Healthy Android Examinations:
Timelining Digital Wellbeing Data

Alexis Brignoni
&
Joshua Hickman

SANS DFIR

About Us

Alexis Brignoni

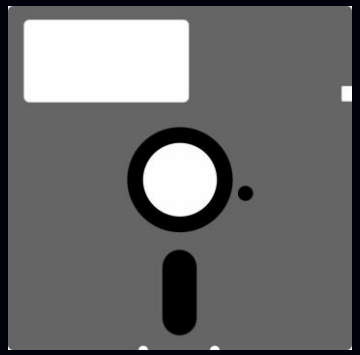
Federal Law Enforcement

Twitter: @AlexisBrignoni

Joshua Hickman

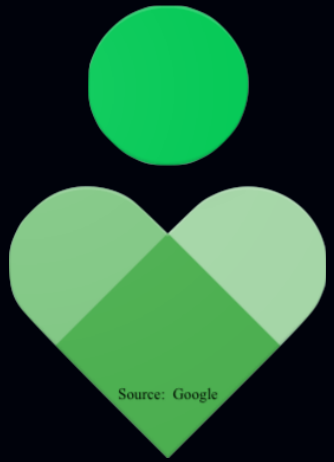
Kroll

Twitter: @josh_hickman1

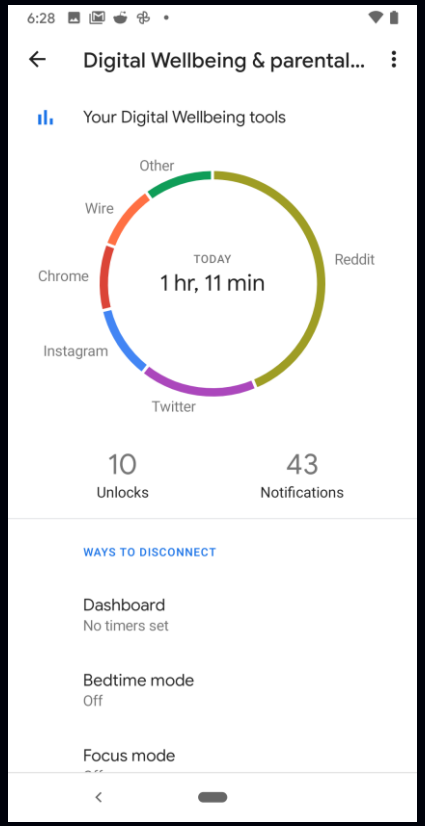


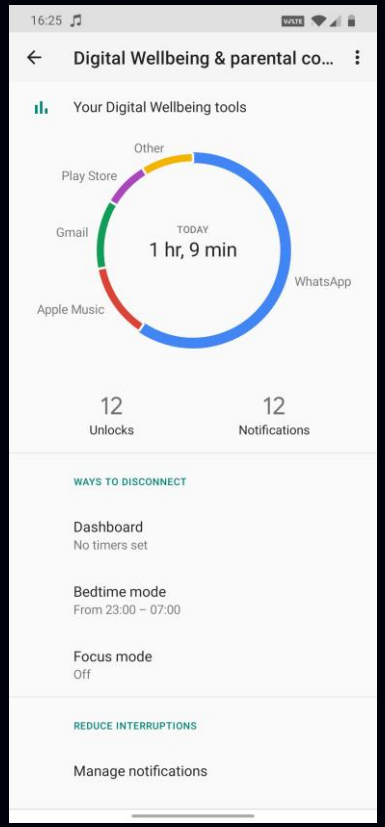
Digital Wellbeing – What Is It?

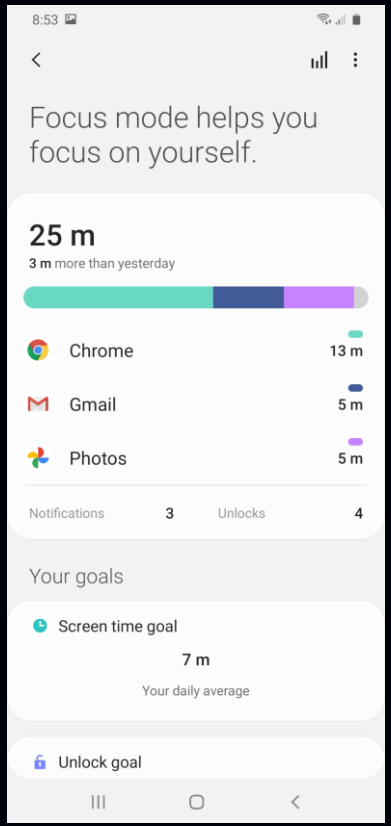
- Introduced at Google I/O 2018
- First seen in Android Oreo (9)
- Initially limited to a specific subset of phones
- 2019 rollout
- Now required on all new devices



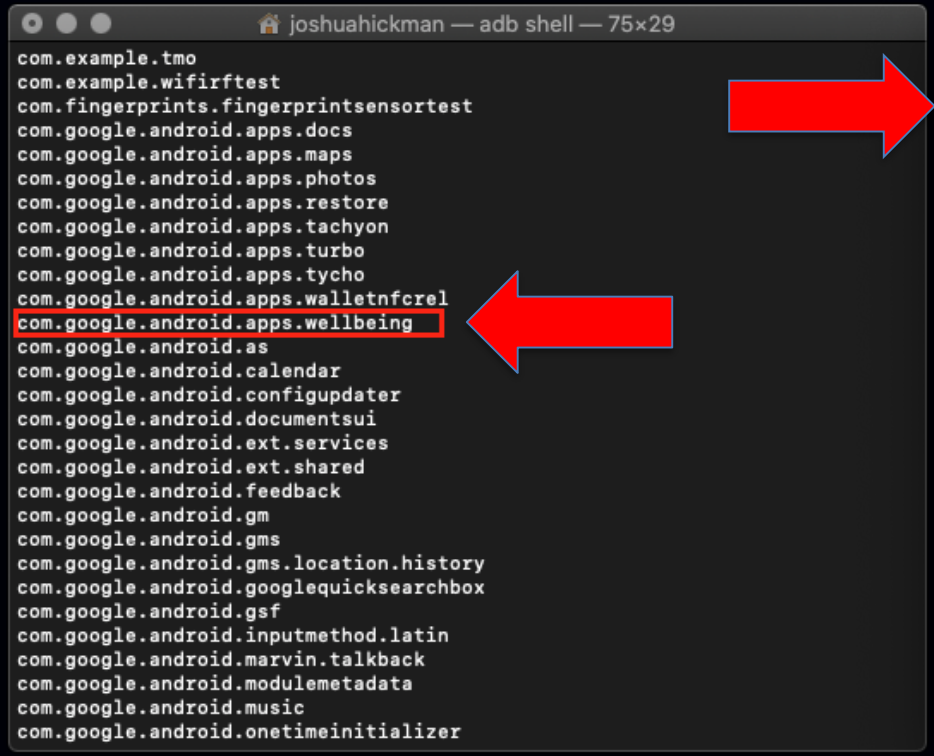
What the User Sees

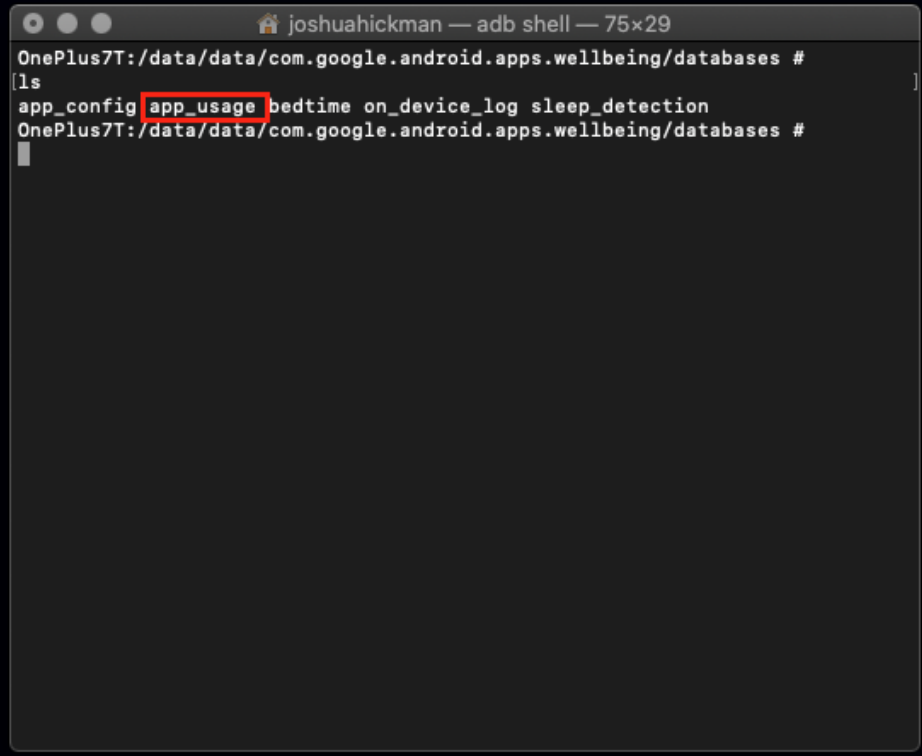






/data/data/com.google.android.apps.wellbeing





events

Table: events

	_id	timestamp	type	package_id	instance_id	task_root_package_id
	Filter	Filter	Filter	Filter	Filter	Filter
1	1	1583530356463	27	1	0	NULL
2	2	1583530369855	1	2	120704734	2
3	3	1583530369903	2	2	120704734	2
4	4	1583530369947	1	3	93173782	3
5	5	1583530370119	19	3	0	NULL
6	6	1583530370124	2	3	93173782	4
7	7	1583530370124	12	3	0	NULL
8	8	1583530370169	1	4	135201230	4
9	9	1583530370400	23	3	93173782	4
10	10	1583530370409	23	2	120704734	2
11	11	1583530373101	12	5	0	NULL
12	12	1583530373103	12	1	0	NULL
13	13	1583530386848	19	6	0	NULL
14	14	1583530386949	12	6	0	NULL
15	15	1583530386970	20	6	0	NULL
16	16	1583530387068	19	5	0	NULL
17	17	1583530387189	12	5	0	NULL
18	18	1583530387309	20	5	0	NULL
19	19	1583530387798	2	4	135201230	4
20	20	1583530387804	1	3	87752118	4
21	21	1583530387850	2	3	87752118	4
22	22	1583530387859	1	3	68158789	4

