Evaluating the Reliability of Android Userland Memory Forensics

Sneha Sudhakaran¹, Aisha Ali-Gombe², Andrew Case³ and Golden G Richard III¹

¹Department of Computer Science, Louisiana State University, Baton Rouge, USA

²Department of Computer Science, Towson University, Towson, USA

³Board of Directors, Volatility Foundation, Reston, USA

ssudha1@lsu.edu aaligombe@towson.edu andrew@dfir.org golden@cct.lsu.edu

Abstract: Memory Forensics is one of the most important emerging areas in computer forensics. In memory forensics, analysis of userland memory is a technique that analyses per-process runtime data structures and extracts significant evidence for application-specific investigations. In this research, our focus is to examine the critical challenges faced by process memory acquisition that can impact object and data recovery. Particularly, this research work seeks to address the issues of consistency and reliability in userland memory forensics on Android. In real-world investigations, memory acquisition tools record the information when the device is running. In such scenarios, each application's memory content may be in flux due to updates that are in progress, garbage collection activities, changes in process states, etc. In this paper we focus on various runtime activities such as garbage collection and process states and the impact they have on object recovery in userland memory forensics. The outcome of the research objective is to assess the reliability of Android userland memory forensic tools by providing new research directions for efficiently developing a metric study to measure the reliability. We evaluated our research objective by analysing memory dumps acquired from 30 apps in different Process Acquisition Modes. The Process Acquisition Mode (PAM) is the memory dump of a process that is extracted while external runtime factors are triggered. Our research identified an inconsistency in the number of objects recovered from analysing the process memory dumps with runtime factors included. Particularly, the evaluation results revealed differences in the count of objects recovered in different acquisition modes. We utilized Euclidean distance and covariance as the metrics for our study. These two metrics enabled the authors to identify how the change in the number of recovered objects in PAM impact forensic analysis. Our conclusion revealed that runtime factors could on average result in about 20% data loss, thus revealing these factors can have an obvious impact on object recovery.

Keywords: Userland, Memory Dump Acquisition, Reliability, Metric Evaluation

1. Introduction

In a recent survey conducted, the Android operating system makes up 71.9% of the mobile operating system market share (Market Share, 2020). The survey results prove the popularity of the operating system among endusers. Over the last decade, there was a parallel increase in cybercrimes, causing damage that cost up to \$6 trillion in February 2021 (Market Crime, 2021). Digital forensics is a branch of forensic science used for recovering, investigating, and examining digital devices to recover evidences (Auty et al., 2007). Memory forensics is one of the techniques in digital forensics for extracting evidence from digital media that can serve as evidence for solving such cyber-crimes (Sylve et al., 2012). This technique can be an efficient solution to extract evidence and solve cybercrime, thereby making end-users more secure. Among different memory forensics techniques, userland (process memory) memory forensics is one important research area for analyzing applications (app) and activities associated with the app is essential in today's cyber world (Auty et al., 2007). One of the most critical components impacting evidence recovery is process memory acquisition (Pagani et al. 2019). The acquisition must be performed with utmost attention to conquer the challenges that persist. While some research has been done on challenges faced during the memory dump acquisition(Pagani et al. 2019), to the best of our knowledge, there is very little research that focuses on external runtime factors that can affect evidence recovery from process dumps that includes RecOOP (Pridgen et al.). The primary focus of this paper is to conduct a study on the impact of the external runtime factors like the Garbage Collection (GC) and the Process States and finally develop a metric evaluation to assess the reliability of userland memory forensic tools. The external factors like GC during process memory acquisition impact object recovery because the number of objects allocated and recovered without GC occurring is more than objects allocated and recovered after GC's occurrence. The object count difference is primarily because some objects are collected and lost after a GC cycle. The difference in object count was observed in different process states and is described in detail. First, we present a methodology to identify the impact on process memory samples with combinations of external runtime factors on object recovery using some available and free Android userland memory forensic tools (Ali-Gombe et al., 2019) and (Sudhakaran et al., 2020). Next, we evaluated multiple apps and derived a metric evaluation criterion for measuring the reliability of userland forensic tools on process memory capture acquired by incorporating the runtime factors during the dump acquisition. The study and conclusion deduced from this research were based on the count of objects recovered from process memory dumps with runtime factors included using current Android memory forensic tools. Developing a metric evaluation is needed because of the noticeable changes in the number of objects retrieved. The difference in the number of objects recovered helped us analyze the integrity, consistency, and data loss in different dumps acquired. Therefore, we could better understand userland memory forensic tools' reliability using metrics like Euclidean distance and covariance.

1.1 Contribution

- Examining the impact of Garbage Collection and Process States on evidence recovery in userland memory.
- Quantifying the integrity, consistency, and damage in recovered data.
- Measuring the reliability of userland memory forensics techniques using metrics like Euclidean distance and Covariance.

The rest of the paper is organized as follows: Section 2 presents the Background of this paper; Section 3 provides an overview of our Design and implementation; Section 4 presents the Evaluation of the proposed approach; Section 5 summarizes the Related Literature and finally section 6 presents the Conclusion

2. Background

2.1 Android Runtime Environment

Android executes apps in an application runtime environment called Android Runtime (ART) (Ali-Gombe et al., 2019) (Schwermer et al., 2018). ART introduced significant improvements like GC and better debugging (Schwermer et al., 2018) (Ali-Gombe et al., 2019) (ART Space, 2017). In Android 8, the developers improved ART by introducing features like Concurrent Copying GC (Ali-Gombe et al., 2019) enabling smaller heap sizes and faster object allocation and deallocation (Schwermer et al., 2018). First, the technique uses a concurrent and moving garbage collection algorithm. Utilizing region-based memory allocation(Ali-Gombe et al., 2019), allocated objects are evacuated from a region and subsequently destroyed if and only if the region has live objects whose count is less than some percentage threshold. Also, this algorithm creates a compacting heap by introducing short pauses during collection. It also utilizes a read barrier configuration to ensure mutators never see old versions of objects. This configuration allows threads to efficiently and concurrently access heap objects during collection. The algorithm uses the RegionSpace allocator, and if the use of TLAB is enabled, the system uses the RegionSpaceTlab allocator for movable objects. On newer Android versions, RegionSpaceTlab (Ali-Gombe et al., 2019) is the default for most small object allocations and LargeObjectSpace (Sudhakaran et al., 2020) for large object allocations. Second, the core Android system components and services like ART are built from native code that relies on native libraries written in C/C++ (ART Platform, 2017). Finally, ART's memory management does not provide a memory swap area but instead uses paging mechanisms and file mapping (Soares, A.M.M., de Sousa Jr, RT, 2017). Overall, for end-users, ART is more beneficial than its predecessor Dalvik by offering improved performance and faster application start-up time (ART Dalvik, 2017). In ART, improvements like Foreground and Background collectors are used when an app is in Foreground and Background process states (Ali-Gombe et al., 2019). This research intends to study in detail the GC and process state improvements made in ART and identify how they impact consistency, data loss/integrity, and reliability of forensic evidence recovery tools.

2.2 Object Allocation and Deallocation

In Android, object allocation utilizes memory management algorithms based on the size of the object (AndroidLOS, 2017) (Ali-Gombe et al., 2019) (Sudhakaran et al., 2020). Objects with an allocation size of fewer than 12KB are small objects like primitives, strings, arrays, and other complex objects such as InetAddress and are allocated using the *Alloc()* function (Ali-Gombe et al., 2019). On the other hand, the *AllocLarge()* function allocates large objects above a certain threshold of 12KB (Sudhakaran et al., 2020). The small objects are allocated using the region-based memory management algorithm, and the large objects are allocated using the large object space algorithm. In a region-based algorithm, objects get allocated in specific memory regions. During GC, an entire region is garbage collected if the objects in the corresponding region alive are below a certain threshold. The Large Object Space (LOS) gets allocated in a region in the process memory called Dalvik Large Object Allocation. In ART, LOS uses discontinuous memory mapping, where object allocation regions are not contiguous. LOS allocates objects in the form of arrays of types such as byte, char, string, float, and int

(AndroidLOS, 2017) (Sudhakaran et al., 2020). The objects and the associated references in the allocated spaces are freed when the allocated object is not alive with a *Free()* function (ART Free, 2017).

2.3 Garbage Collection

There are four major GC algorithms designed for ART. The algorithms are *Semi-Space, Generational Semi-Space, Concurrent Mark Sweep, and Concurrent Copying* (Ali-Gombe et al., 2019) (Jones et al., 2016). Beginning with Android 8, the default GC plan is Concurrent Copying (Ali-Gombe et al., 2019). The other GC plan used in ART is Concurrent Mark Sweep (ART Developers, 2017). When utilizing region-based memory allocation, allocated objects in the region having a live object count less than a certain threshold are evacuated from a region and subsequently destroyed (Ali-Gombe et al., 2019). Similarly, allocated objects having an object count greater than the threshold utilize LOS allocation and the objects are collected and destroyed if and only if the object and its reference are no longer alive. In such situations, the function *FinishGC()* (FinishGC, 2017) is enabled indicates that GC has been enabled. Otherwise, the GC is reset or disabled when the *ResetGCPerformanceInfo()* (ResetGC, 2017) function/method is triggered.

2.4 Process State

In an Android system, the process state is the highest-ranking active component within the app that it hosts (Android Process, 2017). Foreground processes have highest priority & empty processes have lowest priority as shown in Figure 1.



Figure 1: Android Process States

Android's different process states are foreground, background, visible, service, and empty (Android Process, 2017). The different process states are explained below:

2.4.1 Foreground Process

Foreground processes (Android Process, 2017) are the process or the app that is currently an active process running in the Android system and is last to be terminated by the system. A process is in foreground state if it meets one or more of the following conditions given below:

- The process involves activities with user interaction.
- Process hosting a service-connected to user interacting activities.
- Service that is triggered by a function call to *startForeground()*.
- Process that holds services like onCreate(), onResume() or onStart(), onReceive() calls.

2.4.2 Visible Process

A process is classified as a 'visible process' if it contains an activity visible to the user while the activity does not involve interaction with the user (Android Process, 2017).

2.4.3 Service Process

Processes that contain a service that has already been started and is currently in execution are classified as service process (Android Process, 2017).

2.4.4 Background Process

These processes contain activities neither visible to the user nor hosting a service. Android maintains a dynamic list of background processes, terminating processes such that processes that were the least recently in the foreground are killed first (Android Process, 2017).

2.4.5 Empty Process

Empty processes no longer contain any active applications but reserve memory space and serve as hosts for newly launched applications (Android Process, 2017).

This research focuses only on Foreground and Background process states.

3. Analysis Setup

3.1 Experimental Setup

In this work, we used the Genymotion Android emulator in the experimental setup as the execution environment (Genymotion, 2016) to evaluate the selected apps. We created Android Virtual Devices (AVD's) for the Samsung S8 emulator running Android 8.0-API 26 and apps chosen from different categories like Browser, Entertainment, SMS, Social media, Vault, Gaming, and malicious apps from Google Playstore(GooglePlay, 2021) and VirusShare(VirusShare, 2021).

All the emulators had 4GB memory, and selected apps were installed and loaded with chat messages, multiple images, text files, videos to simulate a series of actions performed by a user on real devices. We interacted with all the apps selected manually, with a similar sequence of actions conducted on each app to generate consistent activities for evaluation. E.g., The app *com.appstalking.photoeditor* was installed on the Genymotion emulator, and we performed a sequence of actions in both Foreground and Background states. In the Foreground process state, the activities include opening the app and typing a text message, then uploading an image saved in the Genymotion emulator. Next, we uploaded and edited a pdf file, and finally uploaded a video and watched the video. For the background process state, we repeat the same sequence of actions performed on the *com.appstalking.photoeditor* when it was in the foreground, before putting it in the background with a Gmail app made as a foreground app.

