

PhD Diary

Wei Minn
Singapore Management University

Version 1.0.5
Last compiled: November 29, 2023

Contents

I	2023	1
1	November	3
1.1	November 14, 2023	3
1.1.1	AOSP	3
1.1.2	C++ Primer	6
1.2	November 15, 2023	8
1.2.1	C++ Primer	8
1.2.2	AOSP	11
1.3	November 17, 2023	13
1.3.1	AOSP Hardware Abstraction Layer	13
1.4	November 18, 2023	15
1.4.1	Configuring AOSP for Acme Device on Ubuntu 23	15
1.5	November 19, 2023	16
1.5.1	Building AOSP HAL	16
1.6	November 20, 2023	17
1.6.1	const Qualifier	17
1.6.2	Rudimentary AOSP HAL Application	20
1.7	November 21, 2023	21
1.7.1	Fixing SELinux Policy to Start System Service	21
1.7.2	Memory Dump	21
1.8	November 22, 2023	22
1.8.1	C++ Data Structure	22
1.9	November 23, 2023	24
1.9.1	C++ Types and Data Structures	24
1.10	November 25, 2023	25
1.10.1	Android Memory Dump	25
1.11	November 27, 2023	26
1.11.1	Android Profile Guided Compilation	26
1.12	November 29, 2023	27
1.12.1	Android OAT Dump Parser	27

Part I

2023

Chapter 1

November

1.1 November 14, 2023

1.1.1 AOSP

Zygote

Zygote initializes by pre-loading the entire Android framework. Unlike desktop Java, it does not load the libraries lazily; it loads all of them as part of system start up. After completely initializing, it enters a tight loop, waiting for connections to a socket. When the system needs to create a new application, it connects to the Zygote socket and sends a small packet describing the application to be started. Zygote clones itself, creating a new kernel-level process.

Memory is organized into uniformly sized **pages**. When the application refers to memory at a particular address, the device hardware reinterprets the address as an index into a **page table**. Newly cloned Zygote processes for newly started applications are simply clone of Zygote's page table, pointing to the exact same pages of physical memory. Only the pages the new application uses for its own purposes are not shared:

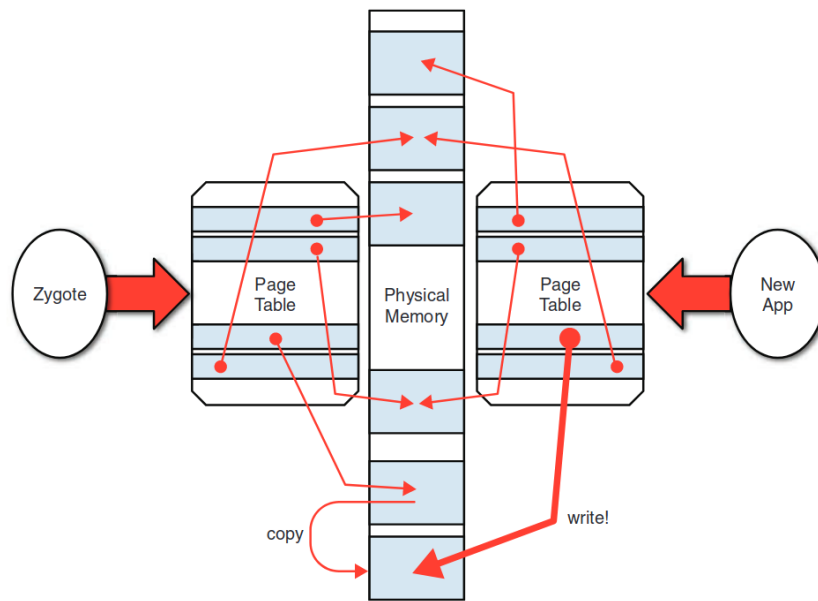


Figure 1.1: Zygote Copy-on Write

Zygote Initialization

Zygote is started by `init`. `ro.zygote` system variable set at platform build time decides which of four types of Zygotes are started and which one is "primary". Both the `init` and Zygote scripts are stored inside `$AOSP/system/core/rootdir`. In the following `init.zygote64_32.rc`, 2 Zygote processes, primary and secondary, are started at 2 different sockets:

```

1  service zygote /system/bin/app_process64 -Xzygote \
2      /system/bin --zygote --start-system-server --socket-name=zygote
3      class main
4      priority -20
5      user root
6      group root readproc reserved_disk
7      socket zygote stream 660 root system
8      socket usap_pool_primary stream 660 root system
9      onrestart exec_background - system system -- /system/bin/vdc volume abort_fuse
10     onrestart write /sys/power/state on
11     onrestart restart audioserver
12     onrestart restart cameraserver
13     onrestart restart media
14     onrestart restart media.tuner
15     onrestart restart netd
16     onrestart restart wificond
17     task_profiles ProcessCapacityHigh MaxPerformance
18     critical window=${zygote.critical_window.minute:-off} target=zygote-fatal
19
20  service zygote_secondary /system/bin/app_process32 -Xzygote \
21      /system/bin --zygote --socket-name=zygote_secondary --enable-lazy-preload
22      class main

```



```

23     priority -20
24     user root
25     group root readproc reserved_disk
26     socket zygote_secondary stream 660 root system
27     socket usap_pool_secondary stream 660 root system
28     onrestart restart zygote
29     task_profiles ProcessCapacityHigh MaxPerformance
30     disabled

```

The actual application that is started as user root at the very highest priority by init is /system/bin/app_process64. The script requests that init create a stream socket for the process and catalog it as /dev/socket/zygote_secondary which will be used by the system to start new Android applications.

Zygote is only started once during the system startup, by app_process64 and app_process32, and is simply cloned to start subsequent applications. Zygote initialization sequence is described below:

Method	Description	Source
init.rc	Imports the init.zygote64_32.rc that contains the script that starts Zygote service.	\$AOSP/system/core/rootdir
init.zygote64_32.rc	Runs app_process64 and app_process32 which will initialize the starting of Zygote service.	\$AOSP/system/core/rootdir
app_process	Creates AppRuntime, a subclass of AndroidRuntime, that does bookkeeping, naming the process, setting up parameter, and the name of the class to run when not running Zygote, and then calls AndroidRuntime.start() to invoke the runtime.	\$AOSP/frameworks/base/cmds/app_process
AppRuntime::start	Invokes startVM.startVM which invokes JNI_CreateJavaVM.	\$AOSP/frameworks/base/core/jni/AndroidRuntime.cpp
JNI_CreateJavaVM	Calls Runtime::Create.	\$AOSP/art/runtime/jni/java_vm_ext.cc
Runtime::Create	Initializes the ART runtime, loading the system OAT files and the libraries they contain.	\$AOSP/art/runtime/runtime.cc

Table 1.1: Zygote Initialization Sequence

The argument that app_process passed to start is com.android.internal.os.Zygote.Init, the source for which is in \$AOSP/frameworks/base/core/java/com/android/internal/os/ZygoteInit.java. app_process is the launcher for all Java programs (not

apps!) in the Android system, and Zygote is one example of the programs (system service) to be launched.