1 - 22 of 29402

packages

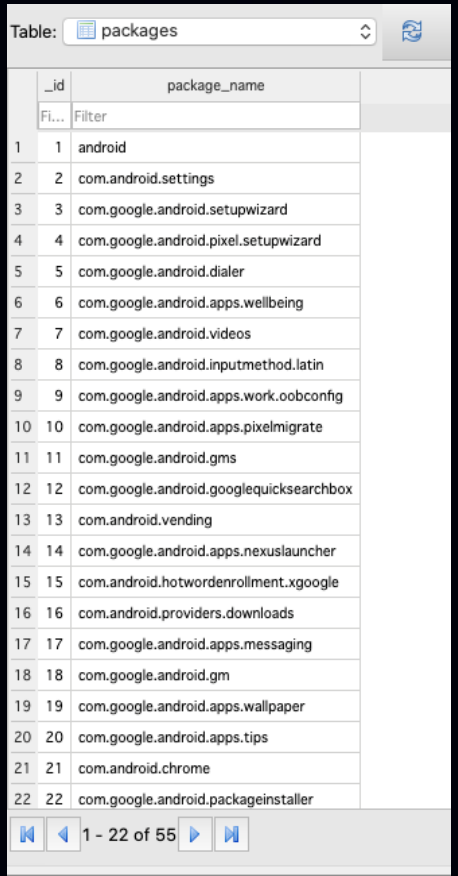


Table: packages

	_id	package_name
	Fi...	Filter
1	1	android
2	2	com.android.settings
3	3	com.google.android.setupwizard
4	4	com.google.android.pixel.setupwizard
5	5	com.google.android.dialer
6	6	com.google.android.apps.wellbeing
7	7	com.google.android.videos
8	8	com.google.android.inputmethod.latin
9	9	com.google.android.apps.work.oobconfig
10	10	com.google.android.apps.pixelmigrate
11	11	com.google.android.gms
12	12	com.google.android.googlequicksearchbox
13	13	com.android.vending
14	14	com.google.android.apps.nexuslauncher
15	15	com.android.hotwordenrollment.xgoogle
16	16	com.android.providers.downloads
17	17	com.google.android.apps.messaging
18	18	com.google.android.gm
19	19	com.google.android.apps.wallpaper
20	20	com.google.android.apps.tips
21	21	com.android.chrome
22	22	com.google.android.packageinstaller

1 - 22 of 55

app_usage

A SQL query will pull the tables together

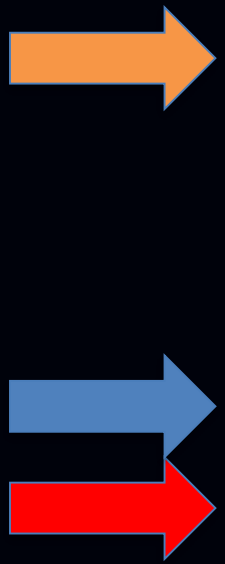
```
SELECT events._id,
datetime(events.timeStamp/1000, "UNIXEPOCH") as timestamps,
Packages.package_name, events.type,
CASE
when events.type=1 THEN 'ACTIVITY_RESUMED'
when events.type=2 THEN 'ACTIVITY_PAUSED’
when events.type=12 THEN 'NOTIFICATION'
when events.type=18 THEN 'KEYGUARD_HIDDEN || DEVICE UNLOCK'
when events.type=19 THEN 'FOREGROUND_SERVICE START'
when events.type=20 THEN 'FOREGROUND_SERVICE_STOP'
when events.type=23 THEN 'ACTIVITY_STOPPED'
when events.type=26 THEN 'DEVICE_SHUTDOWN'
when events.type=27 THEN 'DEVICE_STARTUP'
else events.type
END as eventType
FROM events
INNER JOIN packages ON events.package_id=packages._id
ORDER BY timestamps
```

app_usage

A SQL query will pull the tables together

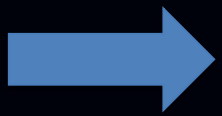
```
SELECT events._id,
datetime(events.timeStamp/1000, "UNIXEPOCH") as timestamps,
Packages.package_name, events.type,
CASE
when events.type=1 THEN 'ACTIVITY_RESUMED'
when events.type=2 THEN 'ACTIVITY_PAUSED’
when events.type=12 THEN 'NOTIFICATION'
when events.type=18 THEN 'KEYGUARD_HIDDEN || DEVICE UNLOCK'
when events.type=19 THEN 'FOREGROUND_SERVICE START'
when events.type=20 THEN 'FOREGROUND_SERVICE_STOP'
when events.type=23 THEN 'ACTIVITY_STOPPED'
when events.type=26 THEN 'DEVICE_SHUTDOWN'
when events.type=27 THEN 'DEVICE_STARTUP'
else events.type
END as eventType
FROM events
INNER JOIN packages ON events.package_id=packages._id
ORDER BY timestamps
```

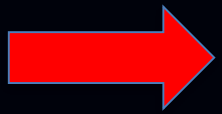
Query Output - Pixel



	_id	timestamps	package_name	type	eventType
29344	29539	2020-07-07 23:28:43	com.wire	2	ACTIVITY_PAUSED
29345	29540	2020-07-07 23:28:43	com.wire	1	ACTIVITY_RESUMED
29346	29541	2020-07-07 23:28:43	com.google.android.apps.nexuslauncher	23	ACTIVITY_STOPPED
29347	29542	2020-07-07 23:28:43	com.wire	23	ACTIVITY_STOPPED
29348	29543	2020-07-07 23:28:59	com.google.android.apps.nexuslauncher	2	ACTIVITY_PAUSED
29349	29544	2020-07-07 23:28:59	com.google.android.apps.nexuslauncher	1	ACTIVITY_RESUMED
29350	29545	2020-07-07 23:28:59	com.wire	2	ACTIVITY_PAUSED
29351	29546	2020-07-07 23:28:59	com.wire	19	FOREGROUND_SERVICE START
29352	29547	2020-07-07 23:28:59	com.wire	20	FOREGROUND_SERVICE_STOP
29353	29548	2020-07-07 23:29:00	com.wire	23	ACTIVITY_STOPPED
29354	29549	2020-07-07 23:29:00	com.wire	12	NOTIFICATION
29355	29550	2020-07-07 23:29:06	com.google.android.apps.nexuslauncher	2	ACTIVITY_PAUSED
29356	29551	2020-07-07 23:29:06	com.google.android.apps.nexuslauncher	23	ACTIVITY_STOPPED
29357	29552	2020-07-07 23:31:52	com.twitter.android	12	NOTIFICATION
29358	29553	2020-07-07 23:35:24	com.google.android.gm	12	NOTIFICATION
29359	29554	2020-07-07 23:35:25	com.google.android.apps.nexuslauncher	1	ACTIVITY_RESUMED
29360	29555	2020-07-07 23:35:25	android	18	KEYGUARD_HIDDEN || DEVICE UNLOCK

Query Output – OnePlus 7T





	_id	timestamp	package_name	type	eventType
2915	3165	2020-07-09 18:03:39	com.google.android.music	19	FOREGROUND_SERVICE START
2916	3166	2020-07-09 18:03:39	com.google.android.music	20	FOREGROUND_SERVICE_STOP
2917	3167	2020-07-09 18:03:40	com.google.android.music	12	NOTIFICATION
2918	3168	2020-07-09 18:03:42	com.google.android.music	19	FOREGROUND_SERVICE START
2919	3169	2020-07-09 18:03:42	com.google.android.music	20	FOREGROUND_SERVICE_STOP
2920	3170	2020-07-09 18:03:42	com.google.android.music	12	NOTIFICATION
2921	3171	2020-07-09 18:53:58	net.oneplus.launcher	2	ACTIVITY_PAUSED
2922	3172	2020-07-09 18:53:58	net.oneplus.launcher	23	ACTIVITY_STOPPED
2923	3173	2020-07-09 18:53:59	android	26	DEVICE_SHUTDOWN
2924	3174	2020-07-09 19:01:51	android	27	DEVICE_STARTUP
2925	3175	2020-07-09 19:01:53	com.android.settings	1	ACTIVITY_RESUMED
2926	3176	2020-07-09 19:01:54	com.android.settings	2	ACTIVITY_PAUSED
2927	3177	2020-07-09 19:01:54	com.android.settings	23	ACTIVITY_STOPPED
2928	3178	2020-07-09 19:02:05	com.android.settings	1	ACTIVITY_RESUMED
2929	3179	2020-07-09 19:02:05	android	18	KEYGUARD_HIDDEN || DEVICE UNLOCK
2930	3180	2020-07-09 19:02:05	com.android.settings	2	ACTIVITY_PAUSED
2931	3181	2020-07-09 19:02:06	net.oneplus.launcher	1	ACTIVITY_RESUMED
2932	3182	2020-07-09 19:02:07	com.android.settings	23	ACTIVITY_STOPPED
2933	3184	2020-07-09 19:02:19	android	12	NOTIFICATION
2934	3185	2020-07-09 19:02:20	com.google.android.googlequicksearchbox	12	NOTIFICATION

Web History...?

Table: component_events

	_id	timestamp	type	component_id
	Fi...	Filter	Filter	Filter
1	1	1594152181111	1	1
2	2	1594152108298	1	1
3	3	1589587549172	1	2
4	4	1589587558046	2	2
5	5	1594152143533	2	1
6	6	1594164382504	1	3
7	7	1594165078413	1	4
8	8	1594161533796	2	3
9	9	1594159744967	1	1
10	10	1594164443982	1	4
11	11	1594164442596	1	3
12	12	1594165142097	2	4
13	13	1594159768103	1	3
14	14	1594164442596	2	5
15	15	1594164516016	2	4
16	16	1594159768103	2	1
17	17	1594164443982	2	3
18	18	1594164389813	2	3
19	19	1594161526489	1	3
20	20	1594159775369	2	3
21	21	1594164389813	1	5

Table: components

	_id	component_name	package_id
	Fi...	Filter	Filter
1	1	arstechnica.com	21
2	2	support.google.com	21
3	3	www.google.com	21
4	4	www.macrumors.com	21
5	5	www.mlb.com	21

Web History...?

