | Active: [<SimState @ 0x4963af>, <SimState @ 0x49635c>]
DEBUG    | 2022-11-13 17:49:34,411 | forsee.techniques.degree_of_concreteness | DOC: 0.93, CumulRatio: 5.37
DEBUG    | 2022-11-13 17:49:34,425 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,426 | forsee.explorer | <SimulationManager with 1 active, 6 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,426 | forsee.explorer | Active: [<SimState @ 0x496366>]
DEBUG    | 2022-11-13 17:49:34,434 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,434 | forsee.explorer | <SimulationManager with 1 active, 6 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,435 | forsee.explorer | Active: [<SimState @ 0x49637c>]
DEBUG    | 2022-11-13 17:49:34,443 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,446 | forsee.explorer | <SimulationManager with 1 active, 6 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,454 | forsee.explorer | Active: [<SimState @ 0x496384>]
DEBUG    | 2022-11-13 17:49:34,464 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,471 | forsee.explorer | <SimulationManager with 1 active, 6 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,471 | forsee.explorer | Active: [<SimState @ 0x496397>]
DEBUG    | 2022-11-13 17:49:34,480 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,487 | forsee.explorer | <SimulationManager with 1 active, 6 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,490 | forsee.explorer | Active: [<SimState @ 0x4963af>]
DEBUG    | 2022-11-13 17:49:34,506 | forsee.techniques.degree_of_concreteness | DOC: 0.91, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,509 | forsee.explorer | <SimulationManager with 1 active, 6 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,509 | forsee.explorer | Active: [<SimState @ 0x4963af>]
DEBUG    | 2022-11-13 17:49:34,516 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,516 | forsee.explorer | <SimulationManager with 1 active, 6 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,517 | forsee.explorer | Active: [<SimState @ 0x4963af>]
DEBUG    | 2022-11-13 17:49:34,523 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,524 | forsee.explorer | <SimulationManager with 1 active, 6 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,524 | forsee.explorer | Active: [<SimState @ 0x4963af>]
DEBUG    | 2022-11-13 17:49:34,531 | forsee.techniques.degree_of_concreteness | DOC: 0.92, CumulRatio: 6.37
DEBUG    | 2022-11-13 17:49:34,532 | forsee.explorer | <SimulationManager with 7 loop_pruned>
DEBUG    | 2022-11-13 17:49:34,532 | forsee.explorer | Active: []
INFO     | 2022-11-13 17:49:34,532 | forsee.explorer | Exploration finished
INFO     | 2022-11-13 17:49:34,532 | forsee.explorer | Max steps exceeded: False
INFO     | 2022-11-13 17:49:34,532 | forsee.explorer | Reached completed state: True
```

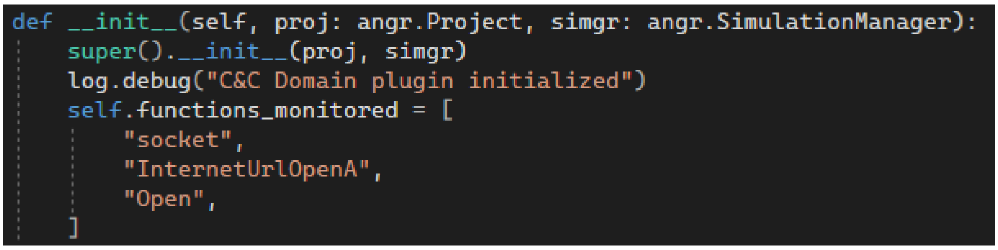
Unfortunately, Forecast failed to detected the socket connection, which should have triggered Forecast "C&C Domain" plugin to warn the user that C&C domain is detected.

3. Improve Forecast performance

We can do some modifications to Forecast code to make Forecast perform better in socket detection (as well as some other malware function detection). Before beginning code modification, let's take a quick look at how Forecast is supposed to do when detecting sockets established by the malware.

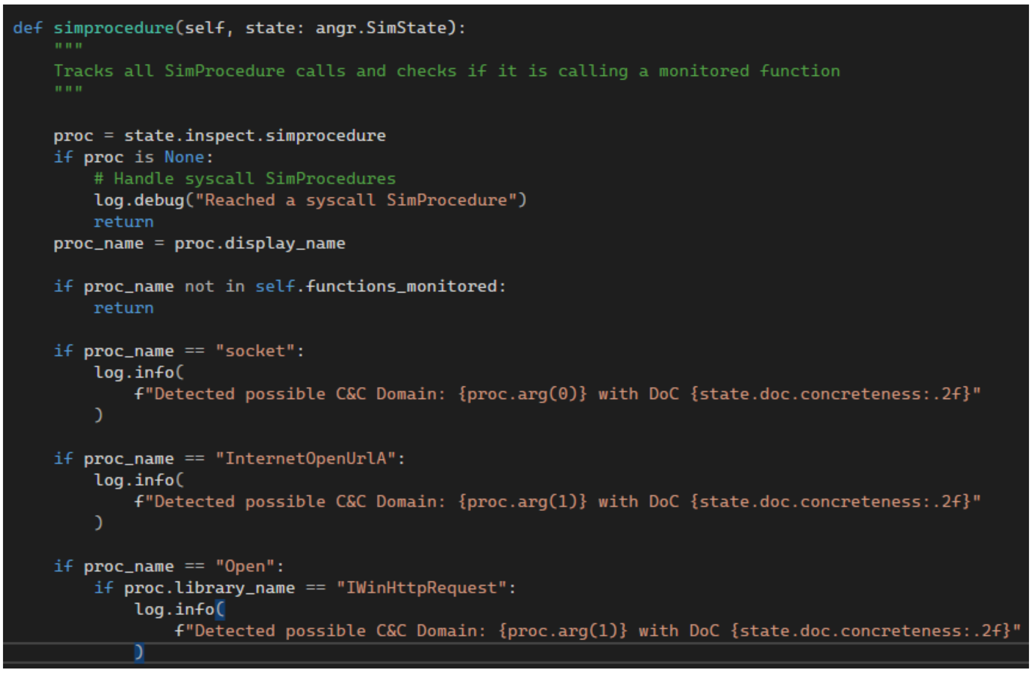
(1) How does Plugin works

For most of the plugins in Forecast directory, it has a list of "functions monitored", which contains a list of function name that related to the malware activity this plugin is taking responsibility for. For instance, function "`socket`", "`InternetUrlOpenA`" and "`Open`" are three functions that being monitored by plugin "cc_domain_dectection". It can be seen in class `CCDomainDetection` in `Forecast\forsee\plugins\cc_domain_detection.py`