3.2 Process Acquisition Modes

As mentioned above, this research leverages two external runtime factors GC and process states. In Figure 2, the memory layout called the vtype (Auty et al., 2007) is explained to understand the different parameters and their memory offsets in the automated script to confirm if the process dump acquired includes the runtime factors or not. The automated script used to check the existence of each runtime factor will be made open source when the paper is published. The heap in the process dump acquired has the vtypes on which this work focuses. The specific vtypes focussed in this work includes GC_collector at location 504; card_table_ at 56; last_gc_type_ at 224; next_gc_type_ at 228; desired_collector_ at 100; block_gc_count_ at 584; block_gc_time_ at 592; gc_plan_ at 440 an concurrent_ copying_ collector_ at 524 as shown in Figure 2.

```
'Heap': [8x6388, {

'GC_collector': [584, ['']],
'card_table': [56, ['']],
'last_gc_type': [274, ['']],
'next_gc_type': [278, ['']],
'desired_collector': [186, ['']],
'block_gc_time_': [584, ['']],
'block_gc_time_': [582, ['']],
'gc_plan__: [448, [']],
'concurrent_copying_collector': [524, ['']],
]],
```

Figure 2: Runtime Structure for External Runtime Factors in Memory

In the case of GC, we identified that when GC is enabled the variables blocking_gc_count is 1 and blocking_gc_time holds some integer(FinishGC, 2017). While the GC is not enabled, the variables blocking_gc_count and blocking_gc_time are set to 0 (ResetGC, 2017). In the case of Process State, the variable desired_collector_ holds a value that indicates if the process was running in the Foreground or Background. The desired_collector_ is 7 when the app is running in foreground and desired_collector_ is 8 when the app runs in background. On executing the automated script on all the selected app for analysis each PAM mode gives the corresponding output mentioned below

3.2.1 F-GC

The variable types with values for this memory dump are desired_collector_= 0x07; block_gc _count_ = 1; block_gc_time_= <value>.

3.2.2 F-NGC

The variable types with values for this memory dump are $desired_collector_= 0x07$; $block_gc_count_=0$; $block_gc_time_= 0$.

Sneha Sudhakaran et ak

3.2.3 B-GC

The variable types with values for this memory dump are <code>desired_collector_= 0x08; block_gc_count_= 1; block_gc_time_=<value>.</code>

3.2.4 B-NGC

The variable types with values for this memory dump are $desired_collector_= 0x08$; $block_gc_count_= 0$; $block_gc_time_= 0$.

3.2.5 Clean

This state of process dump acquisition is the fresh state when the app runs with no runtime state triggered. The combination would be a default condition when a user opens the app and interacts in the foreground. This state is acquired every time before acquiring the process memory with the runtime factor triggered. CleanFGC is the process memory dump acquired before acquiring the F-GC combination dump. Similarly, we acquired a clean dump before F-NGC, B-NGC, and B-GC, and the memory acquisition modes were called CleanFNGC, CleanBNGC, and CleanBGC, respectively.

3.3 Process Memory Acquisition For Analysis

Figure 3 depicts the system architecture of this analysis study. The app memory dump is acquired with an automated tool called Memfetch (Memfetch, 2009) with different runtime factors included, and the process dumps acquired are called the process acquisition mode (PAM). The Memfetch tool is more beneficial as this research mainly focuses on userland memory analysis. Memfetch extracts all anonymous memory blocks like the stack and heap used for object allocation (mem pages) and pages used for files and executables mappings (map pages) into distinct binary files called the mem*.bin and the map*.bin respectively (Memfetch, 2009). Memfetch further provides a statistical metadata file that shows the range, size, segment of each acquired memory block in a file called the mfetch.lst. These files are then analyzed by forensic tools to recover all the objects. In our research, we focus specifically on two runtime factors, the GC and Process States.

In the automated script (https://github.com/ssudha1/metrics/tree/main), before we used Memfetch for acquiring process dumps, we initiated the two runtime factors. The GC was forced from the Android shell using 'adb shell kill -10 PID' where 'kill -10' signals SIGUSR1 (ForceGC, 2013), and PID is the process id of the application. However, the process states during memory acquisition were based on the manual setting by the end-user. We focus on the Foreground and Background process states which predominantly relate to user input. These states occur when the user acquires the process dump by running the automated script. The Foreground state is where the user interacts with the application, and the Foreground Collector gets triggered. The Background process state is where the application under execution is not visible to the user, and the Background Collector is triggered. E.g When the user starts the app in the Foreground process state and then executes the automated script (https://github.com/ssudha1/metrics/tree/main), it generates a process dump without GC enabled called Foreground and No GC enabled (F-NGC) followed by a dump with GC enabled called Foreground and GC triggered(F-GC). Similarly, when the user starts the app in the Background state and the automated script(https://github.com/ssudha1/metrics/tree/main) is executed, the process dump acquired would be initially the dump without GC enabled called Background and No GC enabled (B-NGC) followed by a dump with GC called as the Background and GC enabled (B-GC).

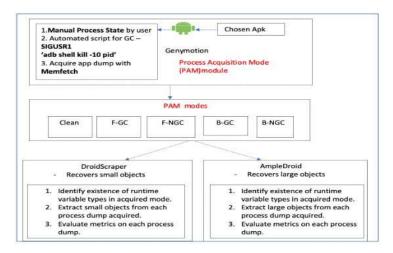


Figure 3: Design Architecture for Evaluation

3.4 Analysis Tools

3.4.1 DroidScraper

Ali-Gombe et al. proposed DroidScraper (Ali-Gombe et. al, 2019), a tool for analyzing the ART RegionSpace memory allocation to extract small objects from process dumps. This tool recovers runtime data

structures by focusing on the recovery of small objects allocated in the RegionSpace. DroidScraper is a userland in-memory object recovery and reconstruction tool to extract runtime artifacts from Android process memory space. The evaluation of DroidScraper has shown that it can recover in-memory data allocated using Android's RegionSpace by using RegionSpaceTlab allocator for recovering small objects with a recovery percentage of almost 90%. Also, DroidScraper can reconstruct and recover objects, thereby detecting evidence of file and network activities, database accesses, and recovery of cryptographic keys.

3.4.2 AmpleDroid

Sudhakaran et al. proposed a tool AmpleDroid (Sudhakaran et. al, 2020) a tool to analyze an Android app dump to extract the large objects allocated in the specific memory region called LargeObjectSpace. The LargeObjectSpace allocation is studied to identify how the objects above a certain threshold are stored in userland memory. AmpleDroid performs a complete process memory analysis on Android version 8 large object memory allocation and extracts multimedia and text files that other tools cannot currently retrieve. This tool is used in forensic investigations to provide an overall idea of how large object files (text, video, image, etc.) are allocated in an app's memory and a high recovery percentage of approximately 91%.

Lastly, in this experimental setup the forensic tools - DroidScraper (Ali-Gombe et al., 2019) and AmpleDroid (Sudhakaran et al., 2020) are used to recover the objects allocated in each acquisition mode. The final objects extracted from all the dumps will include a set of objects extracted from an Android app memory. Finally, the authors were able to identify the objects recovered in each dump and determine how reliable these forensic tools are in recovering objects from process memory.

4. Evaluation

We evaluated 30 apps in different process acquisition modes (cleanFGC, F-GC, cleanFNGC, F-NGC, cleanBGC, B-GC, cleanBNGC, B-NGC), and the results are shown in Figure 4. We evaluated 15 benign apps from different app categories:Browser, Editing, Entertainment, Gaming, SMS, Social Media and 15 malicious apps. Upon analysis, we identified that the process dumps with the acquisition modes - no GC and both process states (Foreground and background) extracted more small and large objects than the process dumps with acquisition modes GC and both process states. We used two metrics, Euclidean distance and covariance, to evaluate the data loss. The Euclidean distance calculated here gives the percentage of dissimilarity between two acquisition modes, e.g. (Data recovered in a clean state, data retrieved with runtime factor triggered). We used the covariance metric to examine the variability of data retrieved in different process acquisition modes, e.g., the variability of data recovered in F-NGC, F-GC, B-NGC, and B-GC. The results in in Figure 4 proves a greater probability for objects and their references get collected in the case of process acquisition modes F-GC and B-GC. On analysis with

Sneha Sudhakaran et ak

DroidScraper and AmpleDroid, we identified that the number of recovered objects in modes F-GC and B-GC was lower than F-NGC and B-NGC. in Figure 4 shows a significant difference in the small and large objects from all acquisition modes in certain benign entertainment apps like com.vid007.videobuddy, com.redbox.tv and com.ezscreenrecorder. The range of data loss calculated using Euclidean distance is approximately 10-20% in the case of GC acquisition modes while 0-10% in the case of No-GC acquisition modes. The data loss in terms of covariance ranges between .06 to .09 in (6-9% varying) both small and large objects. Therefore, we identified the change to be consistent in the case of entertainment apps. In the case of SMS apps, we identified the Euclidean distance as 7-17% and 0-7% for GC and No-GC process acquisition modes, respectively. We also determined that the covariance value was between .04 to .09 (4-9% varying). However, this consistency was not observed in Browser and Editing apps as we observed a Euclidean metric ranging from 0-19% in the case of all the acquisition modes and covariance variability from 0 to 11 (0 to 11% varying). Therefore, we could not identify a consistent range of percentage data loss but can conclude that the loss of data is restricted to 20% in the case of all benign and malicious applications. Thus, the garbage collected objects removed from memory might or might not serve as a loss of a critical piece of evidence during object recovery. In any case, if such pieces of evidence are not recovered, it eventually leads to issues that may question the reliability of forensic investigation tools. Such an object recovery can miss out on evidence that can also cause innocent users to be convicted. Therefore, on analyzing the difference in the count of objects recovered it is clear from in Figure 4 that the objects recovered using B-GC acquisition mode were fewer and had greater Euclidean distance compared to other modes. This also made us understand that among the process states lesser objects were recovered from Background compared to objects recovered from dumps in foreground. For E.g, on comparing F-GC and B-GC, more objects were recovered in F-GC compared to B-GC.