A SQL query will pull the tables together

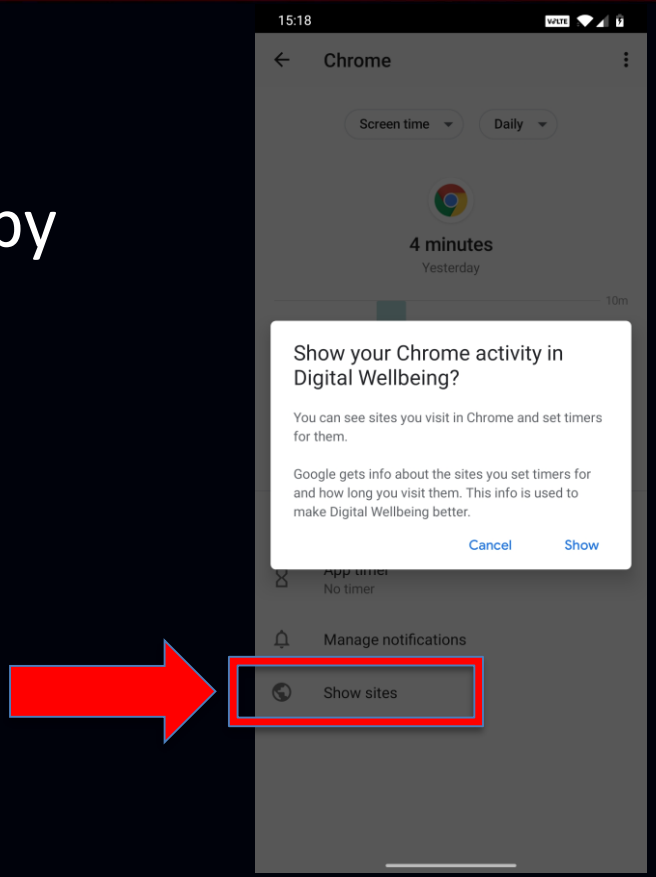
```
SELECT component_events._id,components.package_id,
packages.package_name, components.component_name as
website,
datetime(component_events.timestamp/1000, "UNIXEPOCH") as
timestamp,
CASE
when component_events.type=1 THEN 'ACTIVITY_RESUMED'
when component_events.type=2 THEN 'ACTIVITY_PAUSED'
else component_events.type
END as eventType
FROM component_events
INNER JOIN components ON
component_events.component_id=components._id
INNER JOIN packages ON components.package_id=packages._id
ORDER BY timestamp
```

Yes, Web History

	_id	package_id	package_name	website	timestamp	eventType
1	3	21	com.android.chrome	support.google.com	2020-05-16 00:05:49	ACTIVITY_RESUMED
2	4	21	com.android.chrome	support.google.com	2020-05-16 00:05:58	ACTIVITY_PAUSED
3	2	21	com.android.chrome	arstechnica.com	2020-07-07 20:01:48	ACTIVITY_RESUMED
4	5	21	com.android.chrome	arstechnica.com	2020-07-07 20:02:23	ACTIVITY_PAUSED
5	1	21	com.android.chrome	arstechnica.com	2020-07-07 20:03:01	ACTIVITY_RESUMED
6	9	21	com.android.chrome	arstechnica.com	2020-07-07 22:09:04	ACTIVITY_RESUMED
7	13	21	com.android.chrome	www.google.com	2020-07-07 22:09:28	ACTIVITY_RESUMED
8	16	21	com.android.chrome	arstechnica.com	2020-07-07 22:09:28	ACTIVITY_PAUSED
9	20	21	com.android.chrome	www.google.com	2020-07-07 22:09:35	ACTIVITY_PAUSED
10	19	21	com.android.chrome	www.google.com	2020-07-07 22:38:46	ACTIVITY_RESUMED
11	8	21	com.android.chrome	www.google.com	2020-07-07 22:38:53	ACTIVITY_PAUSED
12	6	21	com.android.chrome	www.google.com	2020-07-07 23:26:22	ACTIVITY_RESUMED
13	18	21	com.android.chrome	www.google.com	2020-07-07 23:26:29	ACTIVITY_PAUSED
14	21	21	com.android.chrome	www.mlb.com	2020-07-07 23:26:29	ACTIVITY_RESUMED
15	11	21	com.android.chrome	www.google.com	2020-07-07 23:27:22	ACTIVITY_RESUMED
16	14	21	com.android.chrome	www.mlb.com	2020-07-07 23:27:22	ACTIVITY_PAUSED
17	10	21	com.android.chrome	www.macrumors.com	2020-07-07 23:27:23	ACTIVITY_RESUMED
18	17	21	com.android.chrome	www.google.com	2020-07-07 23:27:23	ACTIVITY_PAUSED
19	15	21	com.android.chrome	www.macrumors.com	2020-07-07 23:28:36	ACTIVITY_PAUSED
20	7	21	com.android.chrome	www.macrumors.com	2020-07-07 23:37:58	ACTIVITY_RESUMED
21	12	21	com.android.chrome	www.macrumors.com	2020-07-07 23:39:02	ACTIVITY_PAUSED

Yes, Web History…maybe?

- Web history is not captured by default
- User must opt-in
- Can import past history



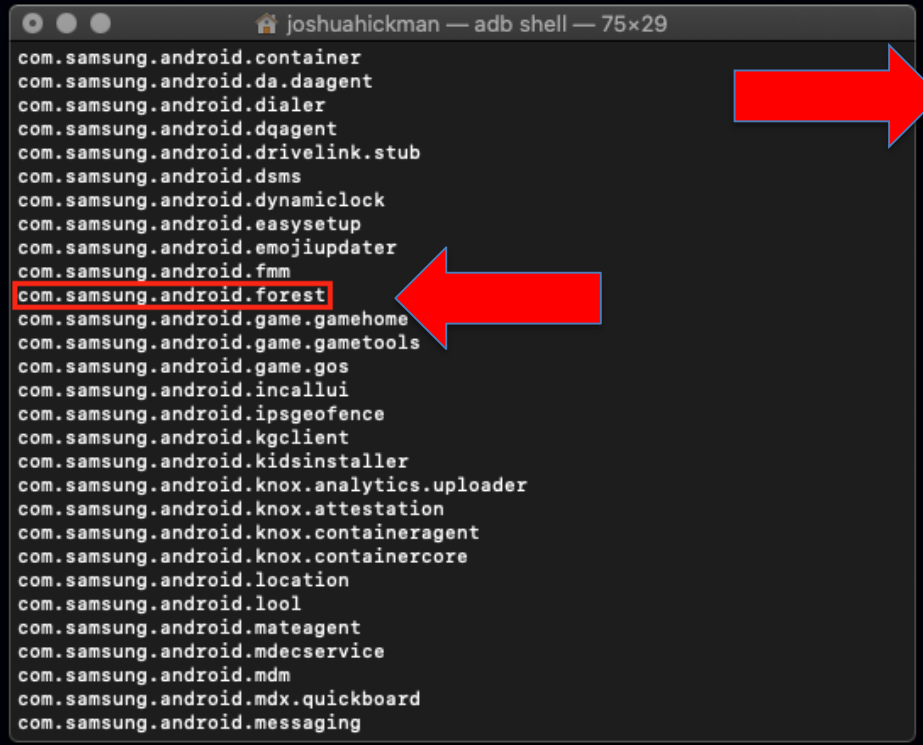
Samsungs Gonna Samsung

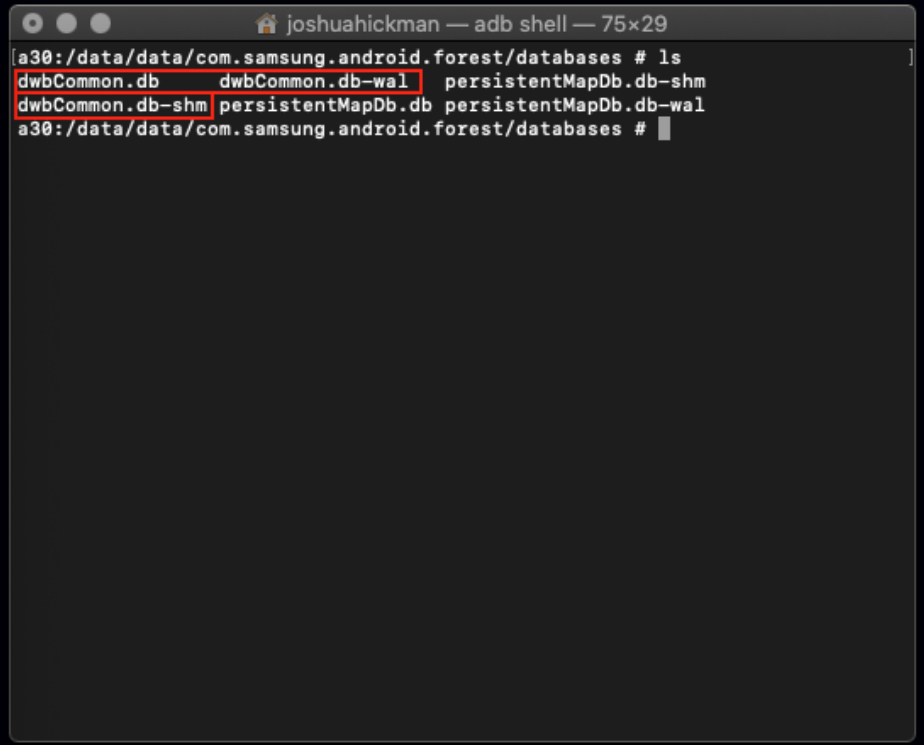
- Because, Samsung
- In-house solution
- Aesthetically different
- Different names

Samsungs Gonna Samsung

- Different APK name
- Different database name
- More Usage Stats codes than Google
- Less data is kept*
- No web history