```
def __init__(self, proj: angr.Project, simgr: angr.SimulationManager):
    super().__init__(proj, simgr)
    log.debug("C&C Domain plugin initialized")
    self.functions_monitored = [
        "socket",
        "InternetUrlOpenA",
        "Open",
    ]
```

Under the same class `CCDomainDetection`, there's a function named `simprocedure` (the code can be seen in the figure below), which acts as an intermedia of detected malware function and the log information presented to the user. Basically, what the function does is taking a variable that represents a function detected by Forecast underlying tools (for instance, angr in this case), and checking whether this function is a member of the function list that it is monitoring. If so, a corresponding waring log information will be presented to the user, and if not, nothing would be displayed on the command window and the program continues to explore the dump file.



```
def simprocedure(self, state: angr.SimState):
    """
    Tracks all SimProcedure calls and checks if it is calling a monitored function
    """

    proc = state.inspect.simprocedure
    if proc is None:
        # Handle syscall SimProcedures
        log.debug("Reached a syscall SimProcedure")
        return
    proc_name = proc.display_name

    if proc_name not in self.functions_monitored:
        return

    if proc_name == "socket":
        log.info(
            f"Detected possible C&C Domain: {proc.arg(0)} with DoC {state.doc.concreteness:.2f}"
        )

    if proc_name == "InternetOpenUrlA":
        log.info(
            f"Detected possible C&C Domain: {proc.arg(1)} with DoC {state.doc.concreteness:.2f}"
        )