		Large	Large	Large	Large	Large	Large	Large	Large	Large	Large	Large	Large	Large:
Packagename	App Category	Clean-Fngc	F-NGC	Euclid%	Clean-Fgc	F-GC	Euclid'X	Clean-Bngc	B-NGC	Euclid%	Clean-Bgc	B-GC	Marine State of the State of th	Covariance
com.brave.browser	Browser	18	18	0.00%	19	16	15.79%	17	17	0.00%	17	14	17.65%	0.11
com.aniplex.fategrandorder	Browser	16	17.00	1 1000000	16	14	12.50%	15	107.5	10000000	15	13	13.33%	0.09
org.mozilla.fenix	Browser	12	0.151	2331227	12	11	8.33%	12	N 1500	1	11	11	20000	0.05
com.appstalking.photoeditor	Editing	18	1 22	9555597	17	16	5.88%	17	t: 1979	-	17	-	1,000	0.08
de.vsmedia.imagesize	Editing	16	1	05.00393	16	14	12.50%	16	10 10077	-	16	- 100	2 10 10 10 10 1	0.09
com.vid007.videobuddy	Editing	11	- 0		11	11	0.00%	11	1-	0.00%	11	11	1 000000	0.00
	100 CO (100 CO) (100 CO (100 CO (100 CO (100 CO) (100 CO) (100 CO (100 CO) (100	10	1	0000000	10	9	10.00%	10	3000	2000000	10	-		1750
com.redbox.tv	Entertainment	1977		050000	2755		2000000		1	0.000000	100	100	/// // // // // // // // // // // // //	0.06
com.ezscreenrecorder	Entertainment	28	20-10-2	1000000	28	27	3.57%	28	f 100 t	0.00000	28	24	7/10/2000	0.07
com.mp3.editor.music.cut.ringtone	Entertainment	30	1999	23900	30	27	10.00%	30	1 100	10.1100	. 30	25	7,000,000,000	0.06
com.tencent.iglite	Gaming	14	14	10000000	13	- 11	15.38%	13	ft (195)	10000000	13	- 11	////	0.12
com.anonymoustexting	Sms	14	14	50.100.00	14	13	7.14%	14	1000	200000	14	12	7550000000	0.07
com.smsplus.app	Sms	18			18	15	16.67%	17	1 10	-	17	15	-	0.06
co.kitetech.messenger	Sms	34	33	2.94%	34	31	8.82%	34	33	2.94%	. 34	31	8,82%	0.04
com.neeo.chatmessenger.ui	Social Media	29	29	0.00%	29	28	3.45%	29	29	0.00%	29	27	6,98%	0.03
gallery.hidepictures.photovault.lockgallery	Vault	19	19	0.00%	19	17	10.53%	19	18	5.26%	19	17	18.53%	0.05
com.nemo.vidmate	Malware	54	54	0.00%	54	48	11.11%	54	51	5.56%	50	46	8,08%	0.07
com.gihoo.appstore	Malware	37	37	0.00%	37	31	16.22%	35	33	5.71%	35	30	14.29%	0.09
com.wBestFreeGameCheatCodesGlitches	Malware	9	. 9	0.00%	9	8	11.11%	8	9	0.00%	9	8	11,11%	0.07
com.ss.android.article.news	Malware	12	12	0.00%	11	9	18.18%	11	10	9.09%	. 11	9	18.18%	0.14
com.namad.instafoliow	Malware	8	8	0.00%	8	8	0.00%	8	8	0.00%	8	8	8.08%	0
com.android.tencent.zdevs.bah	Malware	12	12	0.00%	12	11	8.33%	11	11	0.00%	11	10	9.09%	0.07
ru.delivery.collapse	Malware	22		700000	22	20	9.09%	21	1		21	19		0.06
com.isyjv.kixbinwc.r	Malware	9	9	0.00%	9	8	11.11%	9		0.00%	9	8	11,11%	0.07
org.doviz.cevir	Malware	15		100000000	15	13	13.33%	14	-	-	14	12		0.1
operatore.italia	Malware	13			13	11	15.38%	13		-	13	11		0.08
com.marjansb1.thanksglving	Malware	17		10000000	17	15	11.76%	17			17	14	A William Standard	0.08
com.amazon.mShop.android.shopping.ha	MONTH OF THE PARTY	18		5.56%	17	15	11.76%	17		-	17	14	17.65%	0.08
	Malware	10		- Andreadards	10	9	10.00%	10		10.00%	10	9	18.08%	0.05
com.androiddoctor.battery		10	8	0.00%	8	7	12.50%	8	-	0.00%	8	7	12.58%	0.08
com.maxauto.maxiplusap	Malware			- Contractories	100		10000000			-				
com.plato.dovizim	Malware	.26	26	0.00%	26	24	7.69%	26	25	3.85%	26	22	15.38%	0.07
		Consti	Ownell	County	Count		Consti	Const	Daniel .	Describ		Parall .	County	Power I
Diebassame	Ann Calanno	Small Class Face	Small	TOUR PLAN S	Small Class For	Small	Small	Small Class Rose	Small	Small	Small Clean Ban	Small	2010/03/03	Small
Packagename	App Category	Clean-Fngc	F-NGC	Euclid%	Clean-Fgc	F-GC	Euclid'W	Clean-Brigg	B-NGC	Euclid%	Clean-Bgc	B-GC	Euclid%	Covariance
com.brave.browser	Browser	Clean-Fngc 39159	F-NGC 39002	Euclid% 0.40%	Clean-Fgc 38162	F-GC 33241	Euclid% 12.90%	Clean-Brigg 38831	B-NGC 37198	Euclid% 4.21%	Clean-Bgc 38021	B-GC 33108	Euclid% 12.92%	Covariance 0.08
com.brave.browser com.aniplex.fategrandorder	Browser Browser	Clean-Fngc 39159 41629	F-NGC 39002 40998	Euclid% 0.40% 1.52%	Clean-Fgc 38162 40864	F-GC 33241 35912	Euclid% 12.90% 12.12%	Clean-Brigg 38831 40789	B-NGC 37198 40001	Euclid% 4.21% 1.96%	Clean-Bgc 38021 40008	B-GC 33108 35482	Euclid% 12.92% 11.31%	Covariance 0.08 0.07
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix	Browser Browser Browser	Clean-Fngc 39159 41629 36197	F-NGC 39002 40998 35098	Euclid% 0.40% 1.52% 0.28%	Clean-Fgc 38162 40864 35481	F-GC 33241 35912 30200	Euclid% 12.90% 12.12% 14.88%	38831 40789 33217	8-NGC 37198 40001 30777	Euclid% 4.21% 1.96% 7.35%	38021 40008 32163	B-GC 33108 35482 26939	12.92% 11.31% 16.24%	0.08 0.07 0.11
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor	Browser Browser Browser Editing	Clean-Fngc 39159 41629 35197 30189	F-NGC 39002 40998 35098 30007	0.40% 0.40% 1.52% 0.28% 0.60%	38162 38162 40864 35481 30619	F-GC 33241 35912 30200 26108	12.90% 12.12% 14.88% 14.73%	Clean-Bngc 38831 40799 33217 30201	8-NGC 37198 40001 30777 29009	Euclid% 4.21% 1.96% 7.35% 3.95%	38021 40008 32163 30765	8-GC 33108 35482 28939 27885	Euclid% 12.92% 11.31% 16.24% 9.36%	0.08 0.07 0.11 0.06
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.imagesize	Browser Browser Browser Editing Editing	39159 41629 35197 30189 48910	5-NGC 39002 40998 35098 30007 48008	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84%	38162 40864 35481 30619 48529	F-GC 33241 35912 30200 26108 41198	Euclid% 12.90% 12.12% 14.88% 14.73% 15.11%	Clean-Bngc 38831 40799 33217 30201 48873	8-NGC 37198 40001 30777 29009 42107	4.21% 4.21% 1.96% 7.35% 3.95% 13.84%	38021 40008 32163 30765 48003	8-GC 33108 35482 26939 27885 41298	Euclid% 12.92% 11.31% 16.24% 9.36% 13.97%	Covariance 0.08 0.07 0.11 0.06 0.08
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vid007.videobuddy	Browser Browser Browser Editing Editing Editing	39159 41629 35197 30189 48910 37603	F-NGC 39002 40998 35098 30007 48008 36998	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61%	38162 40864 35481 30619 48529 37062	F-GC 33241 35912 30200 26108 41198 30008	12.90% 12.12% 14.88% 14.73% 15.11%	Clean-Bage 38831 40799 33217 30201 48873 36458	8-NGC 37198 40001 30777 29009 42107 35002	Euclid% 4.21% 1.96% 7.35% 3.95% 13.84% 3.99%	38021 40008 32163 30765 48003 36897	B-GC 33108 35482 26939 27885 41298 32542	Euclid% 12.92% 11.31% 16.24% 9.36% 13.97% 11.88%	0.08 0.07 0.11 0.06 0.08 0.08
com.brave.browser com.aniplex.falegrandorder org.mozilla.fenix com.appstalikg.photoeditor de.vsmedia.imagesize com.vid007.videobuddy com.redbox.tv	Browser Browser Browser Editing Editing Editing Entertainment	Clean-Fngc 39159 41629 35197 30189 46910 37603 17889	F-NGC 39002 40988 35088 30007 48008 36998 17092	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.46%	Clean-Fgc 38162 40864 35481 30619 48529 37062 17167	F-GC 33241 35912 30200 26108 41198 30008 13998	Euclid% 12.90% 12.12% 14.88% 14.73% 15.11% 19.01% 18.46%	Clean-Bngc 38831 40799 33217 32201 48873 36458 17186	B-NGC 37198 40001 30777 29009 42107 35002 16917	Euclid% 4.21% 4.21% 1.96% 7.35% 3.95% 13.84% 3.99%	Clean-Bgc 38021 40008 32163 30765 48003 36897 17165	B-GC 33108 35482 26939 27885 41298 32542 15076	Euclid% 12.92% 11.31% 16.24% 9.36% 13.97% 11.88%	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.09
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vid07.videobuddy com.redbox.tv com.ezscreenrecorder	Browser Browser Browser Editing Editing Editing Entertainment	Clean-Fngc 39158 41629 35197 30189 48910 37603 17889 41332	F-NGC 39012 40988 35088 30007 49018 36988 17092 40975	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.46% 0.88%	Clean-Fgc 38162 40664 35481 30619 48529 37062 17167 41134	F-GC 33241 35912 30200 26108 41198 30008 13998 35882	Euclid% 12.90% 12.12% 14.88% 14.73% 15.11% 19.01% 18.46% 12.77%	Clean-Bngc 38831 40799 33217 30201 48873 38458 17185 41221	B-NGC 37198 40001 30777 29009 42107 35002 16917 39887	Euclid% 4.21% 1.98% 7.35% 3.95% 13.84% 3.99% 1.44% 3.24%	38021 40008 32163 30765 48003 36897 17165 41225	B-GC 33108 35482 26939 27885 41298 32542 15076 35667	Euclid%. 12.925 11.315 16.245 9.365 13.975 11.885 12.175 13.485	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.09
com.brave.browser com.aniplex.fategrandorder org.mozilia.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.esscreenrecorder com.mp3.editor.music.cut.ringtone	Browser Browser Browser Editing Editing Editing Editing Entertainment Entertainment	Clean-Fngc 39158 41628 35197 30188 48910 37603 17888 41332 28967	F-NGC 39002 40998 35098 30007 48008 36998 17092 40975 28103	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.46% 0.88% 2.98%	Clean-Fgc 38162 40864 35481 30619 48529 37062 17167 41134	F-GC 33241 36912 30200 26108 41198 30008 13998 23881	Euclid% 12.80% 12.12% 14.86% 14.73% 15.11% 19.01% 18.46% 12.77% 17.33%	Clean-Bngc 38831 40795 33217 30201 48873 38458 17185 41221 29940	B-NGC 37198 40001 30777 29009 42107 35002 16917 39887 27669	Euclid% 4.21% 1.96% 7.35% 3.95% 13.84% 3.99% 1.44% 3.24% 4.72%	Clean-Bgc 38021 40008 32163 30765 48003 36897 17165 41225 28867	B-GC 33108 35482 26939 27885 41298 32542 15076 35667 24997	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.175 13.485 13.415	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.09 0.07 0.08
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedla.imagesize com.vid007.videobuddy com.redbox.tv com.ezscreenrecorder com.mp3.editor.music.cut.ringtone com.tencent.igilite	Browser Browser Browser Editing Editing Editing Entertainment Entertainment Gaming	Clean-Fngc 39158 41628 35197 30189 48910 37603 17889 41332 26967 21761	F-NGC 39002 40988 35098 30007 48008 36998 17092 40975 28103 21668	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.46% 0.86% 2.98% 0.43%	Clean-Fgc 38162 40864 35481 30619 48529 37062 17167 41134 28886 21322	F-GC 33241 36912 30200 26108 41198 30008 13998 23881 17682	Euclid% 12.90% 12.12% 14.88% 14.73% 15.11% 19.01% 18.46% 12.77% 17.33% 17.07%	Clean-Bngc 38831 40795 33217 30201 48873 38458 17185 41221 29040 21325	B-NGC 37198 40001 30777 29009 42107 35002 18917 39887 27669 20534	Euclid% 4.21% 1.96% 7.35% 3.95% 13.84% 3.99% 1.44% 3.24% 4.72% 3.71%	Clean-Bgc 38021 40008 32163 30765 48003 36897 17165 28867 21583	B-GC 33108 35482 26939 27885 41298 32542 15076 35667 24997 17992	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.178 13.485 13.415	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.09 0.07 0.08 0.08
