

■ Data Analysis Table (ADBFieldDetective Option Table) * Blue: Option Number

Primary Category	Secondary Category	Content	ADB commands ('adb shell +')	Component (Particular Section)	Type of Timestamp	Keywords	Additional Explanation	Raw Data(example)
User Interaction (Direct user behavior) ①	App ① - 1	App Start/End	dumpsys usagstats	Last 24 hour events	YYYY-MM-DD HH:mm:ss	ACTIVITY_RESUMED ACTIVITY_STOPPED	'package': package_name 'instanceID': Activity instance tracking	time="2022-11-17 17:02:10" type=ACTIVITY_RESUMED package=com.kakao.talk class=com.kakao.talk.activity.main.MainActivity instanceId=257324370 taskRootPackage=com.kakao.talk taskRootClass=com.kakao.talk.activity.TaskRootActivity flags=0x0 time="2022-11-17 17:02:13" type=ACTIVITY_STOPPED package=com.kakao.talk class=com.kakao.talk.activity.main.MainActivity instanceId=257324370 taskRootPackage=com.kakao.talk taskRootClass=com.kakao.talk.activity.TaskRootActivity flags=0x0
		App Last Usage Information		In-memory daily stats In-memory monthly stats	YYYY-MM-DD HH:mm:ss	lastTimeUsed totalTimeUsed lastTimeComponentUsed	'package': package_name	package=com.kakaopay.app totalTimeUsed="05:57" lastTimeUsed="2023-01-31 00:49:46" totalTimeVisible="06:10" lastTimeVisible="2023-01-31 00:49:46" lastTimeComponentUsed="2023-01-31 00:49:44" totalTimeFS="00:00" lastTimeFS="1970-01-01 09:00:00" appLaunchCount=8 fgServiceLaunchCount=0
		Camera On/Off	dumpsys media.camera	Camera service events log	MM-DD HH:mm:ss	CONNECT device DISCONNECT device	'package {pkg_name}': App using camera	03-29 21:14:03 : CONNECT device 4 client for package client.pid<1495> (PID 1495, priority 200) 03-29 21:12:56 : DISCONNECT device 1 client for package com.sec.android.app.camera (PID 14358)
			dumpsys media.camera.worker (only samsung)	Dump of CameraServiceWorker COMMON Activity	YYYY-MM-DD HH:mm:ss.sss +0900	Open camera Close camera	'for {pkg_name}': App using camera	2023-05-11 15:23:03.113 +0900, Open camera(0) for com.jeyluta.timestampcamerafree 2023-05-11 15:23:18.123 +0900, Close camera(0) for com.jeyluta.timestampcamerafree
		Call Start/End	dumpsys telecom	Historical Events:	YYYY. MM. DD. {오전/오후} HH:mm:ss / HH:mm:ss.sss	'SET_ACTIVE': Call connected 'SET_DISCONNECTED': Call terminated	'AUDIO_ROUTE (Entering state ActiveEarpieceRoute/ActiveBluetoothRoute/ActiveHeadsetRoute)': audio connected to the phone's earpiece/BT_device/wired_headset 'Code: (MISSED) Reason: (210, INCOMING_MISSED)': Incoming call was not answered 'Code: (LOCAL) Reason: (200, LOCAL)': ended by local user 'Code: (REMOTE) Reason: (210, NORMAL)': ended by the remote user	CallITC@17 [2023. 5. 13. 오후 8:41:16(MT - incoming) 20:41:19.716 - AUDIO_ROUTE (Entering state ActiveEarpieceRoute):ICA.aC->CSFM.rF->CAMSM.pM_1002->CARSM.pM_SWITCH_H_FOCUS(csai)@CEQ 20:41:19.737 - SET_ACTIVE (active set explicitly):CSW.sA(cap)@CEo 20:41:29.683 - SET_DISCONNECTED (disconnected set explicitly> DisconnectCause [Code: (REMOTE) Label: () Reason: (210, NORMAL) Tone: (27) TelephonyCause: 2/-1 lmsReasonInfo: lmsReasonInfo :: {510 : CODE_USER_TERMINATED_BY_REMOTE, 210, null}]:CSW.sD(cap)@CHY
	Device ① - 2	Screen On/Off	dumpsys activity	mars history (only samsung)	MM/DD HH:mm:ss.sss	[SCR ON] [SCR OFF]	-	[05/11 15:22:53.322] [SYS] [SCR ON] [05/11 15:33:21.510] [SYS] [SCR OFF]
			dumpsys usagstats	Last 24 hour events	YYYY-MM-DD HH:mm:ss	SCREEN_INTERACTIVE SCREEN_NON_INTERACTIVE	package={pkg_name}	time="2023-01-30 16:59:58" type=SCREEN_INTERACTIVE package=android flags=0x0