    if proc_name == "Open":
        if proc.library_name == "IWinHttpRequest":
            log.info(
                f"Detected possible C&C Domain: {proc.arg(1)} with DoC {state.doc.concreteness:.2f}"
            )
```

In a larger scale, while exploring the dump file, as soon as an underlying tool detected a malware function, it sends the function name to every plugin that works with this mechanism. If one of the plugins finds that the function being presented is one of the functions that it is monitoring, a serious of if statements in the plugin code would lead to a corresponding waring log on the command window.

(2) Why does this happen

Considering the misfunction of Forecast in this situation, it might be caused by either the three reasons:

(i) The plugin isn't initialized.

(ii) The plugin doesn't get its desired function, so that nothing is shown out.

(iii) The function is presented properly, it's the plugin itself that doesn't perform properly.

As we can see at the very beginning of Forecast outputted result, the log

```
forsee.plugins.cc_domian_detection | C&C Domain plugin initialized
```

indicates that C&C domain detection plugin is initialized, which means the first assumption is a false statement.

To check the other two assumptions, I collected all functions that being presented to these plugins, they are

```
KiFastSystemCallRet
TranslateMessage
DispatchMessageA
GetMessageA
```

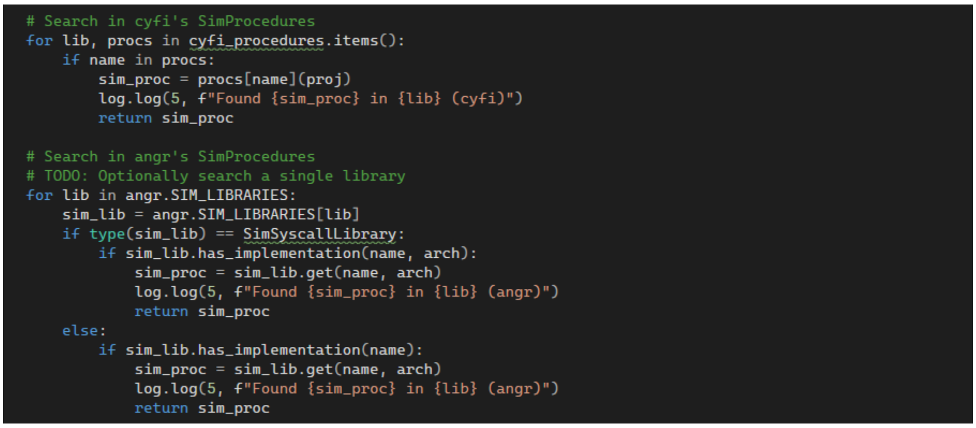
and some of these functions are presented multiple times. The plugin never receives a function named “socket”, no wonder why it fails to warn the user that C&C domain has been detection. To make sure that the plugin can output what is supposed to say when a function is in the list is presented properly, I added the code

```
proc_name = “socket”
```

just before the if statements, which means the variable “proc_name” that originally represents the function presented from the underlying tool, is changed to a fixed string “socket”, and the modified value will be brought to the following if statements. In this case, I got the desired output from the plugin, which means assumption (ii) is the problem we are going to solve, and it could be the entry point to make Forecast perform better.

Does Forecast fail to detect socket function while exploring the dump file? The misfunction of C&C domain detection plugin may seem to be hard to alleviate if this is the case. Luckily, the situation is much better than the worst case, because we can find another source of function list derived from the dump file in somewhere else.

There’s a function `find_sim_procedure` in class `ExportManager` in the file `\Forecast\forsee\techniques\procedure_handler\procedure_handler.py`, which contains the code below



```
# Search in cyfi's SimProcedures
for lib, procs in cyfi_procedures.items():
    if name in procs:
        sim_proc = procs[name](proj)
        log.log(5, f"Found {sim_proc} in {lib} (cyfi)")
        return sim_proc