Zygote System Service

Zygote has 3 major tasks, on startup:

1. Register the socket to which the system will connect to start new application. Handled by `registerServerSocket` method which creates socket using the named passed as parameter for init script.
2. Preload Android resources (classes, libraries, resources and even WebViews) with a call to `preload` method. After preload is finished, Zygote is fully initialized and ready to clone to new applications very quickly.
3. Start Android System Server. Thus, `SystemServer` is the first application to be cloned by Zygote.

After it has completed these three tasks, it enters a loop, waiting for connections to the socket.

1.1.2 C++ Primer

Primitive Built-in Types

Includes **arithmetic types** and a special type named **void** which has no associated values and can be used in only a few circumstances, most commonly as the return type for functions that do not return a value.

The arithmetic types are divided into two categories: **integral types** (which include character and boolean types) and floating-point types.

Type	Meaning	Minimum Size
<code>bool</code>	boolean (true or false)	NA
<code>char</code>	character	8 bits
<code>w_char_t</code>	wide character	16 bits
<code>char16_t</code>	Unicode character	16 bits
<code>char32_t</code>	Unicode character	32 bits
<code>short</code>	short integer	16 bits
<code>int</code>	integer	16 bits
<code>long</code>	long integer	32 bits
<code>long long</code>	long integer	64 bits
<code>float</code>	single-precision floating-point	6 significant digits
<code>double</code>	double-precision floating-point	10 significant digits

long double	extended-precision floating-point	10 significant digits
-------------	-----------------------------------	-----------------------

Table 1.2: Zygote Initialization Sequence

Except for `bool` and extended character types, the integral types may be **signed** (can represent negative or positive numbers) or **unsigned**. By default, `int`, `short`, `long`, `long long` are all signed. To declare unsigned type, prepend `unsigned` to the type. `char` is signed on some machine and unsigned on others, and unsigned `int` is abbreviated as `unsigned`.

Conversions happen automatically when we use an object of one type where an object of another type is expected.

```
1 unsigned u = 10;
2 int i = -42;
3 std::cout << i + i << std::endl; // prints -84
4 std::cout << u + i << std::endl; // if 32-bit ints, prints 4294967264
```

In the above snippet, converting a negative number to unsigned will cause the value to "wrap around" because unsigned values can never be less than 0. Thus, extra care should be taken if we want to write loops with unsigned values and stopping conditions at negative values like the snippet below:

```
1 // WRONG: u can never be less than 0; the condition will always succeed
2 for (unsigned u = 10; u >= 0; --u)
3     std::cout << u << std::endl;
```

As such it is always advisable to not mix signed and unsigned types. By default, integer literals (42) are signed, while octal (024) and hexadecimal (0x14) may be signed or unsigned.

Escape sequences are used as if they were single characters:

```
1 std::cout << '\n'; // prints a newline
2 std::cout << "\tHi!\n"; // prints a tab followed by "Hi!" and a newline
```

Variables

Initialization is not assignment. Initialization happens when a variable is given a value when it is created. Assignment obliterates an object's current value and replaces that value with a new one.

Four different ways to initialize:

```
1 int units_sold = 0;
2 int units_sold = {0}; // list initialization; does not work for built-in types if
    data loss is likely
3 int units_sold{0};
4 int units_sold(0);
```

Variables defined outside any function body are initialized to zero by default. Variables of built-in type defined inside a function are **uninitialized** and therefore undefined. Objects of class type that we do not explicitly initialize have a value that is defined by the class.

A **declaration** makes a name known to the program. A file that wants to use a name defined elsewhere includes a declaration for that name. A **definition** creates the associated entity. A definition involves declaration, allocates storage and may provide the variable with an initial value.

```

1 extern int i;    // declares but not define j
2 int j;          // declares and defines j
3 int k = 12;      // declares, defines and initializes j
4 extern double pi = 3.14;    // definition

```

Variables must be defined only once but can be declared several times. To use a variable in more than one file requires declarations that are separate from the variable's definition. To use the same variable in multiple files, we must define that in one - and only one - file. Other files that use that variable must declare - but not define - that variable.

1.2 November 15, 2023

1.2.1 C++ Primer

Scopes of Names

Most scopes in C++ are delimited by curly braces.

```

1 #include <iostream>
2 int main() {
3     int sum = 0;
4     // sum values from 1 through 10 inclusive
5     for (int val = 1; val <= 10; ++val)
6         sum += val; // equivalent to sum=sum+val
7     std::cout << "Sum of 1 to 10 inclusive is "
8         << sum << std::endl;
9     return 0;
10 }

```

In above program, main - like most names defined outside a function - has **global scope** and thus, is accessible throughout the program. sum has **block scope** and is accessible from its point of declaration throughout the rest of the main function. val is defined in the scope of the for statement and can be used in that statement but not elsewhere in main.

Names declared in the outer scope can also be redefined in an inner scope although it is always a bad idea:

```

1 #include <iostream>
2 // Program for illustration purposes only: It is bad style for a function
3 // to use a global variable and also define a local variable with the same name
4 int reused = 42; // reused has global scope
5 int main() {
6     int unique = 0; // unique has block scope
7
8     // output #1: uses global reused; prints 42 0

```

```

9      std::cout << reused << "␣" << unique << std::endl;
10
11      int reused = 0; // new, local object named reused hides global reused
12      // output #2: uses local reused; prints 0 0
13      std::cout << reused << "␣" << unique << std::endl;
14
15      // output #3: explicitly requests the global reused; prints 42 0
16      std::cout << ::reused << "␣" << unique << std::endl;
17
18      return 0;
19  }

```

When the scope operator (`::` **operator**) has an empty LHS, it is a request to fetch the name on the RHS from the global scope.