		Fingerprint Registration/Deletion, Authentication Success/Failure	dumpsys fingerprint (only samsung)	log	MM/DD HH:mm:ss.sss	-	'Event Type {E / A / R}': Enroll / Action / Remove 'Event Result {M / N / U}': Match / No match / Unknown	E, com.samsung.android.biometrics.app.setting, 05/15 12:53:26.281, 05/15 12:53:50.629, 0, 8, 8, S A, com.android.systemui, 05/15 12:53:55.181, 05/15 12:53:58.852, 176, 0, 0, M A, com.android.systemui, 05/15 12:54:00.516, 05/15 12:54:03.164, 539, 0, 0, N A, com.android.systemui, 05/15 12:54:00.516, 05/15 12:54:04.490, 440, 0, 0, N A, com.android.systemui, 05/15 12:54:00.516, 05/15 12:54:05.769, 419, 0, 0, N A, com.android.systemui, 05/15 12:54:00.516, 05/15 12:54:07.149, 513, 0, 0, N A, com.android.systemui, 05/15 12:54:00.516, 05/15 12:54:08.513, 465, 0, 0, N A, com.android.systemui, 05/15 12:54:00.516, 05/15 12:54:08.523, 0, 5, 0, U R, client, 05/15 12:54:20.015, 05/15 12:54:20.015, 0, 0, 0, null
		Wi-Fi On/Off	dumpsys wifi	UserActionEvents	MM-DD HH:mm:ss.sss	EVENT_TOGGLE_WIFI_ON EVENT_TOGGLE_WIFI_OFF	'EVENT_MANUAL_CONNECT': Manually change network	01-05 13:25:17.614 eventType=EVENT_TOGGLE_WIFI_ON startTimeMillis=46801319 WifiStatus: isConnected=false isValidated=false lastRssi=0 estimatedTxKbps=0 estimatedRxKbps=0 isStuckDueToUserConnectChoice=false 01-05 13:26:21.294 eventType=EVENT_TOGGLE_WIFI_OFF startTimeMillis=46864999 isEphemeral=false isPasspoint=false WifiStatus: isConnected=true isValidated=true lastRssi=-68 estimatedTxKbps=232527 estimatedRxKbps=110144 isStuckDueToUserConnectChoice=false NetworkDisableReason: DisableReason=15 configTemporarilyDisabled=false configPermanentlyDisabled=true bssidDisableReasons=[] 01-05 13:25:35.282 eventType=EVENT_MANUAL_CONNECT startTimeMillis=46818987 isEphemeral=false isPasspoint=false WifiStatus: isConnected=false isValidated=false lastRssi=0 estimatedTxKbps=0 estimatedRxKbps=0 isStuckDueToUserConnectChoice=false NetworkDisableReason: DisableReason=15 configTemporarilyDisabled=false configPermanentlyDisabled=true bssidDisableReasons=[]

Primary Category	Secondary Category	Content	ADB commands ('adb shell +')	Component (Particular Section)	Type of Timestamp	Keywords	Additional Explanation	Raw Data(example)
		Wi-Fi On/Off	dumpsys wifi	wificonnectivity manager	YYYY-MM-DD THH:mm:ss.ssssss	Set WiFi disabled Set WiFi enabled	'prepareForForcedConnection': Manually change network	2023-01-05T13:26:21.606548 - Set WiFi disabled 2023-01-05T13:26:46.948977 - Set WiFi enabled 2023-01-05T13:25:58.672099 - prepareForForcedConnection: SSID="DFRC_5G" # All data is recorded 1-4 seconds late. (Same for dumpsys wifi)
		Bluetooth On/Off	dumpsys bluetooth_ manager	Log (only samsung)	MM-DD HH:mm:ss.sss	USER_TURN_ON BLE_STOPPED	-	05-09 21:48:27.816--AdapterState Current state: BT ON, message: USER_TURN_OFF 01-01 21:13:01.401--AdapterState Current state: Turning BLE OFF, message: BLE_STOPPED
				Enable log	MM-DD HH:mm:ss	com.android.systemui	* 'com.android.systemui': not necessarily by the user	05-22 12:40:24 Enabled due to APPLICATION_REQUEST by com.google.android.gms 05-22 12:40:24 Enabled due to APPLICATION_REQUEST by com.android.systemui
			dumpsys telecom	CallsManager-BluetoothDeviceManager	YYYY-MM-DD THH:mm:ss.ssssss	Device connected Device disconnected	'address: {BT_MAC_Address}'	2022-12-20T23:09:30.380353 - Device connected -- address: C8:BD:4D:98:##:## isHeadingAid: false 2022-12-20T23:30:49.298957 - Device disconnected -- address: C8:BD:4D:98:##:## isHeadingAid: false