com.brave.browser com.aniplex.fatsgrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.escerearrecorder com.mp3.editor.music.cut.ringtone com.tencent.iglite com.anonymoustaxting	Browser Browser Browser Editing Editing Editing Entertainment Entertainment Gaming Sms	Clean-Fngc 39158 41628 35197 30189 48910 37603 17889 41332 26967 21761	F-NGC 39002 40988 35098 30007 48008 36998 17092 40975 28103 21668 38865	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.46% 0.86% 2.98% 0.43% 0.12%	Clean-Fgc 38162 40664 35481 30619 48529 37062 17167 41134 28866 21322 38664	F-GC 33241 35912 30200 26108 41198 30008 13998 23881 17682 33265	Euclid% 12.90% 12.12% 14.88% 14.73% 15.11% 19.01% 18.46% 12.77% 17.33% 17.07% 13.94%	Clean-Bngc 38831 40799 33217 30201 48873 36458 17185 41221 29040 21325 38912	B-NGC 37198 40001 30777 29009 42107 35002 18917 27669 20534 37798	Euclid% 4.21% 1.96% 7.35% 3.95% 13.84% 3.99% 1.44% 3.24% 4.72% 3.71% 2.86%	Clean-Bgc 38021 4008 32163 30765 48003 36897 17165 41225 28867 21583 38912	8-GC 33108 35482 26939 27885 41298 32542 15076 35667 24997 17992 34004	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.178 13.485 13.415 16.645 12.615	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.09 0.07 0.08 0.08 0.08 0.08 0.07 0.08
com.brave.browser com.aniplex.falegrandorder org.mozilla.fenix com.appstalkg.photoeditor dev.smedia.imagesize com.vid097.videobuddy com.redbox.tv com.essersenrecorder com.mp3.editor.music.cut.ringtone com.sment.igilite com.anonymoustexting com.smsplus.app	Browser Browser Browser Editing Editing Editing Editing Entertainment Entertainment Entertainment Gaming Sms Sms	Clean-Fngc 39159 41629 35197 30189 48910 37603 17889 44332 28967 21761 38910 31676	FNGC 39002 40988 35038 30007 49008 36988 17082 4975 28103 21688 38865 31789	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.46% 0.86% 2.98% 0.43% 0.12% 0.34%	Clean-Fgc 38162 40864 35481 30619 48529 37052 17167 41134 28886 21322 38664 31807	F-GC 33241 35912 30200 26108 41198 30008 13998 23881 17682 33265 26673	Euclid% 12.90% 12.12% 14.88% 14.73% 15.11% 19.01% 18.46% 12.77% 17.33% 17.07% 13.94% 16.46%	Clean-Bingc 388313 407896 33217 30201 488733201 488731 290450 21325 38912 31885	B-NGC 37198 40001 30777 29009 42107 35002 16917 39887 27669 20534 37798 29880	Euclid% 4.21% 1.96% 7.35% 3.95% 13.84% 3.99% 1.44% 3.24% 4.72% 3.71% 2.86% 6.29%	Clean-Bgc 38021 40008 32163 30765 48003 36897 17165 41225 28867 21583 38912 31885	B-GC 33108 35482 26939 27885 41288 32542 15076 35667 24997 17992 34004 26356	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.175 13.485 13.415 16.645 12.615	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.07 0.08 0.01 0.08
com.brave.browser com.aniplex.fatsgrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.escerearrecorder com.mp3.editor.music.cut.ringtone com.tencent.iglite com.anonymoustaxting	Browser Browser Browser Browser Edding Edding Edding Entertainment Entertainment Entertainment Saming Sms Sms Sms	Clean-Figs 39158 41629 35197 30188 48510 37603 37603 41332 28667 21761 38610 31876 53844	F-NGC 39002 40988 35088 35088 30007 48008 36988 17092 40975 28103 21668 38865 31766 53281	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.48% 0.29% 0.43% 0.12% 0.34% 1.05%	Clean=gc 38162 40864 35481 30619 48529 37062 17167 41134 28886 21322 38664 31807 52967	FGC 33241 35912 30000 26108 41198 30008 13986 23881 17682 33265 26673 47562	Euclid*\(\) 12.80% 12.12% 14.88% 14.73% 15.11% 19.01% 18.46% 12.77% 17.33% 17.07% 13.84% 16.46%	Clean-Brige 38831 407899 33277 30201 48873 34458 41221 29040 21326 38912 31885 53083	B-NGC 37198 400011 307777 290099 42107 35002 27699 20534 37798 29880 50832	Euclid% 4.21% 1.98% 7.35% 3.95% 13.84% 3.99% 1.44% 3.24% 4.72% 3.71% 2.88% 6.28% 4.24%	Clean-Bgc 38021 40086 32163 30765 48003 38897 17165 28867 21563 38912 31885 53001	8-GC 33108 35482 26939 27885 41298 32542 15076 24997 17992 34004 26356 47667	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.178 13.485 13.415 16.645 12.615 17.345 18.965	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.09 0.07 0.08 0.00 0.00
com.brave.browser com.aniplex.falegrandorder org.mozilla.fenix com.appstalkg.photoeditor dev.smedia.imagesize com.vid097.videobuddy com.redbox.tv com.essersenrecorder com.mp3.editor.music.cut.ringtone com.sment.igilite com.anonymoustexting com.smsplus.app	Browser Browser Browser Editing Editing Editing Editing Entertainment Entertainment Entertainment Gaming Sms Sms	Clean-Fngc 39158 41628 36197 36197 37603 17889 485101 37603 17889 41332 28867 217611 38610 31876 53844 43997	F-NGC 39022 40988 35098 35098 35098 36007 49008 2007 49008 2009 2009 2009 2009 2009 2009 2009	Euclid% 0.40% 1.52% 0.28% 0.60% 1.61% 4.46% 0.68% 2.99% 0.43% 0.12% 0.24% 1.05% 3.04%	Clean=gc 38162 40644 38162 40644 35481 30619 46523 47062 17167 41134 28866 21322 31644 31664 31664 42980	F-GC 33241 35912 3200 3200 26108 41199 30008 13598 23881 17682 23865 26573 47562 38038	Euclid*N 12.80% 12.12% 14.88% 14.88% 15.11% 19.01% 18.46% 12.77% 17.33% 17.07% 13.84% 16.46% 10.20%	Clean-Bingc 388311 407993 33217 33217 488727 39458 117189 41222 293444 21328 318186 53083 43007	B-NGC 37198 40001 30777 42000 42107 35002 16917 39887 27869 20534 37798 28880 58832 39005	Euclid% 4.21% 1.98% 7.35% 3.95% 13.84% 3.99% 4.72% 3.71% 2.88% 6.28% 4.24%	Clean-Bgc 38021 40008 32163 32163 32163 32163 36897 17165 41225 28867 21583 31885 53001 43603	8-9C 33108 35482 35482 26939 26939 26939 2795000000000000000000000000000000000000	Euclid's. 12,925 11,315 16,245 9,365 13,973 11,885 12,175 13,485 13,415 16,645 12,645 12,645	Covariance 0.08 0.07 0.11 0.08 0.08 0.09 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.07 0.08 0.10 0.09 0.09 0.09 0.07
com.brave.browser com.aniplex.falegrandorder org.mozilla.fenix com.appstalking.photoeditor de vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.essersenrecorder com.mp3.editor.music.cut.ringtone com.tencent.igilite com.anonymoustexting com.smsplvs.app co.kitetech.messenger	Browser Browser Browser Browser Editing Editing Editing Entertainment Entertainment Gaming Sms Sms Sms Social Media	Clean-Figs 39159 41629 35197 30189 480101 37603 17689 41332 28967 21761 318765 53844 43997	F-NGC 39012 40988 30012 40988 30008 30088 30088 30087 48008 30888 30087 40875 28133 21686 38855 31786 53288 42881 38974 42881	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.46% 0.88% 0.43% 0.12% 0.12% 0.34% 1.05% 3.04% 2.25%	Clean=gc 38162 40664 35481 30619 46529 37052 17167 41134 28886 21322 38654 42980 38994	F-GC 33241 35912 30200	Euclid*N 12.80% 12.12% 14.88% 14.88% 15.11% 19.01% 18.46% 12.77% 17.33% 17.07% 18.46% 10.20% 11.50% 17.43%	Clean-Bingc 388311 407993 33217 33217 33201 488733 34656 17166 41221 29344 21326 318865 53983 43007 39007	B-NGC 37198 40001 37198 40001 30777 29009 42107 35002 16917 39887 27699 20534 37988 50832 39005 50832 37420	Euclid% 4.21% 1.98% 7.35% 3.95% 13.84% 3.24% 4.72% 3.71% 6.28% 4.24% 4.25% 4.27%	Clean-Bgc 38021 40008 32163 32163 32163 380897 17165 41225 28867 21583 21583 388912 318885 53001 43603 39105	33108 35482 26939 26939 41288 41288 25542 15076 35667 24987 17992 34054 24055 47667 36431	Euclid% 12.925 11.315 16.248 9.365 13.975 11.885 12.175 13.485 13.415 16.645 12.613 17.345 18.655 16.455 7.955	Covariance 0.08 0.07 0.11 0.08 0.08 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.07 0.08 0.11 0.08
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vid07.videobuddy com.redbox.tv com.azscreenrecorder com.mp3.aditor.music.cut.ringtone com.tencent.igilite com.anonymoustexting com.anonymoustexting com.snsplus.app co.kitetoch.messenger com.neoo.chatmessenger.ui	Browser Browser Browser Browser Edding Edding Edding Entertainment Entertainment Gaming Sms Sms Sms Social Media	Clean-Fngc 39158 41628 36197 36197 37603 17889 485101 37603 17889 41332 28867 217611 38610 31876 53844 43997	F-NGC 39002 40988 35098 35098 35098 36007 49008 20007 49008 20007 2000 2000 2000 2000 2000 2000	Euclid% 0.40% 1.52% 0.28% 0.60% 1.61% 4.46% 0.68% 2.99% 0.43% 0.12% 0.24% 1.05% 3.04%	Clean=gc 38162 40644 38162 40644 35481 30619 46523 47062 17167 41134 28866 21322 31644 31664 31664 42980	F-GC 33241 35912 3200 3200 26108 41199 30008 13598 23881 17682 23865 26573 47562 38038	Euclid*N 12.80% 12.12% 14.88% 14.88% 15.11% 19.01% 18.46% 12.77% 17.33% 17.07% 13.84% 16.46% 10.20%	Clean-Bingc 388311 407993 33217 33217 488727 39458 117189 41222 293444 21328 318186 53083 43007	B-NGC 37198 40001 37198 40001 30777 29009 42107 35002 16917 39887 27699 20534 37988 50832 39005 50832 37420	Euclid% 4.21% 1.98% 7.35% 3.95% 13.84% 3.99% 4.72% 3.71% 2.88% 6.28% 4.24%	Clean-Bgc 38021 40008 32163 32163 32163 32163 36897 17165 41225 28867 21583 31885 53001 43603	8-9C 33108 35482 35482 26939 26939 26939 2795000000000000000000000000000000000000	Euclid's. 12,925 11,315 16,245 9,365 13,973 11,885 12,175 13,485 13,415 16,645 12,645 12,645	Covariance 0.08 0.07 0.11 0.08 0.08 0.09 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.07 0.08 0.10 0.09 0.09 0.09 0.07
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vide07.videobuddy com.redbox.tv com.asscreenrecorder com.mp3.editor.music.eut.ringtone com.tencent.igilite com.anonymoustaxting com.sns.plus.app co.kitetoch.messenger com.neoo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery.	Browser Browser Browser Browser Editing Editing Editing Entertainment Entertainment Gaming Sms Sms Sms Social Media	Clean-Figs 39159 41629 35197 30189 480101 37603 17689 41332 28967 21761 318765 53844 43997	F-NGC 39012 40988 30012 40988 30008 30088 30088 30087 48008 30888 30087 40875 28133 21686 38855 31786 53288 42881 38974 42881	Euclid% 0.40% 1.52% 0.28% 0.28% 1.84% 1.61% 4.49% 0.88% 0.12% 0.12% 0.34% 1.05% 3.04% 2.25% 0.88%	Clean=gc 38162 40664 35481 30619 46529 37052 17167 41134 28886 21322 38654 42980 38994	F-GC 33241 35912 30200	Euclid*N 12.80% 12.12% 14.88% 14.88% 15.11% 19.01% 18.46% 12.77% 17.33% 17.07% 18.46% 10.20% 11.50% 17.43%	Clean-Bingc 388311 407993 33217 33217 33201 488733 34656 17166 41221 29344 21326 318865 53983 43007 39007	8-NGC 37198 440011 30777 28009050 42107 350022 16817 27898 28880 28880 37420 42176 42176 42176 42176 42176 42176 42176 400001 37198 5800000000000000000000000000000000000	Euclid% 4.21% 1.98% 7.35% 3.95% 13.84% 3.24% 4.72% 3.71% 6.28% 4.24% 4.25% 4.27%	Clean-Bgc 38021 40008 32163 32163 32163 380897 17165 41225 28867 21583 21583 388912 318885 53001 43603 39105	33108 35482 26939 26939 41288 41288 25542 15076 35667 24987 17992 34054 24055 47667 36431	Euclid% 12.925 11.315 16.248 9.365 13.975 11.885 12.175 13.485 13.415 16.645 12.613 17.345 18.655 16.455 7.955	Covariance 0.08 0.07 0.11 0.08 0.08 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.07 0.08 0.11 0.08