/data/data/com.samsung.android.forest





usageEvents

Table: usageEvents

	eventId	timeStamp	eventType	className	pkgId
	Filter	Filter	Filter	Filter	Filter
1	12196	1594151637327	5	NULL	1
2	12197	1594151637425	5	NULL	1
3	12198	1594151640608	11	NULL	2
4	12199	1594151640608	11	NULL	210
5	12200	1594151640608	11	NULL	211
6	12201	1594151640608	11	NULL	212
7	12202	1594151640608	11	NULL	3
8	12203	1594151640608	11	NULL	4
9	12204	1594151640608	11	NULL	194
10	12205	1594151640608	11	NULL	213
11	12206	1594151640609	11	NULL	5
12	12207	1594151640609	11	NULL	6
13	12208	1594151640609	11	NULL	195
14	12209	1594151640609	11	NULL	214
15	12210	1594151640609	11	NULL	7
16	12211	1594151640609	11	NULL	215
17	12212	1594151640609	11	NULL	176
18	12213	1594151640609	11	NULL	216
19	12214	1594151640609	11	NULL	8
20	12215	1594151640609	11	NULL	9
21	12216	1594151640609	11	NULL	10
22	12217	1594151640609	11	NULL	11

foundPackages

Table: foundPackages

	pkgId	name
	Filter	Filter
1	1	android
2	2	com.samsung.android.provider.filterprovider
3	3	com.samsung.android.smartswitchassistant
4	4	com.sec.vsim.ericssonnsds.webapp
5	5	com.samsung.android.app.galaxyfinder
6	6	com.sec.location.nsflp2
7	7	com.samsung.android.app.aodservice
8	8	com.android.providers.telephony
9	9	com.sec.android.app.ve.vebgm
10	10	com.sec.android.app.parser
11	11	com.android.dynsystem
12	12	com.android.providers.calendar
13	13	com.osp.app.signin
14	14	com.samsung.clipboardsaveservice
15	15	com.sec.automation
16	16	com.samsung.android.smartmirroring
17	17	com.skms.android.agent
18	18	com.sec.android.app.safetyassurance
19	19	com.samsung.android.incallui
20	20	com.samsung.android.knox.containercore
21	21	com.sec.factory.camera
22	22	com.sec.vsimservice

dwbCommon.db

Another SQL query

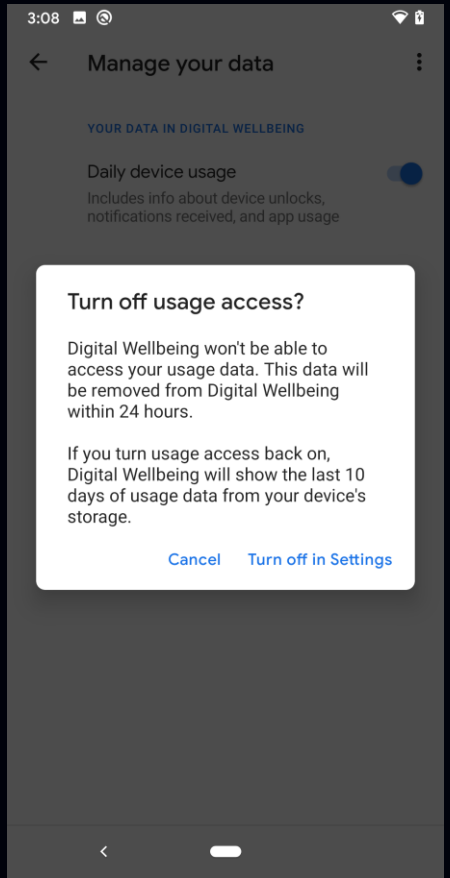
```
SELECT usageEvents.eventId,
datetime(usageEvents.timeStamp/1000, "UNIXEPOCH") as timestamp,
foundPackages.name, usageEvents.eventType,
CASE
when usageEvents.eventType=1 THEN 'ACTIVITY_RESUMED'
when usageEvents.eventType=2 THEN 'ACTIVITY_PAUSED'
when usageEvents.eventType=5 THEN 'CONFIGURATION_CHANGE'
when usageEvents.eventType=7 THEN 'USER_INTERACTION'
when usageEvents.eventType=10 THEN 'NOTIFICATION PANEL'
when usageEvents.eventType=11 THEN 'STANDBY_BUCKET_CHANGED'
when usageEvents.eventType=12 THEN 'NOTIFICATION'
when usageEvents.eventType=15 THEN 'SCREEN_INTERACTIVE (Screen on for full user interaction)'
when usageEvents.eventType=16 THEN 'SCREEN_NON_INTERACTIVE (Screen on in Non-interactive state or
completely turned off)'
when usageEvents.eventType=17 THEN 'KEYGUARD_SHOWN || POSSIBLE DEVICE LOCK'
when usageEvents.eventType=18 THEN 'KEYGUARD_HIDDEN || DEVICE UNLOCK'
when usageEvents.eventType=19 THEN 'FOREGROUND_SERVICE START'
when usageEvents.eventType=20 THEN 'FOREGROUND_SERVICE_STOP'
when usageEvents.eventType=23 THEN 'ACTIVITY_STOPPED'
when usageEvents.eventType=26 THEN 'DEVICE_SHUTDOWN'
when usageEvents.eventType=27 THEN 'DEVICE_STARTUP'
else usageEvents.eventType
END as eventTypeDescription
FROM usageEvents
INNER JOIN foundPackages ON usageEvents.pkgId=foundPackages.pkgId
ORDER BY timestamp
```

Query Output

	eventId	timestamp	name	eventType	eventTypeDescription
1126	13321	2020-07-08 13:39:35	com.android.systemui	11	STANDBY_BUCKET_CHANGED
1127	13322	2020-07-08 13:39:38	com.android.systemui	2	ACTIVITY_PAUSED
1128	13323	2020-07-08 13:39:38	com.sec.android.app.launcher	1	ACTIVITY_RESUMED
1129	13324	2020-07-08 13:39:38	com.android.systemui	23	ACTIVITY_STOPPED
1130	13325	2020-07-08 13:40:11	com.topjohnwu.magisk	11	STANDBY_BUCKET_CHANGED
1131	13326	2020-07-08 13:42:16	com.sec.android.provider.badge	11	STANDBY_BUCKET_CHANGED
1132	13327	2020-07-08 13:45:21	com.google.android.gsf	11	STANDBY_BUCKET_CHANGED
1133	13328	2020-07-08 13:48:48	android	16	SCREEN_NON_INTERACTIVE (Screen on in Non-interactive state or completely turned off)
1134	13329	2020-07-08 13:48:48	com.samsung.android.dynamiclock	11	STANDBY_BUCKET_CHANGED
1135	13330	2020-07-08 13:48:49	com.sec.android.app.launcher	2	ACTIVITY_PAUSED
1136	13331	2020-07-08 13:48:49	com.sec.android.app.launcher	23	ACTIVITY_STOPPED
1137	13332	2020-07-08 13:48:49	android	15	SCREEN_INTERACTIVE (Screen on for full user interaction)
1138	13333	2020-07-08 13:48:49	com.sec.android.app.launcher	1	ACTIVITY_RESUMED
1139	13334	2020-07-08 13:48:49	android	17	KEYGUARD_SHOWN || POSSIBLE DEVICE LOCK
1140	13335	2020-07-08 13:48:50	com.sec.android.app.launcher	2	ACTIVITY_PAUSED
1141	13336	2020-07-08 13:48:50	com.sec.android.app.launcher	23	ACTIVITY_STOPPED
1142	13337	2020-07-08 13:48:50	com.google.android.gsf	11	STANDBY_BUCKET_CHANGED
1143	13338	2020-07-08 13:48:53	com.sec.android.app.launcher	1	ACTIVITY_RESUMED
1144	13339	2020-07-08 13:48:53	android	18	KEYGUARD_HIDDEN || DEVICE UNLOCK
1145	13340	2020-07-08 13:48:54	com.sec.android.app.launcher	2	ACTIVITY_PAUSED
1146	13341	2020-07-08 13:48:54	com.samsung.android.forest	1	ACTIVITY_RESUMED

Overall Limitations…

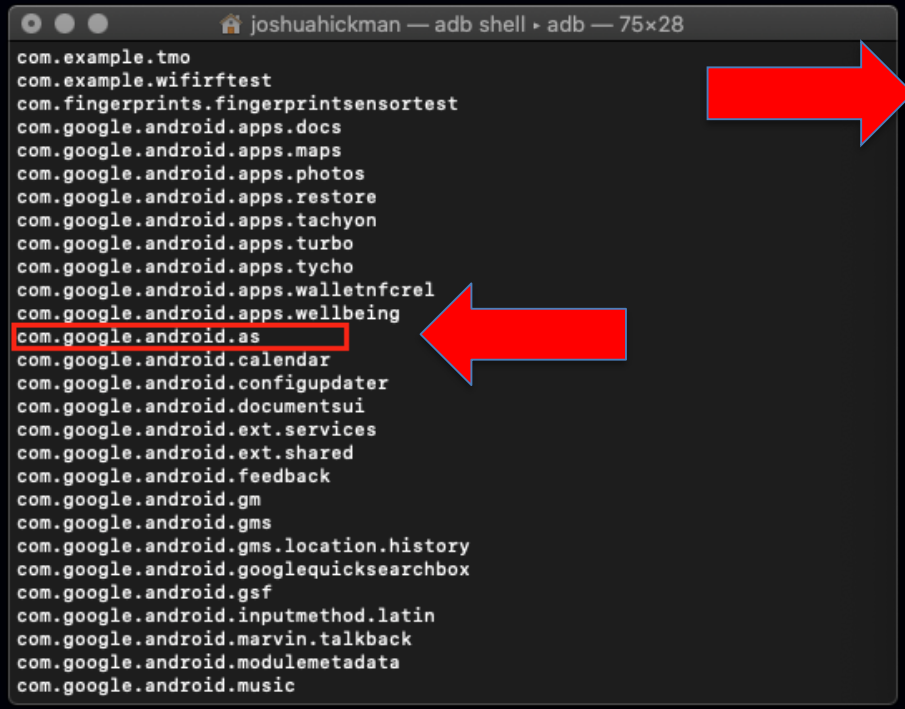
- Retention time
- Users can turn Digital Wellbeing off*
- No data kept on deleted apps