		Charger Connection/Disconnection	dumpsys batterystats	BatteryHistory	+(HH)h(mm)m(ss)s(sss) ms (Elapsed time since reference time)	status=charging status=discharging	'plug=ac': AC charging 'plug=usb': USB charging 'plug=wireless': Wireless charging	+11h36m10s476ms (7) 059 status=charging plug=ac temp=287 volt=3870 txshare_event=0x0 online=3 current_event=0x40000001 misc_event=0x10000 +11h38m05s335ms (6) 061 status=discharging health=unknown plug=none temp=315 volt=4122 txshare_event=0x0 online=6 current_event=0x40000004 misc_event=0x10000 charge=2772 ~plugged # Able to identify the type of plug
		USB Connection/Disconnection	dumpsys activity b	Historical broadcasts summary [foreground]	YYYY-MM-DD HH:mm:ss.ssssss	USB_PORT_CHANGED	'connected={true/false}': USB connection/disconnection 'currentMode=utf': MTP mode (Additional research needed) # 'extras: Bundle[{data}]': Varies by device availability.	#6: act=android.hardware.usb.action.USB_PORT_CHANGED flg=0x11000010 (has extras) +1ms dispatch 0 finish enq=2023-05-15 20:49:45.860 disp=2023-05-15 20:49:45.861 fin=2023-05-15 20:49:45.861 extras: Bundle[{portStatus=UsbPortStatus(connected=true, currentMode=utf, currentPowerRole=sink, currentDataRole=device, supportedRoleCombinations=[source:host, sink:device], contaminantDetectionStatus=0, contaminantProtectionStatus=0), port=android.hardware.usb.ParcelableUsbPort@b9e8331}]
	Anti-forensics ① - 3	Factory Reset, Reboot	getprop	persist.sys.boot.reason.history ro.boot.bootreason sys.boot.reason sys.boot.reason.last	Unix Timestamp(sec)	reboot,factory_reset reboot,userrequested	'userrequested': User-requested manual reboot" 'reboot,ota': Automatic reboot due to update or other reasons 'cold': No record	# Factory Reset reboot,factory_reset,1677488147,reboot,1677488033 reboot,factory_reset reboot,factory_reset reboot # Reboot reboot,userrequested,1677466067, reboot,factory_reset,1668480912 reboot,userrequested reboot,userrequested reboot,userrequested
		App Deletion Information	dumpsys activity b	Historical broadcasts summary [backgroud]	YYYY-MM-DD HH:mm:ss.ssssss	PACKAGE_REMOVED	'dat=package:{pkg_name}' # The package_name is not displayed in Android 13.	#59: act=android.intent.action.PACKAGE_REMOVED dat=package:com.lgplus.navi flg=0x4000010 (has extras) +56ms dispatch +6ms finish enq=2023-05-03 19:42:21.009 disp=2023-05-03 19:42:21.065 fin=2023-05-03 19:42:21.071
		Reboot Record	dumpsys sdhms	CONFIG LIST	YYYY-MM-DD THH:mm:ss	BOOT_COMPLETED	-	87 [2023-01-17 17:33:13] 55 0 BOOT_COMPLETED
		Last Boot Time	uptime	-s	YYYY-MM-DDTHH:mm:ss	-	-	2023-02-27 19:08:14
User Data (Result of user behavior) ②	Call ② - 1	Call Start/End (+Incoming/Outgoing, End Reason)	dumpsys telecom	Analytics:	Unix Timestamp(millisecc)	Call TC@{number}	'startTime: {start_ts}': Call start time('0' if connection fails) 'endTime: {end_ts}': Call end time 'direction: {OUT/IN}': Call direction 'Reason: ({200 / 210}': 200 → Owner ended / 210 → Other ended	Call TC@111: startTime: 1675145236312 endTime: 1675145304795 direction: OUTGOING callTerminationReason: DisconnectCause [Code: (LOCAL) Label: () Description: () Reason: (200, LOCAL) Tone: (27) TelephonyCause: 3/-1 lmsReasonInfo: lmsReasonInfo :: {501 : CODE_USER_TERMINATED, 200, null}] #Omitted unnecessary parts from the original
		Call Start/Duration (+Contact Number, Saved Contact Name)	content query --uri content://call_log/calls	-	Unix Timestamp(millisecc)	ROW: {number}	'type: {call_type}': Call type (1-5: incoming, outgoing, missed, voicemail, reject) 'duration: {num}': Call duration in seconds	Row: 0 date=1683789022642 type=5, duration=0, number=0105081####, _id=167 #Omitted unnecessary parts from the original