com.brave.browser com.aniplex.fategrandorder org.mozilia.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.esscreenrecorder com.mp3.editor.music.cut.ringtone com.encent.igilite com.anonymoustexting com.anonymoustexting com.smp5lus.app co.kitetoch.messenger com.neoc.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.neon.vidmate	Browser Browser Browser Browser Browser Browser Browser Browser Edding Edding Edding Edding Entertainment Entertainment Seming Sms Sms Sms Social Media Vault Malware Malware	Clean-Fngc 39158 41628 41628 41628 48610 37603 17888 41332 28667 21761 38610 31576 4397 39670 43556	F-NGC 39002 40398 40398 35098 35098 40006 36998 17092 21035 21066 38865 31766 38865 31766 428616	Euclid% 0.40% 1.52% 0.28% 0.28% 1.84% 1.61% 4.49% 0.88% 0.12% 0.12% 0.34% 1.05% 3.04% 2.25% 0.88%	Clean-Fgc 381624 40864 40864 336191 46529 37052 17167 41184 28886 21322 38664 31807 52987 42888	F-GC 33241 35912 3292 3292 3292 3292 3292 3292 3292 3	Euclid*N 12.80% 12.12% 12.12% 14.73% 15.11% 19.01% 18.46% 17.73% 17.07% 13.94% 16.46% 11.50% 17.43% 11.48%	Clean-Bingc 388313 40789 38277 38277 38277 48873 38458 17166 12904 1291 21937 38912 21937 31986 31997 39007 43277	8-NGC 37198 440011 30777 28009050 42107 350022 16817 27898 28880 28880 37420 42176 42176 42176 42176 42176 42176 42176 400001 37198 5800000000000000000000000000000000000	Euclid% 4.21% 1.98% 1.98% 3.99% 1.3.84% 3.99% 1.4.45% 3.24% 4.72% 2.88% 6.29% 4.27% 4.07% 2.54% 4.07% 2.54% 4.07% 2.54% 4.07% 2.54% 4.07% 2.54% 4.07% 2.54%	Clean-Bgc 38021 40006 38021 40006 32163 307856 46003 36887 17165 418257 21583 38912 31885 39105 43004	8-9C 33108 35482 29939 27985 41298 32542 15076 32697 24997 17992 34004 28356 44767 36431 35996 37881	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.173 13.485 12.615 17.345 18.065 7.995 11.915	Covariance 0.08 0.07 0.09 0.09 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.09 0.09 0.07 0.08 0.09 0.09 0.09 0.09
com.brave.browser com.aniplex.falegrandorder org.mczilla.fenix com.appstalkimg.photoeditor de vsmedial.imagesize com.vid097.videobuddy com.redbox.tv com.essersenrecorder com.mg3.editor.music.cut.ringtone com.snenstri.gilite com.anonymoustexting com.snesplus.app co.kitetoch.messenger com.neo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.nemo.vidmate com.gihoo.appstore	Browser Browser Browser Browser Browser Browser Browser Browser Edding Edding Edding Edding Entertainment Entertainment Seming Sms Sms Sms Social Media Vault Malware Malware	Clean-Fngc 39158 41628 39158 41628 35197 30158 48510 37603 3	F-NGC 390022 40398 30007 40398 30007 40008 30008 17082 40075 28103 21686 38865 53281 42861 42861 43834 44399	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 4.45% 0.60% 0.43% 0.12% 0.34% 0.12% 0.34% 1.05% 0.28% 0.28% 0.43% 0.10%	Clean=Fgc 38162 40864 40864 35481 305191 48529 37052 17167 41134 21322 38654 31807 52967 43199 443199	F-GC 33341 35912 3341 35912 35	Euclid*N 12.80% 12.12% 12.12% 14.85% 14.73% 15.11% 19.01% 18.46% 12.77% 13.84% 10.20% 11.50% 11.46% 11.46%	Clean-Bingc 3883134 40789 4078	B-NGC 37199 40001 37199 40001 37199 42107 35002 16917 39867 20034 37798 29880 50832 39005 39005 42176 43227 24061	Euclid% 4.21% 1.98% 1.98% 1.98% 1.98% 1.384% 1.384% 1.384% 1.384% 1.384% 1.384% 1.24	Clean-Bgc 38021 4006 38021 4006 32163 30785 46003 36897 17165 41225 21583 38912 31885 53001 43004 44183	B-GC 33108 35482 26939 27985 41298 32542 15076 35667 17992 34004 26935 47667 37681 39681 39681	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.173 13.485 12.615 16.645 12.615 17.345 18.065 11.915	Covariance 0.08 0.07 0.09 0.08 0.09 0.09 0.07 0.08 0.08 0.09 0.00 0.09 0.00 0.00 0.00
com.brave.browser com.aniplex.falegrandorder org.mczilla.fenix com.appstalking.photoeditor de vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.essereenrecorder com.mp3.editor.music.cut.ringtone com.tenigilite com.anonymoustexting com.smsplus.app co.kitetoch.messenger com.neeo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.nemo.vidmate com.qihoo.appstore com.wBestFreeGameCheatCodesGlitches	Browser Browser Browser Browser Edding Edding Edding Entertainment Entertainment Entertainment Sms Sms Sms Social Modia Vault Malware Malware Malware	Clean-Fngc 39158 41629 31978 31978 31979 31979 31979 48101 337603 17888 41332 21761 38610 31876 53844 43997 43565 44472 27881	F-NGC 39002 40988 35088 35088 35088 45089 450800000000000000000000000000000000000	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.48% 0.88% 0.12% 0.12% 0.34% 1.05% 3.04% 2.25% 0.88% 0.16% 4.27%	Clean=fgc 38162 40864 35481 306191 46529 37052 17167 41134 21322 38654 31807 52867 42980 38994 44321 26980	F-GC 33241 35912 32200 32200 32200 32200 32200 32200 32200 32200 3220 3	Euclid*N 12.80% 12.12% 14.88% 14.73% 15.11% 19.01% 18.46% 12.77% 13.94% 16.46% 10.20% 11.50% 11.47% 11.07%	Clean-Bingc 388313 407998 38217 30207 48873 39458 17166 41221 21323 38912 31885 53983 43007 43277 44188	B-NGC 37198 40001 37198 40001 37198 42107 35002 16817 39887 29880 50832 39005 39005 42176 43227 24081	Euclid*% 4.21% 1.98% 1.98% 3.99% 13.84% 3.99% 14.44% 3.24% 4.72% 2.88% 4.72% 2.88% 4.27% 4.27% 1.2.87%	Clean-Bgc 38021 4006 32163 321	8-9C 33108 35482 28939 278855 41288 32542 15076 35667 17982 34004 28356 47667 36431 36986 378818 39881 22780	Euclid% 12.925 11.313 16.245 9.365 13.975 11.885 12.173 13.485 12.173 13.485 12.615 16.648 12.615 17.345 18.965 16.455 17.955 11.915	Covariance 0.08 0.07 0.011 0.06 0.08 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.00 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de vsmedia.imsgesize com.vid007.videobuddy com.redbox.tv com.ezscreenrecorder com.mp3.editor.music.cut.ringtone com.tencent.igilite com.anonymousaxting com.snsphus.app co.kitetoch.messenger.ui gallery.hidepictures.photovault.lockgallery com.nemo.vidmate com.gihoa.appstore com.wBestFreeGameCheatCodesGiltches com.ss.android.article.news	Browser Browser Browser Browser Editing Editing Editing Editing Entertainment Entertainment Sms Sms Sms Sms Social Modia Vault Malware Malware Malware Malware	Clean-Fngc 39158 41629 35197 30189 485101 37603 17889 41512 28667 28667 38706 34876 34876 34876 44472 27881	F-NGC 39002 40988 35088 35088 49088 17092 40975 28103 28103 28103 2928 4288 4288 4288 44389 26880 55121	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.48% 0.88% 0.43% 0.12% 0.24% 0.25% 0.88% 0.16% 4.25% 0.88% 0.16% 4.27%	Clean Fgc 38162 40864 4084 4084 4084 4084 4084 4084 408	F-GC 33241 36912 32200 32200 32200 32200 32200 32200 32200 32200 3220 3	Euclid*N 12.50% 12.12% 14.86% 14.73% 15.11% 19.01% 18.46% 12.77% 17.07% 13.94% 16.46% 10.20% 11.50% 17.43% 11.07% 8.76%	Clean-Bingc 388313 40789 38277 30201 48873 304585 17166 29040 21328 38912 31885 43007 39007 44182 24944 41883 41885 42944 41883 4277 44188	8-NGC 371989 440001 440001 47198 471	Euclid% 4.21% 1.98% 1.98% 3.95% 3.95% 3.95% 3.95% 3.95% 3.95% 3.95% 4.72% 4.72% 4.72% 4.72% 4.72% 4.72% 4.72% 4.75	Clean-Bgc 38021 40006 32163 40006 32163 307655 48003 307655 48003 307655 41225 26867 218667 31865 53001 43603 36105 43004 44183 27034 49388	8-9C 33108 35482 28939 278855 41288 41288 32542 15078 35687 24997 34004 26356 47667 36431 35986 39881 39881 22760 42752	Euclid% 12,925 11,315 16,248 9,365 13,975 11,885 12,175 13,485 13,415 16,645 12,613 17,345 19,975 11,915 19,745 15,815	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.07 0.01 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.asscreenrecorder com.mp3.editor.music.cut.ringtone com.tencent.igilite com.anonymoustexting com.anonymoustexting com.sespec.ui gallery.hidepictures.photovault.lockgallery com.neeo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.neeo.vidmate com.neeo.vidmate com.meeo.vidmate com.meeo.vidmate com.meeo.vidmate com.meeo.vidmate com.meeo.vidmate com.meeo.vidmate com.neo.apscree com.westFreeGameCheatCodesGiltches com.s.s.android.article.news com.namad.instafollov	Browser Browser Browser Browser Editing Editing Editing Editing Entertainment Entertainment Saming Sms Sms Sms Social Modia Vault Malware Malware Malware Malware Malware	Clean-Fnpc 39159 41628 319159 319159 319159 319159 319159 48610 376030 17688 413322 28867 217611 386101 31876 3497 39870 43556 44472 2786811 561336	F-NGC 39002 40398 35098 35098 35098 35098 360980	Euclid% 0.40% 1.52% 0.28% 0.28% 0.60% 1.84% 1.61% 4.49% 0.08% 0.12% 0.43% 0.12% 0.34% 0.12% 0.34% 2.25% 0.86% 0.16% 4.27% 0.03% 4.27% 0.03% 0.27%	Clean-Fgc 38162 40864 354841 30619 48529 37052 17167 41134 28886 21322 38654 31807 42980 38994 43199 44321 28886 256002 28661	F-GC 33341 35912 3	Euclid® 12.80% 12.80% 12.80% 14.88% 14.88% 14.73% 15.11% 19.01% 18.01% 17.73% 17.07% 13.94% 10.20% 17.43% 11.45% 12.77% 17.43% 11.45% 12.77% 17.77% 1	Clean-Bingc 388313 40789 38277 30201 48873 304585 17166 29040 21328 38912 31885 43007 39007 44182 24944 41883 41885 42944 41883 4277 44188	8-NGC 37198 440011 30777 280090 280000 280090 280090 280090 280090 280090 280090 280090 280090 280000000000	Euclid% 4.21% 1.98% 7.385% 3.99% 13.845% 3.99% 1.445% 3.245% 4.725% 2.285% 6.299% 4.07% 2.545% 2.175% 10.805% 2.555% 1.1805% 1.805% 1.805%	Clean-Bgc 38021 4006 4006 32183 30785 48003 38897 17165 412867 21583 38912 31885 43004 44183 43004 44183 270344 49388	B-GC 33108 35482 26939 27885 41288 32542 15076 32697 17992 34004 26366 37881 35986 37881 39881 227865 42752 23986	Euclid% 12.925 11.315 16.248 9.365 13.975 11.885 12.175 13.485 13.485 12.615 17.345 12.615 17.955 11.915 9.745 15.815 17.245 17.965	Covariance 0.08 0.07 0.11 0.06 0.08 0.09 0.07 0.01 0.08 0.09 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08