References

A **reference** defines an alternative name for an object. A reference type can be defined by writing a declarator of the form `&d` where `d` is the name being declared:

```

1  int ival = 1024;
2  int &refVal = ival; // refVal refers to (is another name for) ival
3  int &refVal2; // error: a reference must be initialized

```

When we define a reference, instead of copying the initializer's value, we bind the reference to its initializer. Once initialized, a reference remains bound to its initial object. There is no way to rebind a reference to refer to a different object. Because there is no way to rebind a reference, references must be initialized.

A reference is not an object. Instead, a reference is just another name for an already existing object. Thus, *all* operation on that reference are actually operations on the object to which the reference is bound:

```

1  refVal = 2; // assigns 2 to the object to which refVal refers, i.e., to ival
2  int ii = refVal; // same as ii=ival

```

Because references are not objects, we may not define a reference to a reference. We can define references in a single definition with each identifier that is a reference being preceded by the `&` symbol:

```

1  int i = 1024, i2 = 2048; // i and i2 are both ints
2  int &r = i, r2 = i2; // r is a reference bound to i; r2 is an int
3  int i3 = 1024, &ri = i3; // i3 is an int; ri is a reference bound to i3
4  int &r3 = i3, &r4 = i2; // both r3 and r4 are references

```

Pointers

Like references, pointers are used for indirect access to other objects. Unlike a reference, a pointer is an object in its own right. Pointers can be assigned and copied; a single pointer can point to several different objects over its lifetime. Unlike a reference, a pointer need not be initialized at the time it is defined. Like other built-in types, pointers defined at block scope have undefined value if they are not initialized.

We define a pointer type by writing a declarator of the form `*d`, where `d` is the name being defined. The `*` must be repeated for each pointer variable:

```
1 int *ip1, *ip2; // both ip1 and ip2 are pointers to int
2 double dp, *dp2; // dp2 is a pointer to double; dp is a double
```

A pointer holds the address of another object. We get the address of an object by using the address-of operator (**& operator**):

```
1 int ival = 42;
2 int *p = &ival; // p holds the address of ival; p is a pointer to ival
3
4 double dval;
5 double *pd = &dval; // ok: initializer is the address of a double
6 double *pd2 = pd; // ok: initializer is a pointer to double
7 int *pi = pd; // error: types of pi and pd differ
8 pi = &dval; // error: assigning the address of a double to a pointer to int
```

We can use the dereference operator (*** operator**) to access that object:

```
1 int ival = 42;
2 int *p = &ival; // p holds the address of ival; p is a pointer to ival
3 cout << *p; // * yields the object to which p points; prints 42
4
5 *p = 0; // * yields the object; we assign a new value to ival through p
6 cout << *p; // prints 0
```

When we assign to `*p`, we are assigning to the object to which `p` points. We may dereference only a valid pointer that points to an object.

`void*` is a special pointer type that can hold the address of any object. Its useful for when the type of the object at that address is unknown:

```
1 double obj = 3.14, *pd = &obj; // ok: void* can hold the address value of any data
   // pointer type
2 void *pv = &obj; // obj can be an object of any type
3 pv = pd; // pv can hold a pointer to any type
```

The modifiers `*` and `&` do not apply to all variables defined in a single statement:

```
1 int* p1, p2; // p1 is a pointer to int; p2 is an int
2 int *p1, *p2; // both p1 and p2 are pointers to int
```

As pointers are objects in memory, they also have addresses of their own. Therefore, we can store the address of a pointer in another pointer:

```
1 int ival = 1024;
2 int *pi = &ival; // pi points to an int
3 int **ppi = &pi; // ppi points to a pointer to an int
```

We indicate each pointer level by its own `*`. Dereferencing a pointer to a pointer yields the pointer. So in this case, you must dereference twice to access the underlying object.

1.2.2 AOSP

Starting Android System Server and Other Apps using Zygote

During its initialization, Zygote will check for start-system-server flag, and if set, will bring up SystemServer in the following sequence:

Method	Description	Source
ZygoteInit. forkSystemServer	Runs after the Zygote process has been initialized. It is hardcoded with System Server classpath ¹ as one of the arguments to call Zygote.forkSystemServer to spawn SystemServer process.	AOSP/framework/ base/core/java/com/ android/internal/os/ ZygoteInit.java
Zygote. forkSystemServer	Zygote class wraps native methods that communicate with Android Runtime, one of whom is com_android_internal_os_nativeForkSystemServer.	AOSP/framework/base/ core/java/com/android/ internal/os/Zygote. java
com_android_in- ternal_os_native- ForkSystemServer SpecializeCommon	Calls zygote::ForkCommon and SpecializeCommon which does the actual forking. Looks at the flags and Process ID for setting up sandboxing, configuring the correct SE Linux context, and process capabilities. Afterwards, it will call Zygote methods for post-fork procedures.	AOSP/frameworks/base/ core/jni/com_android_ internal_os_Zygote.cpp AOSP/frameworks/base/ core/jni/com_android_ internal_os_Zygote.cpp
Zygote. callPostForkSystemServerHooks	Calls ZygoteHooks.java at the end of specialization procedures. Only applicable for SystemSever.	AOSP/framework/base/ core/java/com/android/ internal/os/Zygote. java
Zygote. callPostForkChildHooks	Calls ZygoteHooks.java at the end of specialization procedures. Applicable to all applications and services including SystemServer	AOSP/framework/base/ core/java/com/android/ internal/os/Zygote. java

¹com.android.server.SystemServer, the source for which is stored in AOSP/frameworks/base/services/java/com/android/server/SystemServer.java.

Method	Description	Source
ZygoteHooks. postForkSystemService and ZygoteHooks. postForkSystemService	Wrappers for ZygoteHooks inside the Android Runtime. They call their respective native code inside the ART via Java Native Interface.	AOSP/libcore/dalvik/ src/main/java/dalvik/ system/ZygoteHooks. java
ZygoteHooks_ nativePostForkSystemService	Loads the specialized class libraries to start the the System Server.	AOSP/art/runtime/ native/dalvik_system_ ZygoteHooks.cc
ZygoteHooks_ nativePostForkChild	Loads the specialized class libraries to start the service/application.	AOSP/art/runtime/ native/dalvik_system_ ZygoteHooks.cc
handleSystemServiceProcess	After control returns to ZygoteInit, and finish remaining work for the newly forked system server process, and calls ZygoteInit.zygoteInit.	AOSP/framework/ base/core/java/com/ android/internal/os/ ZygoteInit.java
ZygoteInit. zygoteInit	The main function called when started through the zygote process, which calls RuntimeInit.applicationInit	AOSP/framework/ base/core/java/com/ android/internal/os/ ZygoteInit.java
RuntimeInit. applicationInit	Calls the public static void main method of the application	AOSP/framework/ base/core/java/com/ android/internal/os/ RuntimeInit.java
ZygoteServer. runSelectLoop	After forking has finished, the control enters ZygoteServer which starts an endless loop that handles incoming connections with ZygoteConnection.processCommand.	AOSP/framework/ base/core/java/com/ android/internal/os/ ZygoteServer.java
ZygoteConnection. processCommand	Calls Zygote.forkAndSpecialize which is a version of ZygoteInit.forkSystemService for the masses.	AOSP/framework/ base/core/java/com/ android/internal/os/ ZygoteConnection.java
Zygote. forkAndSpecialize	A version of Zygote.forkSystemService for the masses.	AOSP/frameworks/base/ core/jni/com_android_ internal_os_Zygote.cpp