Primary Category	Secondary Category	Content	ADB commands ('adb shell +')	Component (Particular Section)	Type of Timestamp	Keywords	Additional Explanation	Raw Data(example)
	Message ② - 2	SMS and MMS Send/Receive, Send Time, Content	content query --uri content://	sms	Unix Timestamp (millisec)	-	'type={1 / 2}': Received / Sent	address=0108840####, date=1677580382325, body=##### 고객님의 상품(5714570621#)이 배송되었습니다.▶인수자(위탁):문앞, type=1 # Omitted unnecessary parts from the original
				mms	Unix Timestamp (sec)	-	'msg_box={1 / 2}': Received / Sent 'sub': encoded strings 'm_size': bytes	date=1684413598, msg_box=2, read=1, sub=<i>\x90i\x9d i\x8aci\x8aci\x84°e\x94\x94>, , m_size=576355, # Omitted unnecessary parts from the original
	Wi-Fi ② - 3	Wi-Fi Connection Completion/Disconnection	dumpsys wifi	WifiClientModelImpl (Mutiple exist)	MM-DD HH:mm:ss.sss / Unix Timestamp (millisec)	NETWORK_CONNECTION_EVENT NETWORK_DISCONNECTION_EVENT	'reasonCode: {num}': Disconnection reason (1 Network issue / 3 User termination)	rec[10]: time=01-05 13:25:36.007 processed=ConnectingOrConnectedState org=L2ConnectingState dest=L3ProvisioningState what=NETWORK_CONNECTION_EVENT screen=on 10 false 70:5d:cc:b3:##:## nid=10 "DFRC_2.4G"WPA_PSK last="DFRC_2.4G"WPA_PSK rec[25]: time=01-05 13:27:15.376 processed=L3ConnectedState org=L3ConnectedState dest=DisconnectedState what=NETWORK_DISCONNECTION_EVENT screen=on ssid: "DESKTOP-ACING84 1013" bssid: 06:ea:56:7c:##:## reasonCode: 3
		Past Connected Wi-Fi Information		WifiConfigManager - Configured networks Begin		SSID: "{network_name}" lastConnected: {timestamp}	'numRebootsSinceLastUse':The number of reboots since the last use	ID: 9 SSID: "DESKTOP-ACING84 1013" PROVIDER-NAME: null BSSID: null FQDN: null HOME-PROVIDER-NETWORK: false PRIO: 0 HIDDEN: false PMF: falseCarrierId: -1SubscriptionId-1 NetworkSelectionStatus NETWORK_SELECTION_ENABLED connect choice: "DFRC_2.4G"WPA_PSK connect choice rssi: -60 hasEverConnected: true hasNeverDetectedCaptivePortal: true numAssociation 1 validatedInternetAccess shared trusted macRandomizationSetting: 3 mRandomizedMacAddress: 8a:a7:85:66:##:## randomizedMacExpirationTimeMs: 01-06 13:26:50.749 (omitted for brevity) lastConnected: 01-05 13:26:50.767 numRebootsSinceLastUse: 0 recentFailure: Association Rejection code: 0, last update time: 0
		Wi-Fi Connection Record		WifiMetrics		SSID="{network_name}" BSSID={##:##:##:##:##:##}	'durationMillis': The duration of the connection in milliseconds 'wifiState={WIFI_DISCONNECTED / WIFI_ASSOCIATED}': Turned on from off / Network transition	startTime=05-15 15:39:50.213, SSID="DFRC_5G", BSSID=70:5d:cc:b3:48:3c, durationMillis=1066, connectionResult=1, wifiState=WIFI_DISCONNECTED, screenOn=true, useRandomizedMac=true, networkType=TYPE_WPA3, interfaceName=wlan0, isFirstConnectionAfterBoot=true # Omitted unnecessary parts from the original
		Recent Scanned SSID/BSSID		WifiNetworkScoreCache (only android12)		"{SSID}"{BSSID}	-	"KoreaUniv AP"64:a0:e7:f9:##:##: -128 "eduroam"64:a0:e7:f9:##:##: -128
		Last Scanned Wi-Fi Information	dumpsys sem_wifi (only samsung)	scanpool:		SSID: {network_name} BSSID: {##:##:##:##:##:##}	'timestamp:' microseconds since initial scanner detection	SSID: iptime101, BSSID: 70:5d:cc:##:##:de, capabilities: [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS][WPS], level: -90, frequency: 2437, timestamp: 1204980544256, (omitted for brevity)