com.brave.browser com.aniplex.falegrandorder org.mozilla.fenix com.appstalia.jnptotoeditor de.vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.essersenrecorder com.mp3.celitor.music.cut.ringtone com.mp3.celitor.music.cut.ringtone com.securit.jilite com.anonymoustaxting com.smpus.app co.kitetoh.messenger com.seo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.nemo.vidmate com.qino.appstore com.wBestFreeGameCheatCodesGiitches com.se.android.article.news com.namad.instafollow com.android.securit.zdevs.bah	Browser Browse	Clean-Fngc 39158 41628 39158 41628 30158 48610 37603 17888 48610 31876 21761 38610 31876 43526 44472 27881 561535 26762 33267	F-NGC 39002 40398 35098 35098 40098 40008 36998 40008 36998 40075 281033 21988 38865 31766 53281 42881 42881 42881 42881 4399 26890 26890 33198 40988 40988	Euclid% 0.40% 1.52% 0.28% 0.28% 0.60% 1.84% 4.45% 0.86% 0.12% 0.43% 0.12% 0.34% 1.05% 0.86% 0.16% 2.25% 0.86% 0.16% 2.25% 0.86% 0.16% 2.25% 0.26% 0.27% 0.27%	Clean=Fgc 38162 40864 40864 30619 46529 37052 17167 41184 28865 21322 38664 31807 42880 38994 43199 44321 26980 269661 33192 266661	F-GC 33341 35912 3	Euclid*N 12.80% 12.12% 12.12% 14.73% 15.11% 19.01% 18.46% 17.77% 13.94% 16.46% 17.45% 11.46% 12.17% 11.07% 11.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07% 17.07%	Clean-Bingc 388313 40789 382717 30201 48873 30458 17166 29040 21326 21326 38912 29040 44188 43007 44227 44188 20997 44198 20997 43277 44188	8-NGC 37198 40001 30777 28009020 42107 350022 16817 2789802 20834 37798 288802 42176 43227 24081 48181 48181 281818 38069 38109	Euclid% 4.21% 1.98% 7.385% 3.99% 13.845% 3.99% 1.445% 3.245% 4.725% 2.285% 6.299% 4.07% 2.545% 2.175% 10.805% 2.555% 1.1805% 1.805% 1.805%	Clean-Bgc 38021 40006 38021 40006 32183 30785 48003 36897 17165 41225 28867 21583 38912 31885 49033 39105 43004 44183 27034 49388 26685 33215	B-GC 33108 35482 27885 41288 32542 15076 24987 17992 34004 28356 37881 39988 22780 22780 22780 22780 22780 22780	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.173 13.485 12.173 13.485 12.615 17.345 18.065 16.455 7.935 11.915 9.745 15.815 17.245 17.065 17.245	Covariance 0.08 0.07 0.01 0.06 0.08 0.09 0.09 0.07 0.07 0.08 0.09 0.09 0.07 0.08 0.09 0.09 0.09 0.09 0.07 0.08 0.09 0.09 0.09 0.09 0.09 0.09 0.09
com.brave.browser com.aniplex.falegrandorder org.mczilla.fenix com.apstalking.photoeditor de vsmedia.imagesize com.vid097.videobuddy com.redbox.tv com.esscreenrecorder com.mp3.editor.music.cut.ringtone com.tenigilite com.anonymoustexting com.smsplus.app co.kitetoch.messanger com.neoc.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.memo.vidmate com.glhoo.appstore com.wBestFreeGameCheatCodesGittches com.s.android.article.news com.android.article.news com.android.article.news com.android.article.news com.android.stenont.zdevs.bah ru.delivery.collapse com.isyjv.ktzblinwc.r	Browser Browse	Clean-Fngc 39158 41629 39158 41629 30188 48910 37603 17888 41532 21767 21767 38610 31876 53844 43997 43565 44472 27881 56136 22762 332676 41880 25990	F-NGC 39002 40388 30007 40388 30007 40388 30007 40308 40308 17082 40375 21088 38865 31769 53281 42861 38974 43183 44399 26890 55121 20006 33186 40398 40398 25079	Euclid% 0.40% 1.52% 0.28% 0.60% 1.84% 1.61% 4.49% 0.88% 0.10% 0.12% 0.34% 0.12% 0.34% 0.12% 0.34% 0.10% 0.09% 0.25% 0.09% 0.10% 0.25%	Clean=Fgc 38162 40864 40864 35481 305191 48529 37052 17167 41134 28886 21322 38654 31807 52967 429800 38994 43199 44321 26880 28866 33192 44021	F-GC 33341 35912 3341 35912 35	Euclid*N 12.80% 12.12% 12.12% 12.12% 14.73% 15.11% 19.01% 18.46% 12.77% 13.84% 10.20% 11.60% 12.17% 11.60% 12.17% 11.67% 11.67% 11.751%	Clean-Bingc 38833 40799 38873 32217 32202 48873 36458 17166 21232 38812 31885 53983 43007 43077 44188 209977 44188 22997 43988 42005	8-NGC 37198 40001 37198 42107 35002 16817 39867 20539 20534 37798 29880 50832 39005 37420 4217 24081 48131 328689 38109 22567	Euclid% 4.21% 1.98% 1.98% 3.98% 13.84% 3.99% 1.44% 3.24% 4.72% 3.71% 2.88% 6.28% 4.24% 4.07% 2.55% 10.89% 2.17% 10.89% 2.55% 1.89% 2.25% 1.89% 1.25% 2.27%	Clean-Bgc 38021 40006 38021 40006 32163 307856 48003 36897 17165 41225 28687 21583 38912 31885 53001 44004 44183 27044 44183 27044 44183 27044 44183	B-GC 33108 35482 29939 27938 41298 32542 15076 35667 34004 29356 47067 37881 39981 22780 22780 22780 22780 22780 36620 27549 36620 27549 36620 27549 36620	Euclid% 12.925 11.315 12.925 9.365 9.365 13.975 11.885 12.173 13.485 12.173 13.485 12.615 17.345 12.615 17.345 18.065 11.915 9.745 11.915 12.415 12.425 17.085 17.085 17.085 17.085 17.085 17.085 17.085 17.085 17.085	Covariance 0.88 0.07 0.11 0.066 0.08 0.09 0.09 0.07 0.08 0.11 0.08 0.09 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08
com.brave.browser com.aniplex.falegrandorder org.mczilla.fenix com.appstalking.photoeditor de vsmedia.imagesize com.vid007.videobuddy com.redbox.tv com.essersenrecorder com.mg3.editor.music.cut.ringtone com.snentt.igilite com.anonymoustexting com.snsplus.app co.kitetoch.messenger com.neo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.nemo.vidmate com.qihoo.appstore com.westFreeGameCheatCodesGiltches com.snandroid.article.news com.nandroid.nitelollow com.android.instafollow com.android.stencent.zdevs.bah nu.deilvery.collapse	Browser Browser Browser Browser Edding Edding Edding Edding Entertainment Entertainment Sms Sms Sms Social Media Vault Malware	Clean-Fngc 39158 41628 39158 41628 35197 301898 48510 37603 31760	F-NGC 39012 40988 30012 40988 30012 40988 30017 48018 30017 48018 30017 48018 30017	Euclid% 0.40% 1.52% 0.60% 1.84% 1.61% 4.46% 2.99% 0.43% 0.12% 0.34% 1.05% 3.04% 2.25% 0.88% 0.08% 0.25% 0.2	Clean=fgc	F-GC 33241 35912 35241 35912 35241 35912 35241 35912 35241 35912 35241 3	Euclid*N 12.80% 12.12% 12.12% 14.85% 14.73% 15.11% 19.01% 18.46% 12.77% 13.84% 16.46% 10.20% 11.60% 11.47% 11.67% 12.17% 11.07% 17.75% 11.47% 11.75% 11.41%	Clean-Bingc 388313 40789 388217 38227 48873 394588 17166 41221 294040 213262 38912 294040 43207 44188 20997 44289 29997 44188 29997 442099	8-NGC 37198 40017 28009 42107 35002 16817 39808 20634 37798 20634 37798 24080 58032 39005 42176 42176 48131 26648 38109 28567 38109	Euclid*% 4.21% 1.98% 7.95% 3.95% 3.95% 13.84% 3.99% 14.45% 3.24% 4.72% 3.71% 2.86% 4.24% 9.31% 4.07% 2.54% 1.18% 2.55% 1.18% 9.28% 7.77% 3.52%	Clean-Bgc 38021 4006 38021 4006 32163 32763 4603 36897 17165 41225 21583 38912 31885 53001 43603 39105 4304 44183 27044 49388 49388 43215 41785	B-GC 33108 35482 26938 27985 2	Euclid% 12.928 11.315 16.248 9.365 13.978 11.885 12.178 13.448 13.415 16.648 12.613 19.935 11.935 16.748 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 17.948 19.948	Covariance 0.08 0.07 0.011 0.06 0.08 0.09 0.09 0.07 0.011 0.08 0.07
com.brave.browser com.aniplex.fategrandorder org.mozilla.fenix com.appstalking.photoeditor de vsmedia.imsgesize com.vid007.videobuddy com.redbox.tv com.exscreenrecorder com.mos.acitor.music.cut.ringtone com.tencent.igilite com.anonymousaxting com.snsphus.app co.kitetoch.messenger.ui gallery.hidepictures.photovault.lockgallery com.nemo.vidmate com.gihoo.appstore com.wBestFreeGameCheatCodesGilitches com.sa.android.article.news com.amad.instafollow com.android.tencent.zdevs.bah nu.delivery.collapse com.isyix.kbilmwc.r org.doviz.cevir operatore.italia	Browser Browser Browser Browser Browser Editing Editing Editing Editing Editing Entertainment Entertainment Saming Sms Sms Sms Sms Sms Social Modia Vault Malware	Clean-Fnpc 391589 41628 36197 301889 48610 376030 17868 48610 376030 17868 413322 28867 21761 38610 31876 34670 34670 327601 34670 3	F-NGC 39012 40988 30012 40988 30018 40018 30018	Euclid% 0.40% 1.52% 0.26% 0.86% 1.84% 1.61% 4.46% 0.89% 0.43% 0.12% 0.43% 0.12% 0.25% 0.88% 0.16% 2.25% 0.88% 0.16% 2.25% 0.27% 0.23% 2.25% 0.27% 0.23% 0.27% 0.23% 0.27% 0.23% 0.27% 0.23% 0.21% 0.23% 0.21% 0.23% 0.22% 0.23% 0.25% 0.2	Clean-Fgc 38162 40844 40844 30619 48529 37052 17167 41134 28866 21322 38654 31807 42980 38994 43199 44321 26980 55002 28661 33192 41021 42265	F-GC 33241 35912 35912 26108 41198 30008 13988 23881 17682 33265 26573 34218 38241 38926 23799 35201 23799 35201	Euclid® 12.80% 12.80% 12.80% 14.88% 14.88% 14.78% 15.11% 19.01% 18.01% 17.73% 17.07% 13.94% 14.00% 17.43% 14.45% 12.77% 17.51% 18.79% 17.07% 17.51% 18.79% 17.07% 17.51% 18.79% 17.07% 17.51% 18.79% 17.07% 17.51% 14.15% 17.07% 17.51% 14.15% 17.07% 17.51% 14.15% 17.07% 17.51% 14.15% 17.07% 17.51% 14.15% 17.07% 17.51% 14.15% 17.07% 17.51% 14.15% 17.07% 17.51% 17.07% 17.51% 17.07% 17.51% 17.07% 17.51% 17.07% 17.51% 17.07% 17.51% 17.07% 17.51% 17.07% 17.51% 17.07% 17.51% 17.07% 17.51% 17.00% 1	Clean-Bingc 388313 40789 38277 30201 48873 30267 48873 304585 17766 29040 21328 38912 31885 43007 39007 44188 22901 42000 43327 44188 42000 433287 42000 41078 41078	8-NGC 371989 40001 307777 280090 42107 350020 18917 278999 20534 377999 280802 38005 37420 42176 43227 240011 48131 28648 326999 381099 225674 38452	Euclid% 4.21% 1.98% 1.98% 1.98% 1.3.84% 1.3.84% 1.3.84% 1.3.84% 1.2.85% 1.2.85% 1.2.85% 1.2.85% 1.2.85% 1.2.85% 1.2.85% 1.3.85	Clean-Bgc 38021 4006 4008 3183 30785 48003 30785 48003 30887 17165 41267 21583 38812 31885 43004 44183 2004 44183 2204 43988 28995 33215 41785 417865 41988	B-GC 33108 35482 26983 27885 41288 32542 15076 32697 17992 34004 26356 37881 35986 37881 39881 27865 42752 23986 27549 36629 2276 35489 36983	Euclid% 12,925 11,315 16,248 9,365 13,975 11,885 12,175 13,485 13,415 16,645 12,613 17,345 19,915 19,745 11,918 17,745 17,065 11,918 17,245 17,065 12,415 17,245 17,245 17,245 19,193 19,193 11,193 11,193 11,193 11,193 11,193 11,193 11,193 11,193 11,193	Covariance 0.08 0.07 0.06 0.08 0.09 0.09 0.07 0.07 0.08 0.09 0.07 0.08 0.08