Method	Description	Source
<code>com_android_internal_os_native-ForkAndSpecialize</code>	Calls <code>zygote::ForkCommon</code> and <code>SpecializeCommon</code> which does the actual forking, and returns to <code>ZygoteInit</code> and immediately enters <code>ZygoteServer</code> .	<code>AOSP/frameworks/base/core/jni/com_android_internal_os_Zygote.cpp</code>

Table 1.3: System Server and Applications Initialization Sequence

1.3 November 17, 2023

1.3.1 AOSP Hardware Abstraction Layer

The interface to the hardware is a device drivers which are usually device specific and sometimes proprietary. A single set of C header files describes the functionality that a HAL provides to the Android system. HAL Code for a particular device is the implementation of the API defined by those header files, so that no code above the HAL needs to be changed to port Android to use the new device.

HAL Code Structure

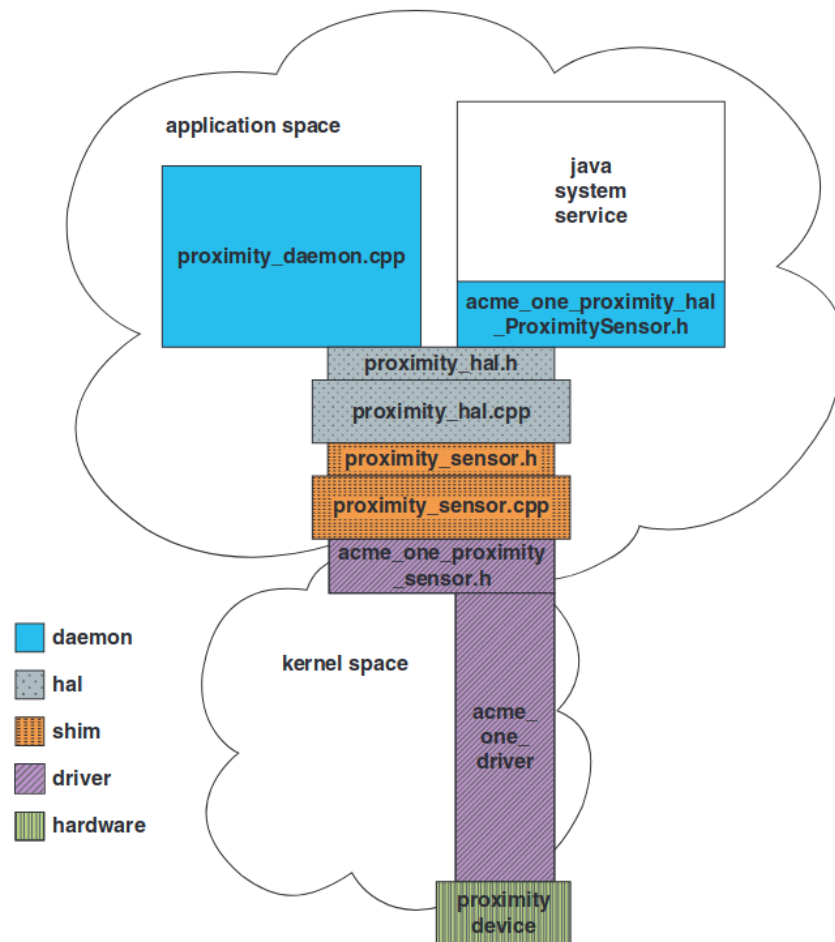


Figure 1.2: HAL Layer Structure

The code consists of four functional components as show in Figure 1.2:

1. **HAL code (dotted boxes):** Abstraction that separates the capabilities of hardware from its specific implementations. The `.h` file defines the HAL interface, and the implementation (`.cpp` file) specializes the Android HAL API for the target hardware.
2. **Shim code (dashed boxes):** Glue code that connects the HAL to a specific device hardware/driver. This code adapts the Android HAL API to the device driver for the hardware.
3. **Daemon (blue):** Stand-alone application that interacts with the hardware through the HAL.

4. **Java System Service (white):** System Service that Android applications will use to access the custom hardware.

The source for those components are structured like in the directory tree below:

```

one
├── app
├── native_daemon
│   ├── ...
├── java_daemon
│   ├── ...
├── proximity
│   ├── include
│   │   ├── dev
│   │   │   ├── ...
│   │   ├── ...
│   ├── dev
│   │   ├── ...
│   ├── hal
│   │   ├── ...
│   ├── jni
│   │   ├── ...

```

where one is the device folder of the AOSP project. All the code implementing the HAL for the proximity sensors goes into a new subdirectory `proximity`.²

1.4 November 18, 2023

1.4.1 Configuring AOSP for Acme Device on Ubuntu 23

Repo Manifest

Top-level subdirectory named `.repo` contains the manifests repository inside `manifests` subdirectory. The `manifests` repo contain one or more manifest files named as the argument of the `-m` command line option. `.repo/manifest` file controls the structure of the rest of the repository, and includes `.repo/manifests/default.xml`³ which is a list of git repositories. `repo` program parses `manifest.xml`, and thus `default.xml`, and clone each repository into a location specified inside `default.xml`.

²To be a "real" HAL, the interface `proximity/include/proximity_hal.h` would have to be promoted from its current directory specifically for the One device, up into the Android source tree to a location that would make it visible to other code that needed to use it. Here, it is only shared by Acme devices, so it is put under the subdirectory of the Acme device directory. If it's visible across device from multiple vendors, it might be promoted into the device directory itself.