	Bluetooth ② - 4	Connected Bluetooth Device Information	dumpsys bluetooth_manager	AdapterProperties- Bonded devices, Restored devices	-	Bonded devices Retored devices	'[BR/EDR]': Bluetooth mode for continuous connections '[DUAL]': Devices supporting both key Bluetooth modes(LE mode and BR/EDR mode)	Bonded devices: C8:BD:4D:98:##:## [BR/EDR] Galaxy Buds2 (2472) (omitted for brevity) (Connected) 58:A6:39:F5:##:## [DUAL] Galaxy Watch4 (969V) (omitted for brevity) 68:84:70:2C:##:## [BR/EDR] NIRO (Handsfree,AudioSink,AvrcpController) Restored devices: E8:E8:B7:6C:##:## [BR/EDR] CARNIVAL
		Bluetooth History	dumpsys bluetooth_manager	Log (only samsung)	MM-DD HH:mm:ss.sss	-	'message: {USER_TURN_ON/USER_TURN_OFF}' 'BTCS-{create/destroy}' 'HFIF- {connect_audio/disconnect_audio}' # All logs do not specifically determine the phone's call connection status # If BT is turned on, the BTCS logs are recorded even if not connected to a device	12-18 14:41:35.908--AdapterState Current state: BLE ON, message: USER_TURN_ON 12-21 14:33:26.762--BTCS-create 12-21 23:04:50.699-HFIF-disconnect_audio([1] c8bd4d_2) # Omitted unnecessary parts from the original

Primary Category	Secondary Category	Content	ADB commands ('adb shell +')	Component (Particular Section)	Type of Timestamp	Keywords	Additional Explanation	Raw Data(example)
	Account ② - 5	Logged Account Information (Partial)	dumpsys account	User UserInfo-Accounts:	-	Accounts:	-	Account {name=khc####@gmail.com, type=com.google} Account {name=khc####@kakao.com, type=com.toast.android.paycoaccount}
	Location ② - 6	Last Location Information	dumpsys location	Location Provider	+(DD)d(HH)h(mm)m(ss)s(sss)ms (Elapsed time since reference time)	last location=Location	'hAcc': Altitude error(smaller value = more accurate altitude) 'vAcc': Location error(smaller value = more precise location) 'et': Fix time estimate(smaller value = faster fix acquisition)	Location Providers: passive provider: last location=Location[network 37.581703,127.026459 hAcc=14.078 et=+1d18h4m52s181ms alt=58.400001525878906 vAcc=2.0450206 {Bundle[mParcelledData.dataSize=68]}] network provider: last location=Location[network 37.581703,127.026459 hAcc=14.078 et=+1d18h4m52s181ms alt=58.400001525878906 vAcc=2.0450206 {Bundle[mParcelledData.dataSize=68]}] fused provider: last location=Location[fused 37.581703,127.026459 hAcc=14.078 et=+1d18h4m52s181ms alt=58.400001525878906 vAcc=1.3145491] gps provider: last location=Location[gps 37.581963,127.026420 hAcc=128.0 et=+1d17h48m38s807ms alt=1.9319239231975636 vAcc=74.200386 vel=0.0 sAcc=1.0611838 {Bundle[{satellites=8, maxCn0=34, meanCn0=27}]]} (Some unnecessary data omitted for brevity)
		Nearby Network Router Information (Scanned but not connected)	dumpsys wifi	wificonnectivity manager	YYYY-MM-DDT HH:mm:ss.sss	Networks filtered out due to low signal strength	'{SSID}:{MAC address}({frequency})-{RSSI}'	2023-02-28T14:37:19.014 - Networks filtered out due to low signal strength: eduroam:00:f2:8b:83:##:##(5GHz)-77 / KoreaUniv AP:00:f2:8b:83:##:##(5GHz)-77 / eduroam:f4:1f:c2:5b:##:##(5GHz)-90 / AT_504_HWWA9K_F2_7cb2:4c:bc:e9:c5:##:##(2.4GHz)-81 / KoreaUniv AP:f4:1f:c2:5b:##:##(5GHz)-90 / 666:58:d9:d5:8b:##:##(2.4GHz)-87 / PET-5G:58:86:94:a5:##:##(5GHz)-90 / SK_WiFiGIGA675E_2.4G:42:23:aa:58:##:##(2.4GHz)-86 / PET-server:58:86:94:a5:##:##(2.4GHz)-83 / beautiful2:80:ca:4b:6b:##:##(2.4GHz)-87 / SK_WiFiGIGA00DC:00:23:aa:bc:##:##(2.4GHz)-84 / SK_WiFiGIGA00DC_2.4G:42:23:aa:bc:##:##(2.4GHz)-84 / ailab-ex:58:86:94:49:##:##(2.4GHz)-86 / jinmo:e8:48:b8:9b:##:##(2.4GHz)-84