com.brave.browser com.aniplex.falegrandorder org.mozilla.fenix com.appstalking.photoeditor de.vsmedia.magesize com.vid007.videobuddy com.redbox.tv com.esscreenrecorder com.mp3.edim.music.cut.ringtone com.men.cent.igilite com.anonymoustexting com.sns.plus.app co.kitetech.messenger com.neoc.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.men.ovidmate com.gihoo.appstore com.w8estFreeGameCheatCodesGiltches com.sand.instafollow com.android.stencent.zdevs.bah ru.deilvery.collapse com.isyly.khbbinwc.r org.doviz.cevir org.edoviz.cevir	Browser Browse	Clean-Fnpc 39158 41628 31959 31959 31959 31959 31959 48610 37603 17889 41369 21761 38610 31876 38670 413569 43579 33677 41880 4377 41880 43877 41880	F-NGC 39012 40398 350398 350398 350398 17092 48008 17092 21666 38865 31766 38865 31786 42861 42861 38374 43183 44399 55121 22006 33196 40388 40388	Euclid% 0.40% 1.52% 0.28% 0.28% 0.26% 1.84% 1.61% 4.46% 0.29% 0.43% 0.12% 0.34% 0.12% 0.34% 0.16% 0.25% 0.26% 0.16% 0.27% 0.27% 0.27% 0.21% 0.27% 0.21% 0.25% 0.26% 0.27%	Clean-Fgc 38162 40864 40864 30619 48529 37052 17167 41184 28886 21322 38654 31807 42880 38994 43199 4321 28661 33192 41021 25321 41021	F-GC 33241 36912 36912 36912 36903 26108 41198 30008 15988 26882 23881 17682 33265 26673 34218 38241 38020 23992 50165 23769 27379 35201 20438 377191 36791	Euclid® 12.80% 12.80% 12.80% 12.80% 12.80% 14.73% 15.11% 19.01% 15.11% 19.01% 17.07% 17.07% 13.84% 16.46% 12.17% 17.07% 1	Clean-Bingc 38833 40786 38873 32020 48873 32020 48873 36458 17166 29040 21325 38912 23452 38912 24325 38912 24325 38912 24325 38912 24325 38912 24325 43007 43277 44188 22990 42006 42006 41078 41078 41078	8-NGC 37198 40001 30777 28009030 42107 350022 18977 27899 28880 28880 37798 28880 37420 42176 43227 42181 28648 32669 381090 381090 22567 389754 384652 28003	Euclid% 4.21% 1.98% 7.36% 3.99% 13.84% 3.99% 1.44% 3.24% 4.72% 2.68% 6.29% 4.07% 2.54% 2.17% 1.18% 1.80% 9.29% 7.77% 3.52% 6.39% 6.39% 6.39% 6.39% 6.39% 6.39% 6.39%	Clean-Bgc 38021 4008 38021 4008 32183 30785 48003 36897 17165 412857 21583 38912 31885 43004 44183 22695 43024 44183 49083 41785 25083 406966 41198	B-GC 33108 35482 35482 27885 41288 32542 15076 32697 17992 34004 23356 37881 39881 39881 22780 42752 23986 27548 36628 20270 354999 36083	Euclid% 12.925 11.315 16.248 9.365 13.975 11.885 12.175 12.175 13.485 12.615 16.645 12.615 17.345 12.955 11.915 9.745 11.915 12.425 12.345 12.345 12.425 12.345 12.345 12.345	Covariance 0.08 0.07 0.08 0.09 0.09 0.09 0.09 0.07 0.07 0.08 0.09 0.09 0.09 0.09 0.09 0.09 0.09
com.brave.browser com.aniplex.falegrandorder org.mczilla.fenix com.appstalking.photoeditor dev.smedia.imagesize com.vid007.videobuddy com.redbox.tv com.essersenrecorder com.mga.editor.music.cut.ringtone com.sms.plus.app co.kitetoch.messenger com.neo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.neo.vidmate com.qihoo.appstore com.westerreGameCheatCodesGiitches com.smand.instafollow com.namad.instafollow com.namd.instafollow com.android.tencent.zdevs.bah ru.deilvery.collapse com.siyk.kiblinwc.r org.doviz.cevir org.doviz.cevir	Browser Browse	Clean-Fngc 39158 41628 39158 41628 39158 48610 37603 30188 48610 37603 30188 48610 37603 30188 3018 3018 3018 3018 3018 3018 3	F-NGC 39002 40388 35088 35078 48008 36988 17082 21688 38865 31786 53281 43883 44389 26980 33186 426881 426881 426881 426881 426881 426881 426881 426881 426881 426881 426881	Euclid% 0.40% 1.52% 0.80% 0.80% 1.84% 4.45% 0.86% 0.16% 0.43% 0.12% 0.34% 1.05% 0.86% 0.18% 2.25% 0.86% 0.18% 4.27% 0.35% 0.25% 0.27% 2.11% 3.51% 2.24% 2.24% 2.24%	Clean=Fgc 38162 40864 40864 30819 46529 37052 17167 41134 28886 21322 38654 31807 52967 42980 38994 43193 44321 26960 33192 41021 25221 25221 25221 25221 25221	F-GC 33241 35912 3241 35912 3241 35912 3241 3241 3241 3241 3241 3241 3241 32	Euclid*N 12.80% 12.12% 12.12% 12.12% 14.73% 15.11% 19.01% 18.46% 17.73% 17.07% 13.84% 10.20% 11.48% 12.17% 11.07% 8.76% 17.25%	Clean-Bingc 388313 40789 388314 40789 38207 38207 48873 38458 17166 29345 21325 38912 21325 38912 22945 43207 44188 22997 44286 22997 44205 22945 22945 22945	8-NGC 37198 40001 30777 28009020 42107 350022 16817 2769802 20534 37798 288802 42176 43227 24081 48131 28131 48131 380699 22567 38109 22567 38109 22567	Euclid% 4.21% 1.98% 1.98% 1.98% 1.384	Clean-Bgc 38021 40006 38021 40008 32163 32763 46003 36897 17165 41225 28667 21563 38912 31885 53001 43004 44183 27094 41185 26095 33215 41785 25093 41188	B-GC 33108 35482 39936 27985 41298 32542 15076 36677 24997 17992 34004 28355 47667 35981 39981 22780 27862 27962 20270 36489 36088 36088 36088	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.173 11.885 12.173 13.445 16.645 12.615 17.345 18.955 11.915 9.745 11.915 17.465 17.965	Covariance 0.08 0.07 0.06 0.08 0.09 0.09 0.07 0.08 0.01 0.06 0.07 0.08 0.08
com.brave.browser com.aniplex.falegrandorder org.mczilla.fenix com.apstalking.photoeditor de v.smedia.imagesize com.vid907.videobuddy com.redbox.tv com.esscreenrecorder com.mp3.editor.music.cut.ringtone com.tencent.igilite com.anonymoustexting com.smsplus.app cow.kitectch.messenger com.neo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.smsplus.app cow.memo.vidmate com.glnoo.appstore com.wBestFreeGameCheatCodesGiltches com.s.android.article.news com.android.stencent.zdevs.bah ru.deilvery.collapse com.isyiv.kbblinwc.r org.doviz.cevir operatore.italia com.maraon.mShop.android.shopping.ha- com.androiddoctor.battery	Browser Browser Browser Browser Browser Edding Edding Edding Edding Entertainment Entertainment Sms Sms Sms Social Media Vault Malware	Clean-Fngc 39158 41628 39158 41628 30198 48510 37603 17688 41532 21761 38610 31676 53844 4352 27681 4472 27681 56135 25990 43871 41880 25990 43871 218762	F-NGC 39002 40388 30007 40088 30007 40088 17082 40975 28103 21688 38865 31766 53281 43881 44389 26880 55121 40988 25076 42889 42886 225046 2250	Euclid% 0.40% 1.52% 0.28% 0.28% 0.60% 1.84% 1.61% 4.45% 0.08% 0.43% 0.12% 0.34% 0.12% 0.34% 1.05% 0.28% 0.28% 0.22% 2.21% 0.351% 0.22% 1.11% 3.51% 2.24% 1.22% 0.27% 0.21% 0.27% 0.21% 0.27% 0.21% 0.27% 0.21% 0.	Clean=Fgc 38162 40864 35481 305191 46529 37052 17167 41134 21322 38654 31807 52967 43199 44321 26980 38994 43199 44321 26980 550661 33192 41021 25321 42765 29318 19662	F-GC 33241 35912 33241 35912 33241 35912 32008 41198 30008 3008 3008 3008 3008 3008 3008 3	Euclid*N 12.80% 12.12% 12.12% 14.85% 14.73% 15.11% 19.01% 18.46% 12.77% 13.84% 10.20% 11.50% 11.50% 11.50% 11.48% 12.17% 11.07%	Clean-Bingc 38833 40799 38837 38277 38277 448873 38458 38912 29040 21326 38912 29040 43277 44188 29999 43277 44188 29999 43277 44188 29999 43277 44192 29040 29050 33267 42005 29050 33267 42005 29050 33267 42005 29050 33267 42005	8-NGC 37198 40001 40001 37198 42107 35002 16817 39867 20939 20534 37798 20809 20534 42176 43227 24081 48131 28959 38109 22567 39874 3269 38109 22567	Euclid*% 4.21% 1.98% 1.98% 3.98% 13.84% 3.99% 1.44% 3.24% 4.72% 3.71% 2.88% 6.28% 4.24% 9.21% 1.089% 2.54% 1.18% 1.18% 1.25% 9.28% 7.77% 3.52% 6.29% 3.52% 6.29% 3.22%	Clean-Bgc 38021 4006 38021 4006 32163 32765 48003 36897 17165 41225 21583 38912 31885 53001 44183 27044 44183 27044 44183 45966 33315 41785 25083 40966 42877 21683	B-GC 33108 35482 27885 41298 32542 15076 36697 17992 34004 26355 47687 39881 22780 22780 22780 22780 20270 35489 20276 35489 20276 35489 20276 36489 20276	Euclid% 12.925 11.315 16.245 9.365 13.975 11.885 12.173 13.485 12.618 13.445 14.618 15.618 13.445 17.245 17	Covariance 0.08 0.07 0.08 0.09 0.09 0.07 0.01 0.08 0.07 0.08 0.01 0.07 0.08 0.08
com.brave.browser com.aniplex.falegrandorder org.mczilla.fenix com.appstalking.photoeditor dev.smedia.imagesize com.vid007.videobuddy com.redbox.tv com.essersenrecorder com.mga.editor.music.cut.ringtone com.sms.plus.app co.kitetoch.messenger com.neo.chatmessenger.ui gallery.hidepictures.photovault.lockgallery com.neo.vidmate com.qihoo.appstore com.westerreGameCheatCodesGiitches com.smand.instafollow com.namad.instafollow com.namd.instafollow com.android.tencent.zdevs.bah ru.deilvery.collapse com.siyk.kiblinwc.r org.doviz.cevir org.doviz.cevir	Browser Browse	Clean-Fngc 39158 41628 39158 41628 39158 48610 37603 30188 48610 37603 30188 48610 37603 30188 3018 3018 3018 3018 3018 3018 3	F-NGC 39012 40988 30008 30008 30088 30008 17082 28103 21688 38865 38874 43183 42861 28006 33188 42899 41006 42899 41006 25549 219166 197782	Euclid% 0.40% 1.52% 0.60% 1.84% 0.60% 1.84% 4.46% 4.46% 0.88% 0.43% 0.12% 0.34% 1.05% 3.04% 2.25% 0.88% 0.25% 0.88% 0.25% 0.25% 0.88% 0.18% 1.19% 1.25% 1.19% 1.25% 1.19% 1.25% 1.2	Clean=Fgc 38162 40864 40864 30819 46529 37052 17167 41134 28886 21322 38654 31807 52967 42980 38994 43193 44321 26960 33192 41021 25221 25221 25221 25221 25221	F-GC 33241 35912 3241 35912 3241 35912 3241 3241 3241 3241 3241 3241 3241 32	Euclid*N 12.80% 12.12% 12.12% 12.12% 14.73% 15.11% 19.01% 18.46% 17.73% 17.07% 13.84% 10.20% 11.48% 12.17% 11.07% 8.76% 17.25%	Clean-Bingc 388313 40789 388314 40789 38207 38207 48873 38458 17166 29345 21325 38912 21325 38912 22945 43207 44188 22997 44286 22997 44205 22945 22945 22945	8-NGC 371989 40017 28009 42107 35002 18817 39808 20534 37798 20634 37798 20800 37420 42176 48131 28648 38269 38269 22567 39874 39452 28003 218999	Euclid*% 4.21% 1.98% 7.98% 3.99% 13.84% 3.99% 14.45% 3.24% 4.72% 3.71% 2.88% 4.27% 4.27% 5.25% 1.18% 1.25% 1.18% 1.26% 1.26% 1.26% 1.26% 1.27% 1.28% 1	Clean-Bgc 38021 40006 38021 40008 32163 32763 46003 36897 17165 41225 28667 21563 38912 31885 53001 43004 44183 27094 41185 26095 33215 41785 25093 41188	B-GC 33108 35482 39936 27985 41298 32542 15076 36677 24997 17992 34004 28355 47667 35981 39981 22780 27862 27962 20270 36489 36088 36088 36088	Euclid% 12,928 11,315 16,248 9,365 13,978 11,885 12,178 13,448 13,415 16,648 12,615 11,918 12,928 11,918 12,928 11,918 12,928 11,918 12,928 11,918 12,428 13,438	Covariance 0.08 0.07 0.08 0.09 0.09 0.09 0.07 0.08 0.09 0.09 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.08 0.07 0.01 0.01 0.01 0.01 0.01 0.01 0.01