³<https://gerrit.googlesource.com/git-repo/+master/docs/manifest-format.md>

Each project element in the XML identifies a git repository by its name, relative to some base URL, its remote; and where that repository should be placed in the local workspace, its path. If the full URL for the repository is not specified, repo will use the default remote specified in the default element near the top of the manifest:

```
1 <default revision="refs/tags/android-13.0.0_r11"
2   remote="aosp"
3   sync-j="4" />
```

where the remote, aosp, is defined likewise in the top of of the default.xml:

```
1 <remote name="aosp"
2   fetch=".."
3   review="https://android-review.googlesource.com/" />
```

Instead of including a URL as its attribute, it includes the fetch attribute which indicates the URL for this remote should be derived from the URL used to initialize the workspace (the argument to the -u option).

```
1 git ls-remote -h https://android.googlesource.com/platform/manifest.git
2 repo init -u https://android.googlesource.com/platform/manifest -b android-10.0.0_r33
3 git config --global user.email "mg.weiminn@gmail.com"
4 git config --global user.name "weiminn"
5 repo init -u https://android.googlesource.com/platform/manifest -b android-10.0.0_r33
6 repo sync -j31
7 source build/envsetup.sh
8 lunch sdk_phone_x86_64-userdebug
9 make -j31
```

Ubuntu 23 does not have the repository for libncurses5 because they already have libncurses6, so you have to add old focal repository to your /etc/apt/sources.list:

```
1 deb http://security.ubuntu.com/ubuntu focal-security main universe
```

After including the old repo, update the repository index and install libncurses5:

```
1 sudo apt update
2 sudo apt install libncurses5
```

1.5 November 19, 2023

1.5.1 Building AOSP HAL

Implementing the HAL

Device driver and its API are usually provided by a third-party hardware provider. Shim code include .h files for one or more device drivers.

New devices can communicate with the processor via USB which is popular. Even without driver, the device can be accessed with generic USB commands. *libusb*⁴ is

⁴<https://libusb.info>

a portable, user-mode, and USB-version agnostic library for using USB devices, and supports Android. If the device has a driver, it is likely to be a specialization of the USB command.

```

1  #ifndef PROXIMITY_HAL_H
2  #define PROXIMITY_HAL_H
3
4  #include <hardware/hardware.h>
5
6  #define ACME_PROXIMITY_SENSOR_MODULE "libproximityhal"
7
8  typedef struct proximity_sensor_device proximity_sensor_device_t;
9
10 struct value_range {
11     int min; int range;
12 };
13
14 typedef struct proximity_params {
15     struct value_range precision;
16     struct value_range proximity;
17 }
18
19 proximity_params_t;
20
21 struct proximity_sensor_device { hw_device_t common;
22     int fd;
23     proximity_params_t params;
24     int (*poll_sensor)(proximity_sensor_device_t *dev, int precision);
25 }; #endif // PROXIMITY_HAL_H

```

1.6 November 20, 2023

1.6.1 const Qualifier

When we have variables whose value we know cannot be changed, and We want to prevent code from inadvertently giving a new value to the variable, we define the variable's type as `const`:

```

1  const int bufSize = 512; // input buffer size
2  bufSize = 512; // error: attempt to write to const object

```

Because we can't change the value of a `const` object after we create it, it must be initialized:

```

1  const int i = get_size(); // ok: initialized at run time
2  const int j = 42; // ok: initialized at compile time
3  const int k; // error: k is uninitialized const

```

`const` is Local to the File

When a `const` object is initialized from a compile-time constant as in:

```

1  const int bufSize = 512;

```

the compiler will usually replace uses of the variable with its corresponding value during compilation. Thus, when we split a program to multiple files, every file that uses that `const` must have a access to its initializer. In order to see the initializer, the variable must be defined in every file that wants to use the variable's value. To support this, we define the `const` in one file, and declare it in other files that use that object.

```
1 // file_1.cc defines and initializes a const that is accessible to other files
2 extern const int bufSize = fcn();
3
4 // file_1.h
5 extern const int bufSize; // same bufSize as defined in file_1.cc
```

Because `bufSize` is `const`, we must specify `extern` in order for `bufSize` to be used in other files. `extern` signifies that `bufSize` is not local to this file and that its definition will occur elsewhere.

References to `const`

Unlike an ordinary reference, a reference to `const` cannot be used to change the object to which the reference is bound:

```
1 const int ci = 1024;
2 const int &r1 = ci; // ok: both reference and underlying object are const
3 r1 = 42; // error: r1 is a reference to const int &r2 =
4 ci; // error: nonconst reference to a const object
```

We can bind a reference to a `const` to a `nonconst` object, literals, or a more general expression:

```
1 int i = 42;
2 const int &r1 = i; // we can bind a const int& to a plain int object
3 const int &r2 = 42; // ok: r1 is a reference to const
4 const int &r3 = r1 * 2; // ok: r3 is a reference to
5 const int &r4 = r * 2; // error: r4 is a plain, nonconst reference
```

It is important to realize that a reference to `const` restricts only what we can do through that reference. Binding a reference to `const` to an object says nothing about whether the underlying object itself is `const`.

Pointers and `const`

Like a reference to `const`, a pointer to `const` may not be used to change the object to which the pointer points. We may store the address of a `const` object only in a pointer to `const`, where we can modify the pointer itself (change the reference stored inside) but not the object (value) pointed to:

```
1 const double pi = 3.14; // pi is const; its value may not be changed
2 double *ptr = &pi; // error: ptr is a plain pointer
3 const double *cptr = &pi; // ok: cptr may point to a double that is const
4 *cptr = 42; // error: cannot assign to *cptr
```

Like a reference to `const`, a pointer to `const` says nothing about whether the object to which the pointer points is `const`, that there is no guarantee that an object pointed to by a pointer to `const` won't change.

We can have a pointer that is itself `const`, and the address it holds cannot be changed. We indicate that the pointer is `const` by putting the `const` by the `const`:

```

1  int errNumb = 0;
2  int *const curErr = &errNumb; // curErr will always point to errNumb
3  const double pi = 3.14159;
4  const double *const pip = &pi; // pip is a constpointer to a const object
5
6  *pip = 2.72; // error: pip is a pointer to const and cannot be changed as the
               // pointer is const
7  // if the object to which curErrpoints (i.e., errNumb) is nonzero
8  if (*curErr) {
9      errorHandler();
10     *curErr = 0; // ok: reset the value of the object to which curErr is bound
                  // because errNumb is not const
11 }
```

Constant Expressions

A constant expression is an expression whose value cannot change and that can be evaluated at compile time. A literal is a constant expression. A `const` object that is initialized from a constant expression is also a constant expression:

```

1  const int max_files = 20; // max_files is a constant expression
2  const int limit = max_files + 1; // limit is a constant expression
3  int staff_size = 27; // staff_size is not a constant expression
4  const int sz = get_size(); // sz is not a constant expression
```

Although `staff_size` is initialized from a literal, it is not a constant expression because it is a plain `int`, not a `constint`. Even though `sz` is a `const`, the value of its initializer is not known until run time, and thus, `sz` is not a constant expression.