	App Package ② - 7	Package Usage Summary Information	dumpsys sdhms (only samsung)	Process usage summary	MM-DD HH:mm:ss	-	-	[12-20 22:04:23 ~ 12-20 22:16:21] uid pid usage (%) Package Name 1000 650 12.69 android.system.suspend@1.0-service 10318 29572 11.91 com.kakao.talk 1000 1371 8.48 system_server 10041 1808 3.67 com.android.systemui 0 540 2.04 ueventd
		Package Process End Time	dumpsys activitiy	activity exit-info	YYYY-MM-DD HH:mm.ss.sss	ApplicationExitInfo	package: {pkg_name}	package: com.google.android.apps.youtube.music Historical Process Exit for uid=10449 ApplicationExitInfo #0: timestamp=2022-12-20 23:01:00.707
		Recent Specific Period Package Foreground Duration (Battery Usage Order)	dumpsys sdhms (only samsung)	Batterystats Collector	(HH)h(mm)m(ss)s	-	-	UID POWER Foreground Time Background Time Package Name 10318 1411.64 1h 54m 37s 13h 17m 38s com.kakao.talk 10311 1105.30 1h 56m 18s 3h 37m 33s com.sec.android.app.sbrowser
		Package Capacity	dumpsys diskstats	log	-	-	-	Package Name: com.korail.talk Package Size=26105344 bytes Data Size=13758464 bytes Cache Size=8835072 bytes Total Size=48698880 bytes # The data format after normalization
		Last Access Record of	dumpsys dbinfo	Applications Database	YYYY-MM-DDT	Database files in {path of	'ctime': Change Time(last modification	KakaoTalk2.db 15183872b ctime=2023-02-08T06:36:03Z

Primary Category	Secondary Category	Content	ADB commands ('adb shell +')	Component (Particular Section)	Type of Timestamp	Keywords	Additional Explanation	Raw Data(example)	
		Database		Info:	HH:mmZ	db file}	time of file attributes) 'mtime': Modified Time(last modification time of file content) 'atime': Access Time(last access time of the file)	mtime=2023-02-08T06:36:03Z atime=2022-05-17T07:05:15Z	
		Executed Database List			YYYY-MM-DD HH:mm.ss.sss	Most recently executed operations	-	Most recently executed operations: 9: [2022-12-20 20:57:38.073] [Pid:(2730)]executeForCursorWindow took 0ms - succeeded, sql="SELECT profileId, packageName, lastUpdated, version, theme, size FROM shortcut_and_widget_previews", path=/data/user/0/com.sec.android.app.launcher/databases/widgetpreviews.db	
Device Info ③	Hardware Information ③ - 1	Manufacturer	getprop	ro.product.manufacturer	-	-	-	samsung	
		Model Name		ro.product.model	-	-	-	SM-N971N	
		Serial Number		ro.serialno	-	-	-	R3CN102Z8PL	
	Software Country	ro.csc.country_code		-	-	-	Korea		
	Android Version	ro.build.version.release		-	-	-	12		
	OS Information ③ - 2	USB Settings		persist.sys.usb.config	-	-	'mtp': Media file transfer. 'conn_gadget': USB tethering. 'adb': Debugging and command execution.	mtp.conn_gadget.adb	
		Firmware Version		gms.version.baseband	-	-	-	N971NKO2HWP1	
		Encryption Method		ro.crypto.type	-	-	-	file	
		Bootloader Version		ro.boot.bootloader	-	-	-	N971NKSU2HWP1	
		Security Patch Date		ro.build.version.security_patch	YYYY-MM-DD	-	-	2023-02-01	
		UTC Time Zone		persist.sys.timezone	-	-	-	'Asia/Seoul'	
		Mobile Phone Time		date	+"%Y-%m-%d-%A"	YYYY-MM-DD HH:mm.ss	-	-	2023-02-27 19:08:14
	Package Information ③ - 3	List of All Installed Packages		pm list packages -f -u	-	-	-	'package:{the path of APK file}={pkg_name}	package:/data/app/~1ToCtJkmvcUONc_JFNMIGA=/com.samsung.android.vtca merasettings-
	Network Basic Information ③ - 4	WiFi Name		settings	get global device_name	-	-	-	Galaxy Note10 5G