# Search in angr's SimProcedures
# TODO: Optionally search a single library
for lib in angr.SIM_LIBRARIES:
    sim_lib = angr.SIM_LIBRARIES[lib]
    if type(sim_lib) == SimSyscallLibrary:
        if sim_lib.has_implementation(name, arch):
            sim_proc = sim_lib.get(name, arch)
            log.log(5, f"Found {sim_proc} in {lib} (angr)")
            return sim_proc
    else:
        if sim_lib.has_implementation(name):
            sim_proc = sim_lib.get(name, arch)
            log.log(5, f"Found {sim_proc} in {lib} (angr)")
            return sim_proc
```

By back tracing the code, we can find that the variable `name` is a name of a specific function Forecast detects while exploring the dump file. The log is set not to display so that user can’t see it in the command window.

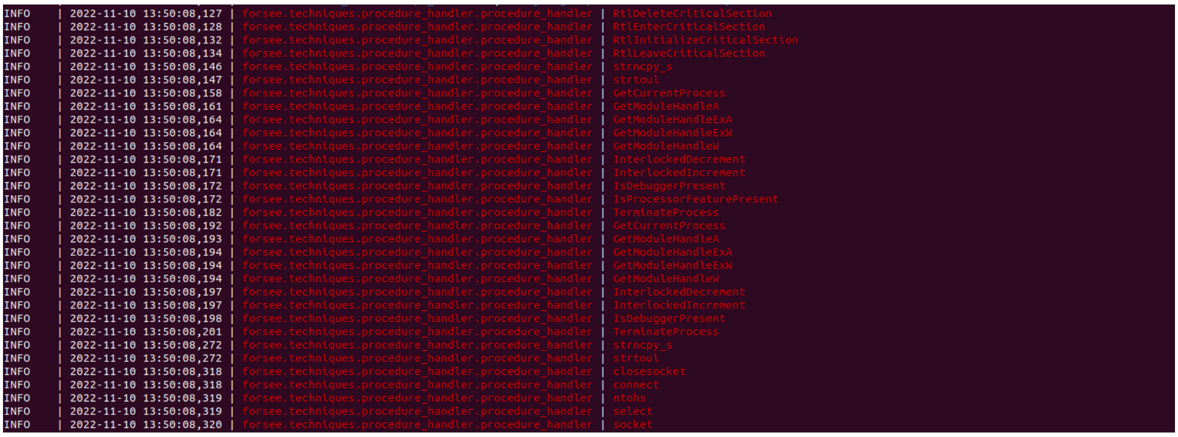
By changing the first parameter in the log function from 5 to 50

```
log.log(50, f"Found {sim_proc} in {lib} (cyfi)")
log.log(50, f"Found {sim_proc} in {lib} (angr)")
log.log(50, f"Found {sim_proc} in {lib} (angr)")
```

we can change the log information to highest priority and can see what it has got from the Forecast output information. It turns out that there are a number of functions that Forecast does detect, but aren’t sent to plugins to process. We can add the code

```
log.info(name)
```

in each if statement to display all functions the program has got. The figure below shows part of the output of `procedure_handler.py` after code modification.