We can ask the compiler to verify that a variable is a constant expression by declaring the variable in a `constexpr` declaration. Variables declared as `constexpr` are implicitly `const` and must be initiated by constant expressions:

```

1  constexpr int mf = 20; // 20 is a constant expression
2  constexpr int limit = mf + 1; // mf+1 is a constant expression
3  constexpr int sz = size(); // ok only if size is a constexpr function
```

Because a constant expression is one that can be evaluated at compile time, only literal types (arithmetic, reference, and pointer) types can be defined as constant expressions. Custom classes, library IO and string types are not literal types. We can point (or bind) to an object that remains at a fixed address.

`constexpr` declaration applies to the pointer, not the type to which the pointer points:

```

1  const int *p = nullptr; // p is a pointer to a constint
2  constexpr int *q = nullptr; // q is a constpointer to int
```

`p` is a pointer to `const` (low-level), whereas `q` is a constant pointer (top-level).

1.6.2 Rudimentary AOSP HAL Application

Create Rudimentary Service source file, `rudi.cpp`, in `AOSP/device/generic/goldfish/app/wei_daemon`

```

1  #include <unistd.h>
2  #include <stdio.h>
3  #include <android/log.h>
4
5  #define DELAY_SECS 2
6  #define ALOG(msg) __android_log_write(ANDROID_LOG_DEBUG, "WEIMINN_PROJECT", msg)
7
8  int main(int argc, char *argv[]) {
9      ALOG("STARTING_WEIMINN_PROJECT");
10
11     int n = 0;
12     while (true) {
13         sleep(DELAY_SECS);
14         n++;
15
16         ALOG("TESTING");
17     }
18 }

```

And create Soong build file, `Android.bp` in the same folder:

```

1  cc_binary {
2      name: "weiminn_daemon",
3      relative_install_path: "hw",
4      init_rc: ["init.weiminn.rc"],
5      header_libs: [
6          "liblog_headers",
7      ],
8      srcs: [
9          "weiminn.cpp"
10     ],
11     shared_libs: [
12         "liblog",
13         "libcutils",
14     ],
15     static_libs: [
16     ],
17     vendor: true,
18     proprietary: true,
19 }

```

Add `wei_rudi_daemon` to the `PRODUCT_PACKAGES+=\` attribute of `AOSP/device/generic/goldfish/vendor.mk`

Add the startup script below to the end of the `init.rc` file:

```

1  service wei_rudi_daemon /vendor/bin/hw/wei_rudi_daemon
2      class main
3      user system
4      group system
5      oneshot

```

But the service cannot start due to SE Policy not being implemented for the service yet:


```

1 11-21 02:13:54.242 1862 1862 W cp : type=1400 audit(0.0:231): avc: denied {
    getattr } for path="/vendor/bin/hw/wei_rudi_daemon" dev="dm-3" ino=110
    scontext=u:r:shell:s0 tcontext=u:object_r:vendor_file:s0 tclass=file
    permissive=0

```

1.7 November 21, 2023

1.7.1 Fixing SELinux Policy to Start System Service

Add seclabel to the startup script:

```

1 service weiminn_daemon /vendor/bin/hw/weiminn_daemon
2     class main
3     user system
4     group system
5     seclabel u:r:ueventd:s0

```

Add start weiminn_daemon under on early-init right after start ueventd.

Got a new permission denied error this time:

```

1 11-21 09:45:47.732 0 0 E init : cannot execv('/vendor/bin/hw/weiminn_daemon'). See
    the 'Debugging init' section of init's README.md for tips: Permission denied
2 11-21 09:45:47.733 0 0 I init : Service 'weiminn_daemon' (pid 1402) exited with
    status 127
3 11-21 09:45:47.733 0 0 I init : Sending signal 9 to service 'weiminn_daemon' (pid
    1402) process group...

```

Adding device/generic/goldfish/sepolicy/x86/weiminn.te with following contents:

```

1 type weiminn, domain;
2 permissive weiminn;
3 type weiminn_exec, vendor_file_type, exec_type, file_type;
4
5 init_daemon_domain(weiminn)

```

and changed seclabel of the startup script to seclabel u:r:weiminn_exec:s0. And it reverts to the previous error:

```

1 11-21 10:19:43.865 0 0 I init : starting service 'weiminn_daemon'...
2 11-21 10:19:43.866 0 0 F init : cannot setexeccon('u:r:weiminn_exec:s0') for
    weiminn_daemon: Invalid argument
3 11-21 10:19:43.867 0 0 I init : Service 'weiminn_daemon' (pid 1827) exited with
    status 6
4 11-21 10:19:43.868 0 0 I init : Sending signal 9 to service 'weiminn_daemon' (pid
    1827) process group...
5 11-21 10:19:43.868 0 0 I libprocessgroup : Successfully killed process cgroup uid
    1000 pid 1827 in 0ms

```

1.7.2 Memory Dump

Try on Android Emulator

Set up emulator environment by appending the following inside ~/.bashrc:

```

1 export ANDROID_SDK_ROOT=~/.Android/Sdk
2 export ANDROID_HOME=~/.Android/Sdk
3 export ANDROID_AVD_HOME=~/.android/avd
4
5 PATH=$PATH:$ANDROID_SDK_ROOT/emulator

```

Register the path:

```
1 source ~/.bashrc
```

Create new AVD, Pixel 7 Pro with Tramisu (Android 13 with Google APIs, not Google Play), via Android Studio.

Run emulator using command:

```
1 emulator -avd Pixel_7_Pro_API_33
```

Load APK into emulator:

```

1 adb devices # to get id of running instance
2 adb root
3 adb install -r de.drmaxnix.birthdaycountdown.apk

```

Clone Fridump⁵:

```

1 git clone https://github.com/Nightbringer21/fridump
2 code fridump
3 pip install frida frida-tools

```

Download and Run Fridump dependencies:

```

1 git clone https://github.com/Nightbringer21/fridump
2 code fridump
3 adb push frida-server /data/local/tmp
4 sudo sysctl kernel.yama.ptrace_scope=0 && frida-ps -D emulator-5554
5 frida-ps -D emulator-5554 | grep Birth # to get process ID of the Birthday app
6
7 # inside emulator shell
8 ./data/local/tmp/frida-server

```

Found out that Fridump doesn't support the latest Android 13 and API 34, so download Android 10 with API 29 with Pixel 3a.