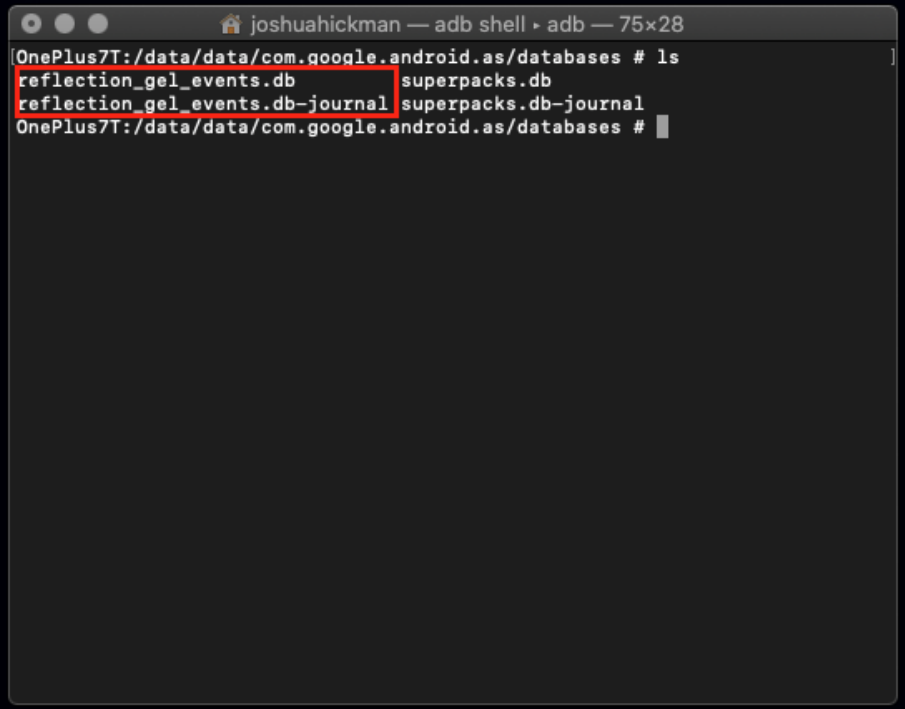


*Settings > Apps & Notifications > Special App Access > Usage Access

Deleted Apps

/data/data/com.google.android.as





reflections_gel_events.db

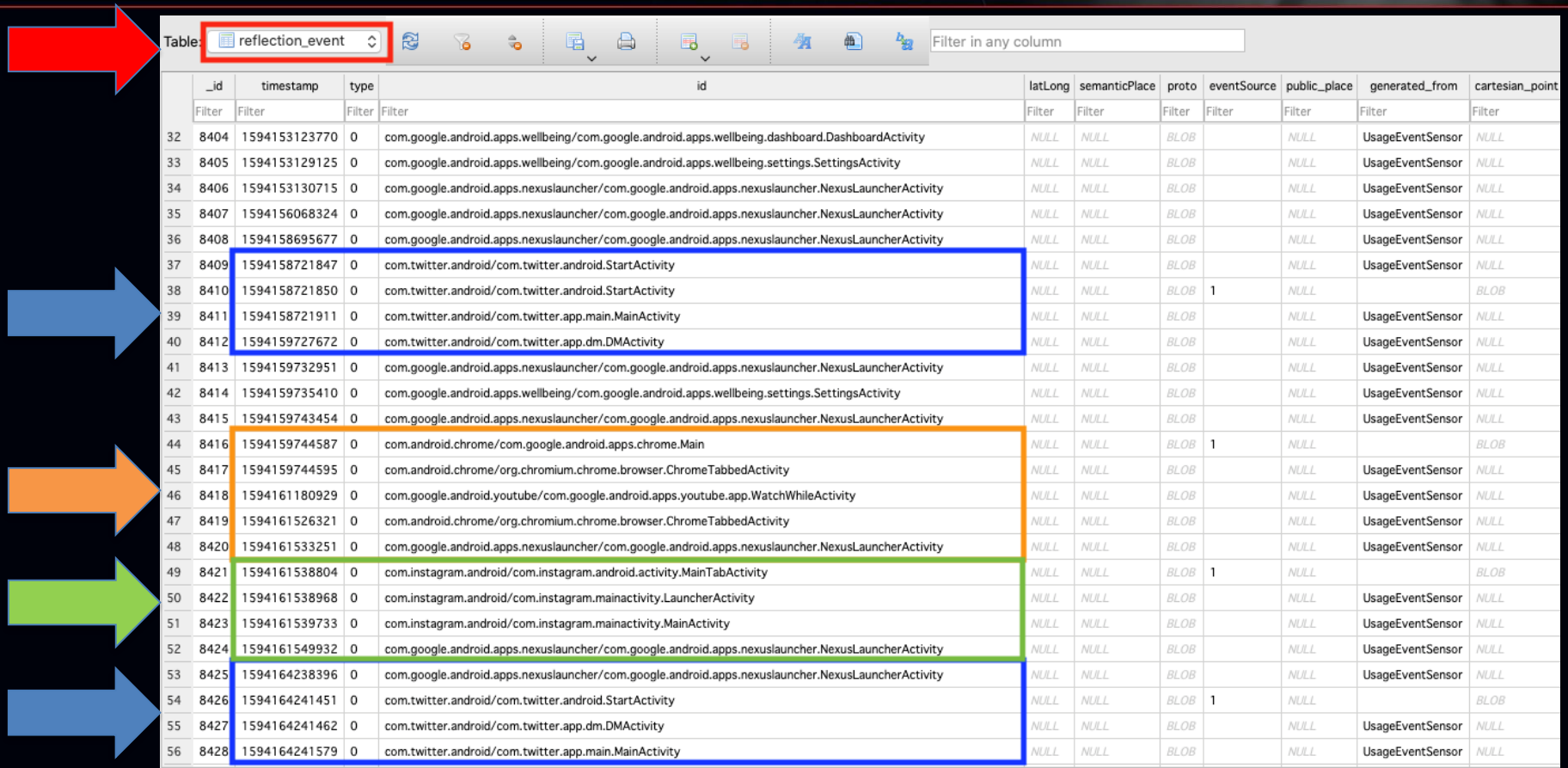


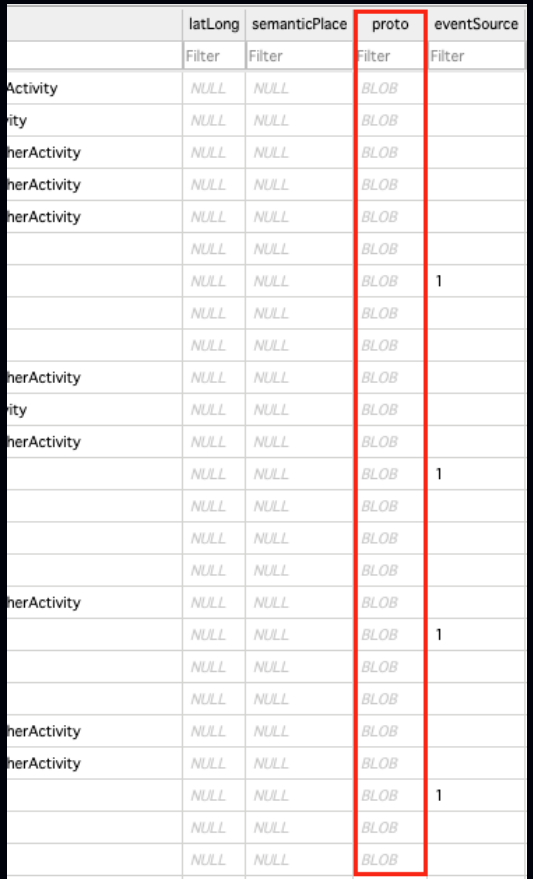
Table: reflection_event

Filter in any column

	_id	timestamp	type	id	latLong	semanticPlace	proto	eventSource	public_place	generated_from	cartesian_point
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
32	8404	1594153123770	0	com.google.android.apps.wellbeing/com.google.android.apps.wellbeing.dashboard.DashboardActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
33	8405	1594153129125	0	com.google.android.apps.wellbeing/com.google.android.apps.wellbeing.settings.SettingsActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
34	8406	1594153130715	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
35	8407	1594156068324	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
36	8408	1594158695677	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
37	8409	1594158721847	0	com.twitter.android/com.twitter.android.StartActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
38	8410	1594158721850	0	com.twitter.android/com.twitter.android.StartActivity	NULL	NULL	BLOB	1	NULL		BLOB
39	8411	1594158721911	0	com.twitter.android/com.twitter.app.main.MainActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
40	8412	1594159727672	0	com.twitter.android/com.twitter.app.dm.DMActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
41	8413	1594159732951	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
42	8414	1594159735410	0	com.google.android.apps.wellbeing/com.google.android.apps.wellbeing.settings.SettingsActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
43	8415	1594159743454	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
44	8416	1594159744587	0	com.android.chrome/com.google.android.apps.chrome.Main	NULL	NULL	BLOB	1	NULL		BLOB
45	8417	1594159744595	0	com.android.chrome/org.chromium.chrome.browser.ChromeTabbedActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
46	8418	1594161180929	0	com.google.android.youtube/com.google.android.apps.youtube.app.WatchWhileActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
47	8419	1594161526321	0	com.android.chrome/org.chromium.chrome.browser.ChromeTabbedActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
48	8420	1594161533251	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
49	8421	1594161538804	0	com.instagram.android/com.instagram.android.activity.MainTabActivity	NULL	NULL	BLOB	1	NULL		BLOB
50	8422	1594161538968	0	com.instagram.android/com.instagram.mainactivity.LauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
51	8423	1594161539733	0	com.instagram.android/com.instagram.mainactivity.MainActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
52	8424	1594161549932	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
53	8425	1594164238396	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
54	8426	1594164241451	0	com.twitter.android/com.twitter.android.StartActivity	NULL	NULL	BLOB	1	NULL		BLOB
55	8427	1594164241462	0	com.twitter.android/com.twitter.app.dm.DMActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL
56	8428	1594164241579	0	com.twitter.android/com.twitter.app.main.MainActivity	NULL	NULL	BLOB		NULL	UsageEventSensor	NULL

Protobuf

- Data in the proto column is a replay of what is in the other columns
- Using protoc can decode the data



	latLong	semanticPlace	proto	eventSource
	Filter	Filter	Filter	Filter
Activity	NULL	NULL	BLOB	
ity	NULL	NULL	BLOB	
herActivity	NULL	NULL	BLOB	
herActivity	NULL	NULL	BLOB	
herActivity	NULL	NULL	BLOB	
	NULL	NULL	BLOB	
	NULL	NULL	BLOB	1
	NULL	NULL	BLOB	
	NULL	NULL	BLOB	
herActivity	NULL	NULL	BLOB	
ity	NULL	NULL	BLOB	
herActivity	NULL	NULL	BLOB	
	NULL	NULL	BLOB	1
	NULL	NULL	BLOB	
	NULL	NULL	BLOB	
	NULL	NULL	BLOB	
herActivity	NULL	NULL	BLOB	
	NULL	NULL	BLOB	1
	NULL	NULL	BLOB	
	NULL	NULL	BLOB	
herActivity	NULL	NULL	BLOB	
herActivity	NULL	NULL	BLOB	
	NULL	NULL	BLOB	1
	NULL	NULL	BLOB	
	NULL	NULL	BLOB	