Bluetooth Name, MAC Address		settings	get secure bluetooth_name get secure bluetooth_address	-	-	-	Galaxy Note10 5G 74:9E:F5:7F:##:##		
screen Information ③ - 5	Screen activation status	dumpsys wifi	WifiClientModelImpl	MM-DD HH:mm:ss.sss	screen={on/off}	'screen': Indicates screen status at a given time, not user intent.	rec[0]: time=11-21 19:26:24.292 processed=ConnectableState org=DisconnectedState dest=<null> what=CMD_RESET_SIM_NETWORKS screen=off 2 0 rec[1]: time=11-21 19:26:24.453 processed=ConnectableState org=DisconnectedState dest=<null> what=what:131372 screen=on 0 0		
User Files ④	Documents	*.hwp and 16 Other Types	adb backup	-all -shared -system -apk -f	YYYY:MM:DD HH:mm:ss	-	-	\".hwp\", \"doc\", \"docx\", \"ppt\", \"pptx\", \"xls\", \"xlsx\", \"pdf\", \"txt\", \"rtf\", \"csv\", \"odt\", \"odp\", \"ods\", \"pages\", \"key\", \"numbers\", \"mp4\", \"3gp\", \"mkv\", \"mov\", \"avi\", \"flv\", \"wmv\", \"m4v\", \"mpeg\", \"mpg\", \"vob\", \"rm\", \"swf\", \"mp3\", \"m4a\", \"aac\", \"wav\", \"ogg\", \"flac\", \"alac\", \"wma\", \"opus\", \"amr\", \"jpg\", \"jpeg\", \"png\", \"bmp\", \"gif\", \"webp\", \"tiff\", \"ico\", \"raw\", \"svg\", \"psd\", \"zip\", \"rar\", \"tar\", \"gz\", \"7z\", \"bz2\", \"xz\", \"iso\", \"tar.gz\", \"tar.bz2	
	Videos	*.mp4 and 12 Other Types							
	Audios	*.mp3 and 9 Other Types							
	Images	*.jpg and 10 Other Types							
	Others	9 Types							

■ Volatility Analysis Table (ADBFieldDetective Volatility Table)
 * Blue: Option Number

Primary Category	Secondary Category	Content	ADB commands ('adb shell +')	Component (Particular Section)	Storage Duration	Storage Capacity Limit	Reboot Resistance	Remarks
User Interaction (Direct user behavior) ①	App ① - 1	App Start/End	dumpsys usagstats	Last 24 hour events	24h	-	O	-
		App Last Usage Information		In-memory daily stats In-memory monthly stats	Under 1 day Under 1 month	-	O	Approximately 12 hours Approximately 10 days
		Camera On/Off	dumpsys media.camera	Camera service events log	-	100 lines	X	-
			dumpsys media.camera.worker (only samsung)	Dump of CameraServiceWorker COMMON Activity	1+ months	600+ lines	X	-
		Call Start/End (+Recording/Speakerphone/Bluetooth Usage, End Reason)	dumpsys telecom	Historical Events:	-	20 records	X	-
	Device ① - 2	Screen On/Off	dumpsys activity	mars history (only samsung)	-	5000 Lines	X	-
			dumpsys usagstats	Last 24 hour events	24 hours	-	O	-
		Fingerprint Registration/Deletion, Authentication Success/Failure	dumpsys fingerprint (only samsung)	log	-	20 lines	X	-
		Wi-Fi On/Off	dumpsys wifi	UserActionEvents:	2+ months	130+ lines	X	Additional research needed
		Wi-Fi On/Off	dumpsys wifi	wificonnectivity manager	-	1024 lines	X	Remove past records after reaching 1024 lines
		Bluetooth On/Off	dumpsys bluetooth_manager	Log	1 week to 2 month (Subject to usage)	-	O	-
				Enabled	-	20 lines	X	-
		Charger Connection/Disconnection	dumpsys batterystats	CallsManager-BluetoothDeviceManager	-	20 lines	X	-
				BatteryHistory	Reset when fully charged	-	O	Further research required
		USB Connection/Disconnection	dumpsys activity b	Historical broadcasts summary [foreground]	-	300 records	X	-
	Anti-forensics ① - 3	Factory Reset, Reboot	getprop	persist.sys.boot.reason.history ro.boot.bootreason sys.boot.reason sys.boot.reason.last	-	-	-	Last reboot reason recorded
		App Deletion Information	dumpsys activity b	Historical broadcasts summary [foreground]	-	300 records	X	-
		Reboot Record	dumpsys sdhms	CONFIG LIST	-	-	-	All data retained after reset
		Last Boot Time	uptime	-s	-	-	-	Latest boot time