Figure 4: Evaluation Result

4.1 Recovery Consistency and Data Loss

On analysis, we identified that the results in Figure 5 reveal that we retrieved more non-Gui objects (Class name, text, etc.) in case of benign (apps selected from each category) and malicious applications than Gui and network objects. When we compared the count of Gui objects recovered from dumps with GC triggered and dumps with No-GC triggered, we identified that in the Foreground process dumps, the Editing, Entertainment, and SMS apps had an average of 19% reduction while the malware apps had an average of 24% reduction. When we compared the Gui object count for B-NGC and B-GC, in the case of Editing, Entertainment and SMS, and Malware apps, the reduction in object recovered was 19% !9.5%, 24.5%, and 21%, respectively. When we compared the count of Non-Gui objects recovered from dumps with GC triggered and dumps with No-GC triggered, we identified that in the Foreground process dumps, the Editing, Entertainment, and SMS apps had an average of 20% reduction. In comparison, the malware apps had an average of 22% reduction. When we compared the Gui object count

for B-NGC and B-GC, in the case of Editing, Entertainment and SMS, and Malware apps, the reduction in object recovery count was 20%.

Similarly, the reduction in Network objects recovered ranges between 18% to 23% in all the apps studied in this research. The histograms in Figure 6 include component-based recovery from a few apps selected from each app category. Figure 6 depicts that we retrieved more Android Services than Android activity components and resource files on plotting apps from each category like editing, malware, SMS, entertainment.

Acquisition Mode	Package Name	Package type	Large	Gui	Non-Gui	Network
	com.appstalking.photoeditor	Editing	18	1728	24721	205
	de.vsmedia.imagesize	Editing	16	2552	38119	429
	com.redbox.tv	Entertainment	10	1273	11883	128
	com.ezscreenrecorder	Entertainment	28	2181	30449	398
	com.anonymoustexting	SMS	14	2003	28771	361
	com.smsplus.app	SMS	17	1549	21553	318
	com.androiddoctor.battery	Malware	10	1161	10001	102
F-NGC	com.maxauto.maxiplusap	Malware	8	1004	9883	111
Acquisition Mode	Package Name	Package type	Large	Gui	Non-Gui	Network
	com.appstalking.photoeditor	Editing	16	1400	15281	134
	de.vsmedia.imagesize	Editing	14	1994	31108	317
	com.redbox.tv	Entertainment	9	991	8329	99
	com.ezscreenrecorder	Entertainment	27	1772	25771	253
	com.anonymoustexting	SMS	14	1558	23165	321
	com.smsplus.app	SMS	13	1287	16459	276
	com.androiddoctor.battery	Malware	9	792	7648	81
F-GC	com.maxauto.maxiplusap	Malware	7	839	7805	87
Acquisition Mode	Package Name	Package type	Large	Gui	Non-Gui	Network
	com.appstalking.photoeditor	Editing	17	1806	21904	191
	de.vsmedia.imagesize	Editing	15	2469	36881	431
	com.redbox.tv	Entertainment	10	1309	12115	133
	com.ezscreenrecorder	Entertainment	28	2471	31985	405
	com.anonymoustexting	SMS	14	2096	29001	380
	com.smsplus.app	SMS	16	1602	20998	338
	com.androiddoctor.battery	Malware	9	1201	11998	119
B-NGC	com.maxauto.maxiplusap	Malware	8	1188	12006	97
Acquisition Mode	Package Name	Package type	Large	Gui	Non-Gui	Network
	com.appstalking.photoeditor	Editing	15	1489	16098	148
	de.vsmedia.imagesize	Editing	13	1992	31116	338
	com.redbox.tv	Entertainment	9	997	9003	102
	com.ezscreenrecorder	Entertainment	24	2097	25993	297
	com.anonymoustexting	SMS	12	1496	25669	319
	com.smsplus.app	SMS	15	1274	16889	269
	com.androiddoctor.battery	Malware	9	992	8003	97
B-GC	com.maxauto.maxiplusap	Malware	7	907	8251	83

Figure 5: Component based Analysis

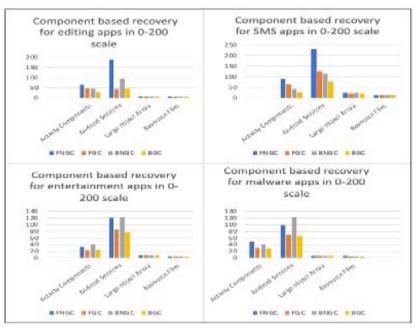


Figure 6: Histogram analysis of various files in selected apps

5. Related Literature

The analysis of software tools' reliability is inevitable in today's digital world (Ivanov, et. al, 2018)}. The reliability assessment is more critical if the analyzed tool is used for solving cyber-related cases. Reliability assessment of such tools is required to analyze if the tool is unreliable, then the evidence extracted by the tool also becomes unreliable, thereby ending up generating incorrect evidence. Hence the reliability assessment of such tools is mandatory, and this research provides a methodology for one such assessment. We identified multiple published works on reliability assessment; however, only a few were related to reliability testing of memory dump acquisition for forensic analysis. Most of the reliability measurement works were based on multiple approaches to develop software reliability growth models using techniques like fuzzy models, regression analysis, neural networks, and machine learning (Ivanov et al., 2018). Another technique for reliability testing is by methodologies like training and testing neural networks (Fisch et. al, 2010) (Park et. al, 2013). However, in this work, we focus on issues about software that focus on the extraction of all types of objects (small and large) from smartphone app memory. This is difficult due to the challenges faced during process dump acquisition (Sylve et. al, 2012) (Pagani et. al, 2019) (Schatz et. al, 2007). There are many works associated with the recovery of forensic data. However, only a few works address the challenges faced by forensic investigators with memory acquisition (Pagani et. al, 2019), are more useful in this work. Among different memory dump acquisition techniques mentioned in works like Volatility (Auty et. al, 2007), (Schatz et al., 2007) - Schatz, in his work, explained his technique for reliable volatile memory dump recovery. Also, Pagani et al., in their work, explained how memory forensics should consider the time in which each memory dump was acquired (Pagani et. al, 2019). Pagani et al. in their work provided a way to assess the reliability of a result obtained thereby minimizing the effect of the acquisition time or detect inconsistencies in the data. While our research closely relates to the idea of reliability (Huelsbergen et. al, 1993) but focuses primarily on external runtime factors, we could not find any work that mentioned runtime factors as critical during memory dump acquisition. Therefore, our research provides a new research dimension of focusing on the critical memory dump acquisition. Hasanbadi et al. proposed an approach to determine approximately how much sequential memory acquisition at a designated time-intervals can mitigate the current challenges in memory forensics (Hasanbadi et al., 2018).

6. Conclusion

In this paper, the methodology identified two runtime factors that can impact Android application dump acquisitions. We presented the analysis results highlighting the changes in the count of objects recovered in every app dump analyzed using userland memory forensic tools. We evaluated multiple apps and identified a difference in object recovery rate during the analysis of app dumps with the runtime factors included during memory acquisition. Finally, we calculated the reliability of userland memory forensic tools using Euclidean distance and covariance metrics. Our evaluation of 30 apps (benign and malicious apps) shows these process states can impose data loss of approximately 20% with a metric Euclidean distance and less than 18% data loss with covariance metric. Furthermore, our comparative analysis found that the count of objects recovered from Foreground acquisitions modes are greater than objects recovered from Background acquisition modes in most of the apps analyzed. The userland forensic analysis's reliability study was conducted on both small and large object recovery tools. The result will be more reliable in object recovery for a forensic investigator who can extract all the objects allocated in memory from the app startup. Also, this research highlights runtime factors and helps investigators explain the environment during memory acquisition, thereby providing a better understanding of reliability factors when dealing with forensic tools during memory dumps acquisition.

References

AndroidLOS, 2017 http://androidxref.com/8.0.0 r4/xref/art/runtime/gc/space/large object space.cc#180 [Online: accessed 13-March 2021]

Market Crime, 2021 "300 terrifying cybercrime and cybersecurity statistics trends" Online:

https://www.comparitech.com/vpn/cybersecurity\ protect\discretionary

Android 8.0 ART Improvements, 2017 Online: https://source.android.com/devices/tech/dalvik/improvements. [Online: accessed 13-March 2021].

Android platform architecture, 2017 URL: https://developer.android.com/guide/platform. [Online: accessed 10-March 2021]

Androidxrefspace URL: http://androidxref.com/8.0.0_ r4/xref/art/runtime/gc/space/. [Online: accessed 10-March 2021]. AndroidLOS, 2017 http://android xref/art/runtime/gc/space/large_object_space.h

Android Dal, 2017 URL:https://source.android.com/devices/tech/dalvik/gc-debug.

Zalewski, M. (2002) from http://lcamtuf.coredump.cx/soft/memfetch. tgz [Online; accessed 17-February 2021].

Market Share, 2020 https://gs.statcounter.com/os-market-share/mobile/worldwide. [Online: accessed 10-March 2021].

Sneha Sudhakaran et ak

- Android Process, 2017,URL: https://learncswithandroid.blogspot.com/2017/ 12/android- process- states.html [Online: accessed 10-March 2021].
- Ali-Gombe, A., Sudhakaran, S., Case, A., Richard III, G.G., 2019. "DroidScraper: A tool for android in-memory object recovery and reconstruction", in: 22nd International Symposium on Research in At- tacks, Intrusions and Defenses ({RAID} 2019), pp. 547–559.
- Auty, M., Case, A., Cohen, M., Dolan-Gavitt, B., Ligh, M.H., Levy, J., Walters, A., (2007). "Volatility-an advanced memory forensics framework".
- Fisch, D., Hofmann, A., Sick, B., 2010. "On the versatility of radial basis function neural networks: A case study in the field of intrusion detection", Information Sciences 180, 2421–2439.
- Hasanabadi, S.S., Lashkari, A.H. and Ghorbani, A.A., 2018, October. "The Next Generation of Robust Linux Memory Acquisition Technique via Sequential Memory Dumps at Designated Time Intervals." In 2018 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.
- ResetGC, 2017, http://androidxref.com/8.0.0 r4/xref/art/runtime/gc/heap.cc#1147
- Ivanov, V., Reznik, A., Succi, G.,. 2018, "Comparing the reliability of software systems: A case study on mobile operating systems". Information Sciences 423.
- Jones, R., Hosking, A., Moss, E., 2016, "The garbage collection handbook: the art of automatic memory management", CRC Press.
- Pagani,F.,Fedorov,O.,Balzarotti,D.,2019, "Introducing the temporal dimension to memory forensics. ACM Transactions on Privacy and Security (TOPS)" 22, 1–21.
- Park, B.J., Oh, S.K., Pedrycz, W., 2013, "The design of polynomial function-based neural network predictors for detection of software defects", Information Sciences 229, 40–57.
- Schatz, B.,2007, "Toward reliable volatile memory acquisition by software" URL: https://www.dfrws.org/2007/proceedings/p126-schatz.pdf. [Online: accessed 10-March 2021].
- Schwermer, P., 2018, "Performance evaluation of Kotlin and Java on Android Runtime"
- Soares, A.M.M., de Sousa Jr, R.T., 2017. "A technique for extraction and analysis of application heap objects within android
- runtime (ART)", in: ICISSP, pp. 147–156.
 Sudhakaran, S., Ali-Gombe, A., Orgah, A., Case, A. and Richard, G.G., 2020, December. "AmpleDroid recovering large object files from Android application memory". In 2020 IEEE International Workshop on Information Forensics and Security
- Sylve, J., Case, A., Marziale, L., Richard, G.G., 2012. "Acquisition and analysis of volatile memory from android devices". Digital Investigation 8, 175–184
- Pridgen, A., Garfinkel, S., Wallach, D. S, "Picking up the trash: Exploiting generational GC for memory analysis", DFRWS,
- Memfetch, 2009, http://shellcoders.blogspot.com/2009/05/using-memfetch-page-37.html
- Genymotion Emulator , 2016, https://www.genymotion.com [Online: accessed 10- September2021]
- FinishGC, 2017, http://androidxref.com/8.0.0_r4/xref/art/runtime/gc/heap.cc#2804
- GooglePlay, 2021, https://play.google.com/store?hl=en_US&gl=US
- VirusShare, 2021, https://virusshare.com

(WIFS) (pp. 1-6). IEEE.

ForceGC, 2013, http://www.codeflow.fi/2013/09/21/force-gc-from-shell/