Protobuf

It retains data about activity in deleted apps

Deleted App Data

Table: reflection_event

New Record

	_id	timestamp	type	id	latLong	semanticPlace	proto	eventSource
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
2723	2723	1584482802854	0	com.google.android.contacts/com.google.android.apps.contacts.editorlite.InsertOrEditActivity	NULL	NULL	BLOB	
2724	2724	1584482810616	0	com.whatsapp/com.whatsapp.Conversation	NULL	NULL	BLOB	
2725	2725	1584482881082	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActiv...	NULL	NULL	BLOB	

Table: reflection_event

New Record Delete Record

	_id	timestamp	type	id	latLong	semanticPlace	proto	eventSource
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
2723	2723	1584482802854	0	com.google.android.contacts/com.google.android.apps.contacts.editorlite.InsertOrEditActivity	NULL	NULL	BLOB	
2724	2724	1584482810616	0	/deleted_app/_8	NULL	NULL	BLOB	
2725	2725	1584482881082	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB	

Deleted App Data

Table: reflection_event

New Record

	_id	timestamp	type	id	latLong	semanticPlace	proto	eventSource
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
2723	2723	1584482802854	0	com.google.android.contacts/com.google.android.apps.contacts.editorlite.InsertOrEditActivity	NULL	NULL	BLOB	
2724	2724	1584482810616	0	com.whatsapp/com.whatsapp.Conversation	NULL	NULL	BLOB	
2725	2725	1584482881082	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActiv...	NULL	NULL	BLOB	

Table: reflection_event

New Record

Delete Record

	_id	timestamp	type	id	latLong	semanticPlace	proto	eventSource
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
2723	2723	1584482802854	0	com.google.android.contacts/com.google.android.apps.contacts.editorlite.InsertOrEditActivity	NULL	NULL	BLOB	
2724	2724	1584482810616	0	/deleted_app/_8	NULL	NULL	BLOB	
2725	2725	1584482881082	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB	

Decoded protobuf

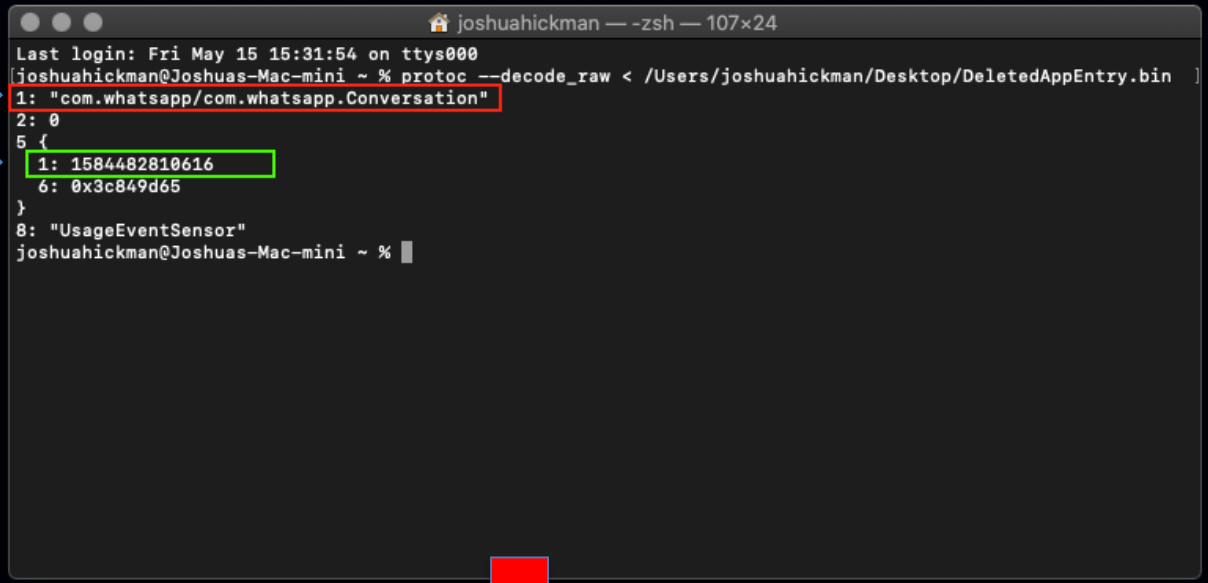


Table: reflection_event

New Record | Delete Record

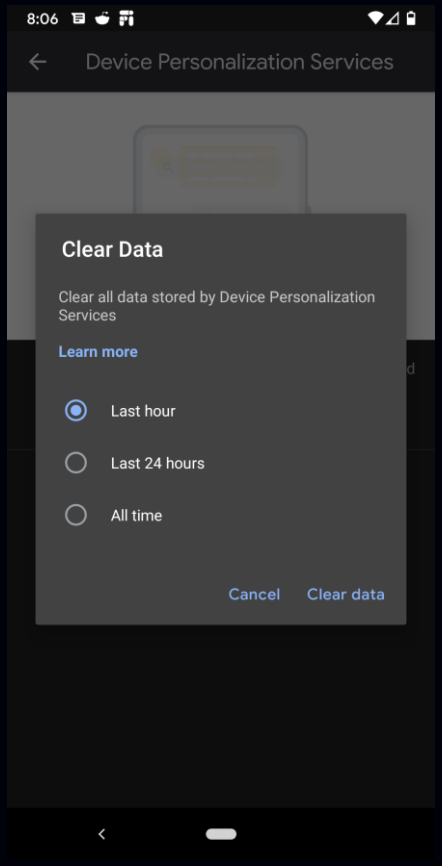
	_id	tim	type	id	latLong	semanticPlace	proto	eventSource
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
2723	2723	1584482802854	0	com.google.android.contacts/com.google.android.apps.contacts.editorlite.InsertOrEditActivity	NULL	NULL	BLOB	
2724	2724	1584482810616	0	/deleted_app/_8	NULL	NULL	BLOB	
2725	2725	1584482881082	0	com.google.android.apps.nexuslauncher/com.google.android.apps.nexuslauncher.NexusLauncherActivity	NULL	NULL	BLOB	

Limitations

Users have options:

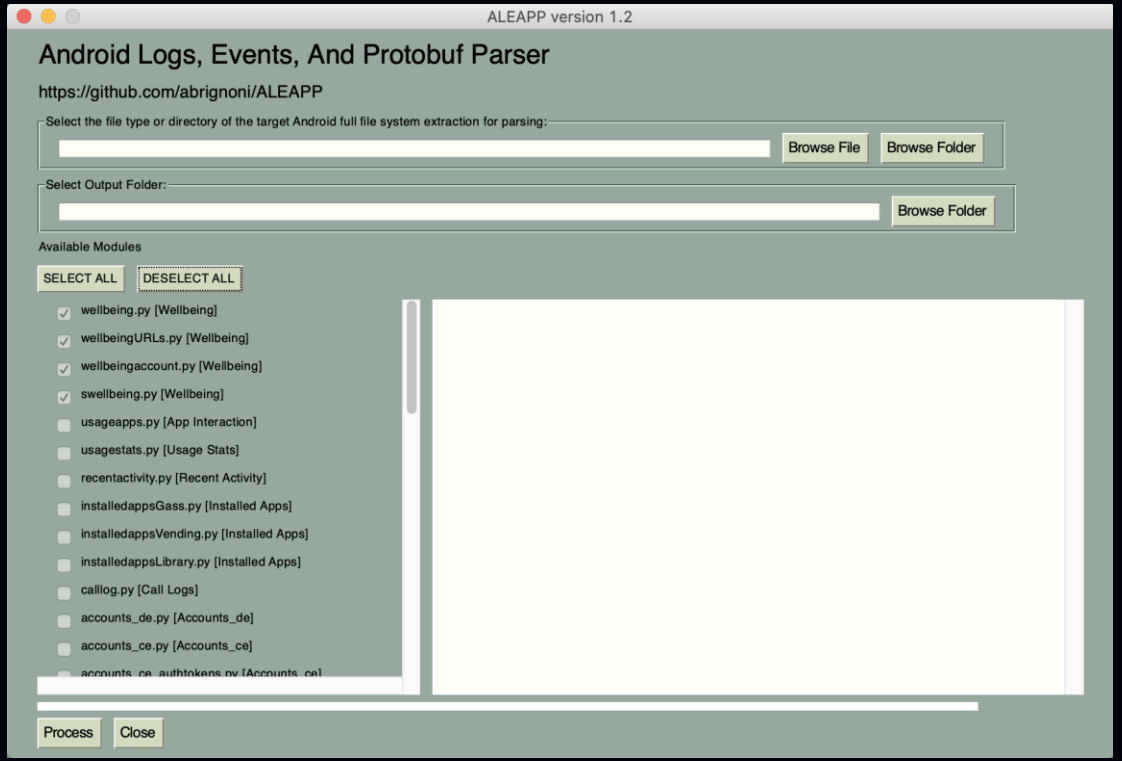
- Delete the last hour of data
- Delete the last 24 hours of data
- Delete all data
- Turn DPS off*

*Settings > Apps & Notifications > Special App Access > Usage Access



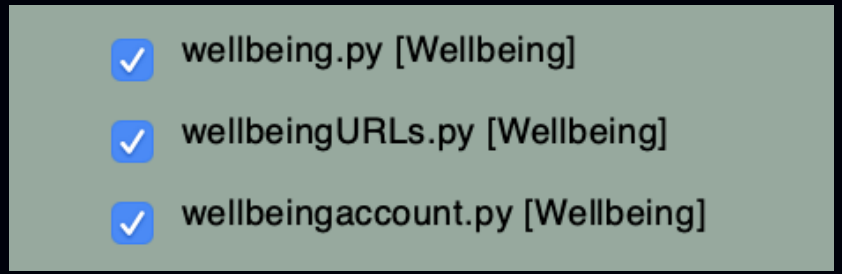
Implementation

ALEAPP (Android Logs Events And Protobuf Parser)



Implementation

ALEAPP (Android Logs Events And Protobuf Parser)



https://github.com/abrignoni/ALEAPP

ALEAPP Report

ALEAPP 1.2

SAVED REPORTS
- Report Home

ACCOUNTS_CE
- accounts_ce_0
- Authtokens_0

ACCOUNTS_DE
- accounts_de_0
- accounts_de_11

APP INTERACTION
- Personalization Services

CALL LOGS
- Call logs

CHROME
- Chrome Bookmarks
- Chrome Cookies
- Chrome Downloads
- Chrome History
- Chrome Keyword Search Terms
- Chrome Login Data
- Chrome Offline Pages
- Chrome Search Terms

DEVICE INFO
- Build Info
- Partner Settings

Android Logs Events And Protobuf Parser

ALEAPP is an open source project that aims to parse every known Android artifact for the purpose of forensic analysis.