Run Fridump:

```
1 python fridump.py -U -s Birthday\ Countdown
```

and it works now!

1.8 November 22, 2023

1.8.1 C++ Data Structure

Sales_item Struct

The data structure does not support any operations⁶ any requires the user to implement the operations themselves:

⁵<https://pentestcorner.com/introduction-to-fridump>

⁶Basically, class with only attributes, and no methods.

```

1 struct Sales_data {
2     std::string bookNo;
3     unsigned units_sold = 0;
4     double revenue = 0.0;
5 };

```

The names defined inside the class must be unique within the class but can reuse names defined outside the class. We define data members the same way that we define normal variables: We specify a base type followed by a list of one or more declarators.

The close curly that ends the class body must be followed by a semicolon. The semicolon is needed because we can define variables after the class body:

```

1 struct Sales_data { /* ... */ } accum, trans, *salesptr;
2 // equivalent, but better way to define these objects
3 struct Sales_data { /* ... */}; Sales_data accum, trans, *salesptr;

```

The semicolon marks the end of the (usually empty) list of declarators. Ordinarily, it is a bad idea to define an object as part of a class definition. Doing so obscures the code by combining the definitions of two different entities—the class and a variable—in a single statement.

We use the dot operator (.) to read into the member attributes of the object:

```

1 Sales_data data1, data2;
2 double price = 0; // price per book, used to calculate total revenue
3
4 // read the first transactions: ISBN, number of books sold, price per book
5 std::cin >> data1.bookNo >> data1.units_sold >> price;
6
7 // calculate total revenue from price and units_sold
8 data1.revenue = data1.units_sold * price;
9
10 // read the second transaction
11 std::cin >> data2.bookNo >> data2.units_sold >> price;
12 data2.revenue = data2.units_sold * price;

```

Preprocessor

In order to ensure that the class definition is the same in each file, classes are usually defined in header files. Typically, classes are stored in headers whose name derives from the name of the class. Thus, we will define our `Sales_data` class in a header file named `Sales_data.h`.

Headers often need to use facilities from other headers. For example, because our `Sales_data` class has a string member, `Sales_data.h` must `#include` the string header. As we've seen, programs that use `Sales_data` also need to include the string header in order to use the `bookNo` member. As a result, programs that use `Sales_data` will include the string header twice: once directly and once as a side effect of including `Sales_data.h`. Because a header might be included more than once, we need to write our headers in a way that is safe even if the header is included multiple times.

The **preprocessor** is a program that runs before the compiler and changes the source text of our programs. Our programs already rely on one preprocessor facility, `#include`. When the preprocessor sees a `#include`, it replaces the `#include` with the contents of the specified header.

Header guards can be defined using the preprocessor. Preprocessor variables have one of two states: defined and not defined. `#define` directive takes a name as a preprocessor variable. `#ifdef` is true if the variable has been defined, and `#ifndef` is true if the variable has not been defined. If the test is true, then everything following the `#ifdef` or `#ifndef` is processed up to the matching `#endif`:

```

1  #ifndef SALES_DATA_H
2
3  #define SALES_DATA_H
4  #include <string>
5
6  struct Sales_data {
7      std::string bookNo;
8      unsigned units_sold = 0;
9      double revenue = 0.0;
10 };
11
12 #endif

```

The first time `Sales_data.h` is included, the `#ifndef` test will succeed. The preprocessor will process the lines following `#ifndef` up to the `#endif`. As a result, the preprocessor variable `SALES_DATA_H` will be defined and the contents of `Sales_data.h` will be copied into our program. If we include `Sales_data.h` later on in the same file, the `#ifndef` directive will be false. The lines between it and the `#endif` directive will be ignored.

Preprocessor variables, including names of header guards, must be unique throughout the program. Typically we ensure uniqueness by basing the guard's name on the name of a class in the header. To avoid name clashes with other entities in our programs, preprocessor variables usually are written in all uppercase.

1.9 November 23, 2023

1.9.1 C++ Types and Data Structures

Aliases

Traditionally, we use `typedef` for synonym for another type:

```

1  typedef double wages; // wages is a synonym for double
2  typedef wages base, *p; // base is a synonym for double, p for double*

```

The new standard introduced a second way to define **alias declaration** type alias:

```

1  using SI = Sales_item; // SI is a synonym for Sales_item

```

It is also possible to declare "pointer to" alias:

```

1 typedef char *pstring;
2 const pstring cstr = 0; // equivalent to char *const cstr = 0;
3 const pstring *ps; // equivalent to const char *ps;

```

auto Type Specifier

We can let the compiler deduce the type from the initializer for us by using the auto type specifier:

```

1 // the type of item is deduced from the type of the result of adding val1 and val2
2 auto item = val1 + val2; // item initialized to the result of val1+val2

```

The initializer for all the variables must have types that are consistent with each other:

```

1 auto i = 0, *p = &i; // ok: i is int and p is a pointer to int
2 auto sz = 0, pi = 3.14; // error: inconsistent types for sz and pi

```

auto ignores top-level consts, and only low-level initializer are usually kept:

```

1 auto i = 0, *p = &i; // ok: i is int and p is a pointer to int
2 auto sz = 0, pi = 3.14; // error: inconsistent types for sz and pi

```

1.10 November 25, 2023

1.10.1 Android Memory Dump

Heap Dump

```

1 adb shell am dumpheap <PID> <HEAP-DUMP-FILE-PATH>
2 adb shell cat <HEAP-DUMP-FILE-PATH> > <LOCAL-FILE-PATH>
3 strings <LOCAL-FILE-PATH> <LOCAL-FILE-PATH-FOR-STRINGS>
4
5 pip install objection
6 frida-ps -Uai
7 # objection -g de.drmaxnix.birthdaycountdown explore
8 objection -g bloodpressure.bpdinary explore
9
10 android hooking list classes #List all loaded classes, As the target application
    gets usedmore, this command will return more classes.
11
12 android hooking search classes bloodpressure.bpdinary
13 android hooking search methods bloodpressure.bpdinary recordDbActivity
14
15 android hooking watch class bloodpressure.bpdinary.recordDbActivity --dump-args --
    dump-return
16
17 android hooking watch class_method bloodpressure.bpdinary.recordDbActivity.
    showWeight --dump-args --dump-backtrace --dump-return