```
INFO     | 2022-11-10 13:50:08,127 | forsee.techniques.procedure_handler.procedure_handler | RtlDeleteCriticalSection
INFO     | 2022-11-10 13:50:08,128 | forsee.techniques.procedure_handler.procedure_handler | RtlEnterCriticalSection
INFO     | 2022-11-10 13:50:08,132 | forsee.techniques.procedure_handler.procedure_handler | RtlInitializeCriticalSection
INFO     | 2022-11-10 13:50:08,134 | forsee.techniques.procedure_handler.procedure_handler | RtlLeaveCriticalSection
INFO     | 2022-11-10 13:50:08,146 | forsee.techniques.procedure_handler.procedure_handler | strncpy_s
INFO     | 2022-11-10 13:50:08,147 | forsee.techniques.procedure_handler.procedure_handler | strtoul
INFO     | 2022-11-10 13:50:08,158 | forsee.techniques.procedure_handler.procedure_handler | GetCurrentProcess
INFO     | 2022-11-10 13:50:08,161 | forsee.techniques.procedure_handler.procedure_handler | GetModuleHandleA
INFO     | 2022-11-10 13:50:08,164 | forsee.techniques.procedure_handler.procedure_handler | GetModuleHandleExA
INFO     | 2022-11-10 13:50:08,164 | forsee.techniques.procedure_handler.procedure_handler | GetModuleHandleExW
INFO     | 2022-11-10 13:50:08,164 | forsee.techniques.procedure_handler.procedure_handler | GetModuleHandleW
INFO     | 2022-11-10 13:50:08,171 | forsee.techniques.procedure_handler.procedure_handler | InterlockedDecrement
INFO     | 2022-11-10 13:50:08,171 | forsee.techniques.procedure_handler.procedure_handler | InterlockedIncrement
INFO     | 2022-11-10 13:50:08,172 | forsee.techniques.procedure_handler.procedure_handler | IsDebuggerPresent
INFO     | 2022-11-10 13:50:08,172 | forsee.techniques.procedure_handler.procedure_handler | IsProcessorFeaturePresent
INFO     | 2022-11-10 13:50:08,182 | forsee.techniques.procedure_handler.procedure_handler | TerminateProcess
INFO     | 2022-11-10 13:50:08,192 | forsee.techniques.procedure_handler.procedure_handler | GetCurrentProcess
INFO     | 2022-11-10 13:50:08,193 | forsee.techniques.procedure_handler.procedure_handler | GetModuleHandleA
INFO     | 2022-11-10 13:50:08,194 | forsee.techniques.procedure_handler.procedure_handler | GetModuleHandleExA
INFO     | 2022-11-10 13:50:08,194 | forsee.techniques.procedure_handler.procedure_handler | GetModuleHandleExW
INFO     | 2022-11-10 13:50:08,194 | forsee.techniques.procedure_handler.procedure_handler | GetModuleHandleW
INFO     | 2022-11-10 13:50:08,197 | forsee.techniques.procedure_handler.procedure_handler | InterlockedDecrement
INFO     | 2022-11-10 13:50:08,197 | forsee.techniques.procedure_handler.procedure_handler | InterlockedIncrement
INFO     | 2022-11-10 13:50:08,198 | forsee.techniques.procedure_handler.procedure_handler | IsDebuggerPresent
INFO     | 2022-11-10 13:50:08,201 | forsee.techniques.procedure_handler.procedure_handler | TerminateProcess
INFO     | 2022-11-10 13:50:08,272 | forsee.techniques.procedure_handler.procedure_handler | strncpy_s
INFO     | 2022-11-10 13:50:08,272 | forsee.techniques.procedure_handler.procedure_handler | strtoul
INFO     | 2022-11-10 13:50:08,318 | forsee.techniques.procedure_handler.procedure_handler | closesocket
INFO     | 2022-11-10 13:50:08,318 | forsee.techniques.procedure_handler.procedure_handler | connect
INFO     | 2022-11-10 13:50:08,319 | forsee.techniques.procedure_handler.procedure_handler | ntohs
INFO     | 2022-11-10 13:50:08,319 | forsee.techniques.procedure_handler.procedure_handler | select
INFO     | 2022-11-10 13:50:08,320 | forsee.techniques.procedure_handler.procedure_handler | socket
```

We can see that the function `socket` is detected, this source of function detection seems to be a better one compared to the one that the plugins are using. If we could add this source of function to all the plugins, it might lead to an improvement of performance on malware detection and analysis.

(3) Help Forecast perform better

To begin with, we need to create a container to store the list of function that listed in `procedure_handler.py`.

I created a new class `FunctionList` in a new file `function_detected.py` under directory `/Forecast/forsee/techniques` to do the job. A python dictionary is defined in the class to collect all the function names `procedure_handler.py` has got. Also, an add function is defined in the class to add new detected function in the dictionary, and the add process will not be executed if the same function already exists in the dictionary.