Case Information

Details | Script run log | Processed files list

Extraction location	/Volumes/Black_Samsung_T5/Pixel 3.zip
Extraction type	zip
Report directory	/Volumes/Black_Samsung_T5/Output/ALEAPP_Reports_2020-07-06_Monday_143153
Processing time	00:01:20 (Total 80.99928 seconds)

All dates and times are in UTC unless noted otherwise!

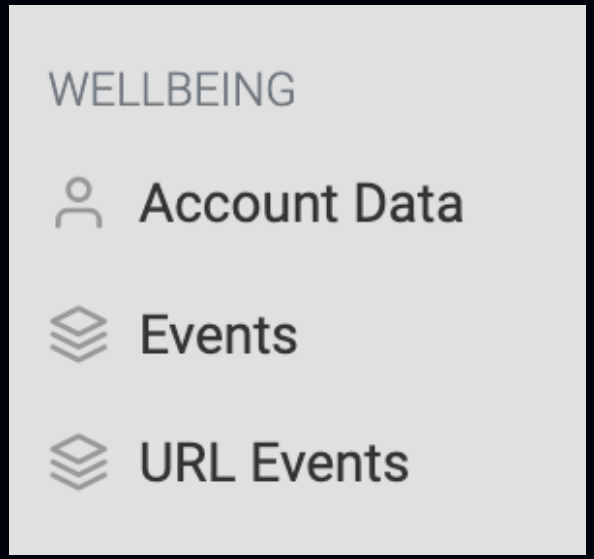
Thank you for using ALEAPP

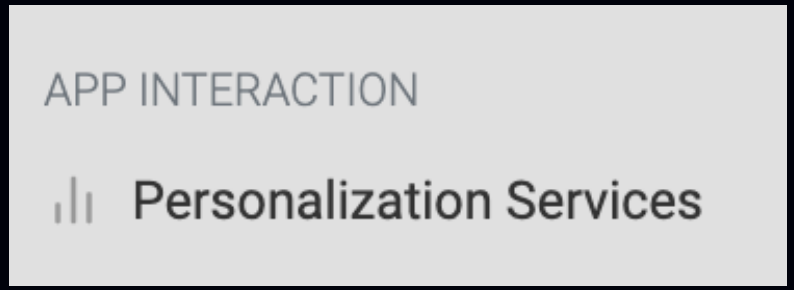
Support open source and report any bugs!

Project Home

ALEAPP Team

Report Categories





Wellbeing events report

Total number of entries: 7827

Wellbeing events located at: /Volumes/Black_Samsung_T5/Output/ALEAPP_Reports_2020-07-06_Monday_143153/temp/Pixel 3/data/data/com.google.android.apps.wellbeing/databases/app_usage

Show 15 entries

Search:

Timestamp	Package ID	Event Type
2020-01-29 15:38:03	android	DEVICE_STARTUP
2020-01-29 15:38:10	com.android.settings	ACTIVITY_RESUMED
2020-01-29 15:38:10	com.android.settings	ACTIVITY_PAUSED
2020-01-29 15:38:10	com.google.android.setupwizard	ACTIVITY_RESUMED
2020-01-29 15:38:10	com.google.android.setupwizard	FOREGROUND_SERVICE_START
2020-01-29 15:38:10	com.google.android.setupwizard	ACTIVITY_PAUSED
2020-01-29 15:38:10	com.google.android.setupwizard	NOTIFICATION
2020-01-29 15:38:10	com.google.android.pixel.setupwizard	ACTIVITY_RESUMED
2020-01-29 15:38:11	com.google.android.setupwizard	ACTIVITY_STOPPED
2020-01-29 15:38:11	com.android.settings	ACTIVITY_STOPPED
2020-01-29 15:38:13	android	NOTIFICATION
2020-01-29 15:38:17	com.google.android.apps.tycho	NOTIFICATION
2020-01-29 15:38:29	com.google.android.apps.wellbeing	FOREGROUND_SERVICE_START
2020-01-29 15:38:29	com.google.android.apps.wellbeing	FOREGROUND_SERVICE_STOP
2020-01-29 15:38:29	com.google.android.apps.wellbeing	NOTIFICATION
Timestamp	Package ID	Event Type

Showing 1 to 15 of 7,827 entries

2020-01-29 20:06:37	com.imgur.mobile	ACTIVITY_STOPPED
2020-01-29 20:11:35	com.imgur.mobile	ACTIVITY_PAUSED
2020-01-29 20:11:35	com.imgur.mobile	ACTIVITY_STOPPED
2020-01-29 20:14:09	com.imgur.mobile	ACTIVITY_RESUMED
2020-01-29 20:14:09	android	KEYGUARD_HIDDEN & || Device Unlock
2020-01-29 20:14:18	com.google.android.apps.messaging	NOTIFICATION
2020-01-29 20:14:19	com.google.android.gm	NOTIFICATION
2020-01-29 20:14:22	com.google.android.apps.nexuslauncher	ACTIVITY_PAUSED
2020-01-29 20:14:22	com.google.android.apps.nexuslauncher	ACTIVITY_RESUMED
2020-01-29 20:14:22	com.imgur.mobile	ACTIVITY_PAUSED
2020-01-29 20:14:22	com.imgur.mobile	ACTIVITY_STOPPED
2020-01-29 20:14:26	com.google.android.apps.nexuslauncher	ACTIVITY_PAUSED
2020-01-29 20:14:26	com.imgur.mobile	ACTIVITY_RESUMED
2020-01-29 20:14:26	com.google.android.apps.nexuslauncher	ACTIVITY_STOPPED
2020-01-29 20:16:08	com.google.android.apps.messaging	NOTIFICATION
2020-01-29 20:16:09	com.google.android.apps.messaging	NOTIFICATION
2020-01-29 20:16:21	com.imgur.mobile	ACTIVITY_PAUSED
2020-01-29 20:16:21	com.google.android.gms	ACTIVITY_RESUMED
2020-01-29 20:16:28	com.google.android.gms	ACTIVITY_PAUSED
2020-01-29 20:16:28	com.imgur.mobile	ACTIVITY_RESUMED
2020-01-29 20:16:28	com.google.android.gms	ACTIVITY_STOPPED
2020-01-29 20:16:30	com.imgur.mobile	ACTIVITY_PAUSED
2020-01-29 20:16:30	com.google.android.gms	ACTIVITY_RESUMED
2020-01-29 20:16:32	com.google.android.gms	ACTIVITY_PAUSED
2020-01-29 20:16:32	com.imgur.mobile	ACTIVITY_RESUMED
2020-01-29 20:16:33	com.google.android.gms	ACTIVITY_STOPPED
2020-01-29 20:17:25	com.imgur.mobile	ACTIVITY_PAUSED

Wellbeing events report

Total number of entries: 7827

Wellbeing events located at: /Volumes/Black_Samsung_T5/Output/ALEAPP_Reports_2020-07-06_Monday_143153/temp/Pixel 3/data/data/com.google.android.apps.wellbeing/databases/app_usage

Show 15 entries

Search: wickr

Timestamp	Package ID	Event Type
2020-01-29 18:46:37	com.mywickr.wickr2	ACTIVITY_RESUMED
2020-01-29 18:46:37	com.mywickr.wickr2	ACTIVITY_PAUSED
2020-01-29 18:46:37	com.mywickr.wickr2	ACTIVITY_RESUMED
2020-01-29 18:46:38	com.mywickr.wickr2	ACTIVITY_STOPPED
2020-01-29 18:47:22	com.mywickr.wickr2	ACTIVITY_PAUSED
2020-01-29 18:47:22	com.mywickr.wickr2	ACTIVITY_RESUMED
2020-01-29 18:47:23	com.mywickr.wickr2	ACTIVITY_STOPPED
2020-01-29 18:47:37	com.mywickr.wickr2	ACTIVITY_PAUSED
2020-01-29 18:47:37	com.mywickr.wickr2	ACTIVITY_STOPPED
2020-02-01 00:59:38	com.mywickr.wickr2	ACTIVITY_RESUMED
2020-02-01 00:59:39	com.mywickr.wickr2	ACTIVITY_PAUSED
2020-02-01 00:59:39	com.mywickr.wickr2	ACTIVITY_RESUMED
2020-02-01 00:59:39	com.mywickr.wickr2	ACTIVITY_STOPPED
2020-02-01 00:59:42	com.mywickr.wickr2	ACTIVITY_PAUSED
2020-02-01 00:59:42	com.mywickr.wickr2	ACTIVITY_RESUMED
Timestamp	Package ID	Event Type

Showing 1 to 15 of 193 entries (filtered from 7,827 total entries)

Wellbeing URL events report

Total number of entries: 11

Wellbeing URL events located at: /Volumes/Black_Samsung_T5/Output/ALEAPP_Reports_2020-07-08_Wednesday_125320/temp/Pixel 3/data/data/com.google.android.apps.wellbeing/databases/app_usage

Show All entries

Search:

Timestamp	Event ID	Package ID	Package Name	Website	Event
2020-01-29 16:33:25	3	21	com.android.chrome	www.google.com	ACTIVITY_RESUMED
2020-01-29 16:33:25	10	21	com.android.chrome	newtab	ACTIVITY_PAUSED
2020-01-29 16:33:32	2	21	com.android.chrome	www.google.com	ACTIVITY_PAUSED
2020-01-29 16:33:32	7	21	com.android.chrome	magiskmanager.com	ACTIVITY_RESUMED
2020-01-29 16:33:56	4	21	com.android.chrome	magiskmanager.com	ACTIVITY_PAUSED
2020-01-29 16:33:56	8	21	com.android.chrome	magiskmanager.com	ACTIVITY_RESUMED
2020-01-29 16:34:55	6	21	com.android.chrome	magiskmanager.com	ACTIVITY_PAUSED
2020-01-29 16:35:17	11	21	com.android.chrome	magiskmanager.com	ACTIVITY_RESUMED
2020-01-29 16:35:19	5	21	com.android.chrome	magiskmanager.com	ACTIVITY_PAUSED
2020-02-01 02:11:13	1	21	com.android.chrome	magiskmanager.com	ACTIVITY_RESUMED
2020-02-01 02:12:10	9	21	com.android.chrome	magiskmanager.com	ACTIVITY_PAUSED
Timestamp	Event ID	Package ID	Package Name	Website	Event

Showing 1 to 11 of 11 entries

Previous 1

Implementation

ALEAPP (Android Logs Events And Protobuf Parser)

https://github.com/abrignoni/ALEAPP

Device Personalization Services report

This is data stored by the reflection_gel_events.db, which shows data usage from apps to included deleted apps.