```

1.11 November 27, 2023

1.11.1 Android Profile Guided Compilation

7 8

Baseline Profiles

```

1 adb shell cmd package dump-profiles bloodpressure.bpdiaary
2 adb shell cat /data/misc/profman/bloodpressure.bpdiaary-primary.prof.txt >
  bpdiaary_profile.txt

```

Perfetto

Simpleperf

9

```

1 git clone https://android.googlesource.com/platform/system/extras
2 cd extras/simpleperf/demo/scripts/
3 python3 app_profiler.py -p simpleperf.example.java
4 python3 report_html.py --add_source_code --source_dirs ../demo --add_disassembly
5 sudo apt-get install python3-tk
6 ./report.py

1 python3 app_profiler.py -p bloodpressure.bpdiaary
2 adb shell /data/local/tmp/simpleperf record -o /data/local/tmp/perf.data -e task-
  clock:u -f 1000 -g --duration 10 --log info --app bloodpressure.bpdiaary

```

Profcollct

10

This is only supported by Coresight ETM-enabled ARM devices, so emulator doesn't work.

Inside ADB shell:

```

1 device_config put profcollect_native_boot enabled true
2 setprop persist.device_config.profcollct_native_boot.collection_interval 60
3 setprop persist.device_config.profcollct_native_boot.sampling_period 1000
4 setprop persist.device_config.profcollct_native_boot.max_trace_limit 53687091200
5 setprop persist.device_config.profcollct_native_boot.enabled true
6 setprop ctl.stop profcollectd
7 setprop ctl.start profcollectd
8 ps -e | grep profcollectd

```

⁷<https://developer.android.com/games/agde/pgo-overview>

⁸<https://newandroidbook.com/files/ArtOfDalvik.pdf>

⁹<https://android.googlesource.com/platform/system/extras/+/main/simpleperf/demo/README.md>

¹⁰<https://android.googlesource.com/platform/system/extras/+/master/profcollectd/>

1.12 November 29, 2023

1.12.1 Android OAT Dump Parser

The format for OAT files is described in AOSP/art/dex2oat/linker/oat_writer.h.

.bss¹¹ is the portion of an object file, executable, or assembly language code that contains statically allocated variables that are declared but not have been assigned a value yet.

```

1 import argparse
2
3 # helper function
4 def findLineWith(arr, s):
5     for i in range(len(arr)):
6         if s in arr[i]:
7             return i
8
9 def parse_method(method_arr):
10     method_sig_raw = method_arr.pop(0)
11     method_sig_raw_ = method_sig_raw[0: method_sig_raw.index(',') + 1]
12     method_sig_raw__ = method_sig_raw_.split(':')[1:]
13     method_sig = method_sig_raw__[0].strip()
14
15     method_arr.pop(0) # discard "DEX CODE:"
16     endOfDex = findLineWith(method_arr, "OatMethodOffsets")
17     dexCode = method_arr[0: endOfDex]
18
19     startOfOat = findLineWith(method_arr, "CODE:")
20     nativeCode = method_arr[startOfOat+1:] # Exclude "CODE: "
21
22     parsed_method = {'method_sig': method_sig, 'dex': dexCode, 'native':
23         nativeCode}
24
25     # print("Parsed", method_sig)
26
27     return parsed_method
28
29 def parse_type(type_arr):
30     method_indexes = [i for i in range(len(type_arr)) if 'method_idx' in type_arr[
31         i]]
32     if len(method_indexes) > 0:
33         method_indexes.append(len(type_arr))
34     methods_raw = [type_arr[method_indexes[i]:method_indexes[i+1]] for i in range
35         (0, len(method_indexes)-1)]
36
37     methods = []
38     for mraw in methods_raw:
39         methods.append(parse_method(mraw))
40
41     return {'type_name': type_arr[0].split()[1], 'methods': methods}
42
43 def load_oat_dump(p):
44     f = open(p)
45     lines = f.readlines()
46 
```

¹¹<https://en.wikipedia.org/wiki/.bss>

```

44     # determine the start and end of DEX code
45     startOfOatDex = lines.index('OatDexFile:\n')
46     endOfOatDex = lines.index('OAT_FILE_STATS:\n')
47     OatDex = lines[startOfOatDex:endOfOatDex]
48
49     # extract the classes and types
50     type_indexes = [i for i in range(len(OatDex)) if 'type_idx' in OatDex[i]]
51     type_indexes.append(len(OatDex))
52     all_types = [OatDex[type_indexes[i]:type_indexes[i+1]] for i in range(0, len(
        type_indexes)-1)]
53
54     all_methods = []
55     all_methods_dict = {}
56
57     for t in all_types:
58         parsed = parse_type(t)
59         all_methods += parsed['methods']
60
61         for m in parsed['methods']:
62             all_methods_dict[m['method_sig']] = {}
63             all_methods_dict[m['method_sig']]['dex'] = m['dex']
64             all_methods_dict[m['method_sig']]['native'] = m['native']
65
66     # return all_methods
67     return all_methods_dict
68
69 def load_schema(p):
70     f = open(p)
71     lines = f.readlines()
72
73     schema = []
74     for l in lines:
75         split = l.split('|||')
76         schema.append(split[1][:-1]) # -1 to remove \n character
77         # print("Added schema", schema[-1])
78     return schema
79
80 parser = argparse.ArgumentParser(description='OAT_Debloatation_Checker')
81 parser.add_argument('--oat', type=str, help='OAT_Dump_TXT_file')
82 parser.add_argument('--schema', type=str, help='Debloating_schema_file')
83
84 try:
85     args = parser.parse_args()
86     # print("Options:", args.OAT, args.schema)
87
88     # Load Debloated OAT Dump
89     print("Debloated_OAT_Dump:", args.oat)
90     normal_methods = load_oat_dump(args.oat)
91     # normal_methods = load_oat_dump('prelim_results/com.storiestime/10
        min_normal_com.storiestime_oat_dump.txt')
92
93     # Load Schema
94     print("Schema_File:", args.schema)
95     schema = load_schema(args.schema)
96     # schema = load_schema('Money_script/success_schema/169_com.
        storiestime_removed_methods.txt')
97
98     # Check if debloated
99     for m in schema:

```



```
100         retrieve = normal_methods[m]
101         if 'NO_CODE!' in retrieve['native'][0]:
102             print(m, 'is debloated!')
103         else:
104             print(m, 'is not debloated!')
105
106         # print('test')
107     except Exception as e:
108         print("Exception!", str(e))
```