User Data (Result of user behavior) ②	Call ② - 1	Call Start/End (+Incoming/Outgoing, End Reason)	dumpsys telecom	Analytics:	-	100+ records	X	-
		Call Start/Duration (+Contact Number, Saved Contact Name)	content query --uri content://	call_log/calls	-	-	O	Untile deleted from the UI
	Message ② - 2	SMS and MMS Send/Receive, Send Time, Content	content query --uri content://	sms, mms	-	-	-	Untile deleted from the UI
	Wi-Fi ② - 3	Wi-Fi Connection Completion/Disconnection	dumpsys wifi	WifiClientModelmpl: (Mutiple exist)	-	100 records	X	-
		Past Connected Wi-Fi Information		WifiConfigManager - Configured networks Begin ----	-	-	O	-
		Wi-Fi Connection Record		WifiMetrics:	Before reboot (estimated)	-	X	2+ months of research
		Recent Scanned SSID/BSSID		WifiNetworkScoreCache (only android12)	-	-	O	Before reset
		Last Scanned Wi-Fi Information	dumpsys sem_wifi	scanpool:	Before reboot (estimated)	-	X	-

Primary Category	Secondary Category	Content	ADB commands ('adb shell +')	Component (Particular Section)	Storage Duration	Storage Capacity Limit	Reboot Resistance	Remarks	
	Bluetooth ② - 4	Connected Bluetooth Device Information	dumpsys bluetooth_manager	AdapterProperties	-	-	-	All data retained after reset	
		Bluetooth History	dumpsys bluetooth_manager	log	3+ weeks	13,000+ lines	0	Additional research needed	
	Account ② - 5	Logged Account Information (Partial)	dumpsys account	User UserInfo	-	-	0	before account logout	
	Location ② - 6	Last Location Information	dumpsys location	Location Provider	-	-	X	-	
		Nearby Network Router Information (Scanned but not connected)	dumpsys wifi	wificonnectivity manager	-	1024Line (overlap)	X	-	
	App Package ② - 7	Package Usage Summary Information	dumpsys sdhms (only samsung)	Process usage summary	1.5 hours	-	0	-	
		Package Process End Time	dumpsys activity	activity exit-info	-	Recent 15 items per package	0	-	
		Recent Specific Period Package Foreground Duration (Battery Usage Order)	dumpsys sdhms (only samsung)	Batterystats Collector	Data within 48 hours (based on dumping time)	-	0	-	
		Package Capacity	dumpsys diskstats	log	-	-	0	-	
		Last Access Record of Database	dumpsys dbinfo	Applications Database Info:	-	-	0	checking	
		Executed Database List			-	-	0		
	Device Info ③	Hardware Information ③ - 1	Manufacturer	getprop	ro.product.manufacturer	-	-	0	-
Model Name			ro.product.model		-	-	0	-	
Serial Number			ro.serialno		-	-	0	-	
OS Information ③ - 2		Software Country	ro.csc.country_code		-	-	0	-	
		Android Version	ro.build.version.release		-	-	0	-	
		USB Settings	persist.sys.usb.config		-	-	0	-	
		Firmware Version	gms.version.baseband		-	-	0	-	
		Encryption Method	ro.crypto.type		-	-	0	-	
		Bootloader Version	ro.boot.bootloader		-	-	0	-	
		Security Patch Date	ro.build.version.security_patch		-	-	0	-	
		UTC Time Zone	persist.sys.timezone		-	-	0	-	
		Mobile Phone Time	date		+%Y-%m-%d-%A"	-	-	0	-
		Package Information ③ - 3	List of All Installed Packages		pm list packages -f -u	-	-	0	-
Network Basic Information ③ - 4		WiFi Name	settings		get global device_name	-	-	0	-
		Bluetooth Name, MAC Address	settings		get secure + bluetooth_address, bluetooth_name	-	-	0	-
screen Information ③ - 5		Screen activation status	dumpsys wifi		WifiClientModelImpl	-	100 records	X	-
User Files ④	Documents	*.hwp and 16 Other Types	adb backup	-all -shared -system -apk -f	-	-	0	Data unrecoverable after deletion	
	Videos	*.mp4 and 12 Other Types							
	Audios	*.mp3 and 9 Other Types							
	Images	*.jpg and 10 Other Types							
	Others	9 Types							