Total number of entries: 2838

Device Personalization Services located at: /Volumes/Black_Samsung_T5/Output/ALEAPP_Reports_2020-07-06_Monday_143153/temp/Pixel 3/data/data/com.google.android.as/databases/reflection_gel_events.db

Show 15 entries

Search: wickr

Timestamp	Deleted?	BundleID	From	From in Proto	Proto Full
2020-02-14 01:14:17		com.mywickr.wickr2/com.wickr.enterprise.chat.PrivateChatActivity	UsageEventSensor	1059401331	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.chat.Privat '5': {'1': 1581642857184, '6': 1059401331}, '8': 'UsageEvent
2020-02-14 01:13:06		com.mywickr.wickr2/com.wickr.enterprise.call.ui.CallActivity	UsageEventSensor	1059401331	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.call.ui.Call 1581642786319, '6': 1059401331}, '8': 'UsageEventSensor
2020-02-14 01:13:04		com.mywickr.wickr2/com.wickr.enterprise.call.ui.CallActivity	UsageEventSensor	1059401331	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.call.ui.Call 1581642784915, '6': 1059401331}, '8': 'UsageEventSensor
2020-02-14 01:08:12		com.mywickr.wickr2/com.wickr.enterprise.chat.PrivateChatActivity	UsageEventSensor	999122136	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.chat.Privat '5': {'1': 1581642492009, '6': 999122136}, '8': 'UsageEventS
2020-02-14 01:08:11		com.mywickr.wickr2/com.wickr.enterprise.verification.VerificationChatActivity	UsageEventSensor	999122136	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.verification.Ver '2': 0, '5': {'1': 1581642491988, '6': 999122136}, '8': 'UsageEv
2020-02-14 01:08:09		com.mywickr.wickr2/com.wickr.enterprise.dashboard.DashboardActivity			{'1': 'com.mywickr.wickr2/com.wickr.enterprise.dashboard '5': {'1': 1581642489364}, '9': ['GEL', '1']}
2020-02-14 01:08:09		com.mywickr.wickr2/com.wickr.enterprise.dashboard.DashboardActivity	UsageEventSensor	999122136	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.dashboard '2': 0, '5': {'1': 1581642489404, '6': 999122136}, '8': 'UsageEv
2020-02-14		com.mywickr.wickr2/com.wickr.enterprise.dashboard.DashboardListActivity	UsageEventSensor	999122136	{'1':

Device Personalization Services report

This is data stored by the reflection_gel_events.db, which shows data usage from apps to included deleted apps.

Total number of entries: 2838

Device Personalization Services located at: /Volumes/Black_Samsung_T5/Output/ALEAPP_Reports_2020-07-06_Monday_143153/temp/Pixel 3/data/data/com.google.android.as/databases/reflection_gel_events.db

Show 15 entries

Search:

Timestamp	Deleted?	BundleID	From	From in Proto	Proto Full
2020-01-29 15:38:13		com.android.settings/com.android.settings.CryptKeeper	UsageEventSensor	951664537	{'1': 'com.android.settings/com.andro 951664537}, '8': 'UsageEventSensor'}
2020-01-29 15:38:13		com.google.android.setupwizard/com.google.android.setupwizard.SetupWizardActivity	UsageEventSensor	965979305	{'1': 'com.google.android.setupwizard '5': {'1': 1580312293258, '6': 9659793
2020-01-29 15:38:13		com.google.android.pixel.setupwizard/com.google.android.pixel.setupwizard.user.WelcomeActivity	UsageEventSensor	0	{'1': 'com.google.android.pixel.setupwizar '2': 0, '5': {'1': 1580312293462, '6': 0},
2020-01-29 15:38:13		com.google.android.pixel.setupwizard/com.google.android.pixel.setupwizard.user.WelcomeActivity	UsageEventSensor	1027945393	{'1': 'com.google.android.pixel.setupwizar '2': 0, '5': {'1': 1580312293462, '6': 102
2020-01-29 15:38:35		com.google.android.setupwizard/com.google.android.setupwizard.WizardManagerActivity	UsageEventSensor	1033286588	{'1': 'com.google.android.setupwizard 0, '5': {'1': 1580312315582, '6': 10332
2020-01-29 15:38:35		com.google.android.setupwizard/com.google.android.setupwizard.ProgressActivity	UsageEventSensor	1033286588	{'1': 'com.google.android.setupwizard {'1': 1580312315644, '6': 1033286588
2020-01-29 15:38:35		com.google.android.setupwizard/com.google.android.setupwizard.WizardManagerActivity	UsageEventSensor	1033286588	{'1': 'com.google.android.setupwizard 0, '5': {'1': 1580312315719, '6': 10332

Device Personalization Services report

This is data stored by the reflection_gel_events.db, which shows data usage from apps to included deleted apps.

Total number of entries: 2838

Device Personalization Services located at: /Volumes/Black_Samsung_T5/Output/ALEAPP_Reports_2020-07-06_Monday_143153/temp/Pixel 3/data/data/com.google.android.as/databases/reflection_gel_events.db

Show 15 entries

Search: wickr

Timestamp	Deleted?	BundleID	From	From in Proto	Proto Full
2020-02-14 01:14:17		com.mywickr.wickr2/com.wickr.enterprise.chat.PrivateChatActivity	UsageEventSensor	1059401331	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.chat.Privat '5': {'1': 1581642857184, '6': 1059401331}, '8': 'UsageEvent
2020-02-14 01:13:06		com.mywickr.wickr2/com.wickr.enterprise.call.ui.CallActivity	UsageEventSensor	1059401331	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.call.ui.Call/ 1581642786319, '6': 1059401331}, '8': 'UsageEventSensor'
2020-02-14 01:13:04		com.mywickr.wickr2/com.wickr.enterprise.call.ui.CallActivity	UsageEventSensor	1059401331	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.call.ui.Call/ 1581642784915, '6': 1059401331}, '8': 'UsageEventSensor'
2020-02-14 01:08:12		com.mywickr.wickr2/com.wickr.enterprise.chat.PrivateChatActivity	UsageEventSensor	999122136	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.chat.Privat '5': {'1': 1581642492009, '6': 999122136}, '8': 'UsageEventS
2020-02-14 01:08:11		com.mywickr.wickr2/com.wickr.enterprise.verification.VerificationChatActivity	UsageEventSensor	999122136	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.verification.Ver '2': 0, '5': {'1': 1581642491988, '6': 999122136}, '8': 'UsageEv
2020-02-14 01:08:09		com.mywickr.wickr2/com.wickr.enterprise.dashboard.DashboardActivity			{'1': 'com.mywickr.wickr2/com.wickr.enterprise.dashboard '5': {'1': 1581642489364}, '9': ['GEL', '1']}
2020-02-14 01:08:09		com.mywickr.wickr2/com.wickr.enterprise.dashboard.DashboardActivity	UsageEventSensor	999122136	{'1': 'com.mywickr.wickr2/com.wickr.enterprise.dashboard '2': 0, '5': {'1': 1581642489404, '6': 999122136}, '8': 'UsageEv
2020-02-14 01:08:09		com.mywickr.wickr2/com.wickr.enterprise.dashboard.DashboardListActivity	UsageEventSensor	999122136	{'1':

Personalization Services

Timestamp	Deleted?	BundleID	From	From in Proto	Proto Full
2020-01-29 18:52:06	/deleted_app/_4	com.tencent.mm/com.tencent.mm.plugin.webview.ui.tools.WebViewUI	UsageEventSensor	1060387971	{'1': 'com.tencent.mm/com.tencent.mm.plugin.webvie '2': 0, '5': {'1': 1580323926306, '6': 1060387971}, '8': 'Us
2020-01-29 18:52:34	/deleted_app/_4	com.tencent.mm/com.tencent.mm.plugin.webview.ui.tools.WebViewUI	UsageEventSensor	1060387971	{'1': 'com.tencent.mm/com.tencent.mm.plugin.webvie '2': 0, '5': {'1': 1580323954563, '6': 1060387971}, '8': 'Us
2020-01-29 18:58:34	/deleted_app/_4	com.tencent.mm/com.tencent.mm.plugin.webview.ui.tools.WebViewUI	UsageEventSensor	1060387971	{'1': 'com.tencent.mm/com.tencent.mm.plugin.webvie '2': 0, '5': {'1': 1580324314585, '6': 1060387971}, '8': 'Us
2020-01-29 18:51:25	/deleted_app/_3	com.tencent.mm/com.tencent.mm.plugin.account.ui.RegByMobileRegAIOUI	UsageEventSensor	1060387971	{'1': 'com.tencent.mm/com.tencent.mm.plugin.account.ui '2': 0, '5': {'1': 1580323885494, '6': 1060387971}, '8': 'Us
2020-01-29 18:52:20	/deleted_app/_3	com.tencent.mm/com.tencent.mm.plugin.account.ui.RegByMobileRegAIOUI	UsageEventSensor	1060387971	{'1': 'com.tencent.mm/com.tencent.mm.plugin.account.ui '2': 0, '5': {'1': 1580323940912, '6': 1060387971}, '8': 'Us

Links

- Contributor list:
  - https://abrignoni.blogspot.com/2020/01/awesome-friends.html
- DFIR Resources for xLEAPP, Python, and DFIR:
  - https://abrignoni.blogspot.com/2020/07/dfir-resources.html

Thanks For Watching!

Alexis Brignoni

@AlexisBrignoni

https://abrignoni.blogspot.com

Joshua Hickman

@josh_hickman1

https://thebinaryhick.blog