```
class FunctionList:
    dic = {'fucntion_name': 'function_name'}
    def add(the_name: str, the_list :dict = dic):
        if the_name in the_list.keys():
            return
        else:
            the_list[the_name] = the_name
            return
```

When we need this class, simply add

`from forsee.techniques.procedure_handler.function_detected import FunctionList`

at the top of the file to import this class to the file we want.

Then it’s time to feed all the plugin with this new source we have just modified. We are not going to change the source from previous one to this dictionary. Instead, we are going to add an additional source to each plugin to help it performs better.

Let's take the plugin `cc_domain_detection` for example. Basically, within the function `simprocedure`, after comparing `function_monitored` with the original source and executing all the if statements to display corresponding result, we are going to make it compare to our new defined collection after dealing with the old source, and execute the set of if statements for information display again. This could be done by iteratively assigning the value of `proc_name`, which initially represents the function name provided by the default source, to function names collected in our collection, and then executing all the if statement to determine the output.

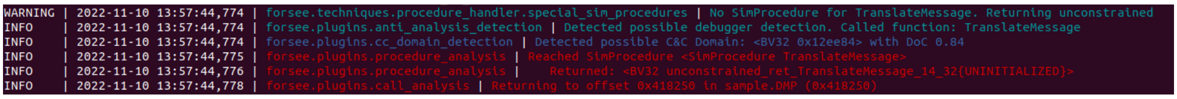
In order to avoid code repetition, it's better to define a new function taking charge of displaying information based on what we have got. When it comes to determine what should be displayed on the output, just pass the function name to the display function and it will make the decision.

```
def saySomething(self, proc_name: str, state: angr.SimState):
    proc = state.inspect.simprocedure
    if proc_name not in self.functions_monitored:
        return

    if proc_name == "socket":
        log.info(
            f"Detected possible C&C Domain: {proc.arg(0)} with DoC
            {state.doc.concreteness:.2f}"
        )

    if proc_name == "InternetOpenUrlA":
        log.info(
            f"Detected possible C&C Domain: {proc.arg(1)} with DoC
            {state.doc.concreteness:.2f}"
        )

    if proc_name == "Open":
        if proc.library_name == "IWinHttpRequest":
            log.info(
                f"Detected possible C&C Domain: {proc.arg(1)} with DoC
                {state.doc.concreteness:.2f}"
            )
```

And the function `simprocedure` becomes

```
def simprocedure(self, state: angr.SimState):
    #Tracks all SimProcedure calls and checks if it is calling a monitored function
    proc = state.inspect.simprocedure
    if proc is None:
        # Handle syscall SimProcedures
        log.debug("Reached a syscall SimProcedure")
        return
    proc_name = proc.display_name
    self.saySomething(proc_name, state)
    for function, typ in FunctionList.dic.items():
        self.saySomething(typ, state)
```

For all other plugins that work with a list of `function_monitored`, we can do similar modification to add a new source for comparation. After all the modification are done, we can execute `run_minidump.py` with the same dump file sample.DMP, and see if there's any improvement on its performance.



```
WARNING | 2022-11-10 13:57:44,774 | forsee.techniques.procedure_handler.special_sim_procedures | No SimProcedure for TranslateMessage. Returning unconstrained
INFO    | 2022-11-10 13:57:44,774 | forsee.plugins.anti_analysis_detection | Detected possible debugger detection. Called function: TranslateMessage
INFO    | 2022-11-10 13:57:44,774 | forsee.plugins.cc_domain_detection | Detected possible C&C Domain: <BV32 0x12ee84> with DoC 0.84
INFO    | 2022-11-10 13:57:44,775 | forsee.plugins.procedure_analysis | Reached SimProcedure <SimProcedure TranslateMessage>
INFO    | 2022-11-10 13:57:44,776 | forsee.plugins.procedure_analysis |     Returned: <BV32 unconstrained_ret_TranslateMessage_14_32{UNINITIALIZED}>
INFO    | 2022-11-10 13:57:44,778 | forsee.plugins.call_analysis | Returning to offset 0x418250 in sample.DMP (0x418250)
```

Luckily, there're new findings listed in Forecast output after modification. The function `socket` is detected, and it triggers a warning message. Meanwhile, the plugin `anti_analysis detection` also finds a function being provided by the new source is among its monitoring list, and another waring message comes out unsurprisingly.

What needs to be pointed out is that, the code modification above is just adding new analyzing approach in the program, it doesn't remove any existed functionality in Forecast code.

(4) Shortcomings and deficiencies

After the code modification above, it's good news that Forecast can detect malware activity that is previously ignored, but this modification is far more from making Forecast a perfect one. The warning message is outputted, but it does not always come out with the accurate address and DoC value.