CYFI 330 / 700 Mobile Forensics

Package .XML from Android Phone

Under the Guidance of

Melvin de la Cruz

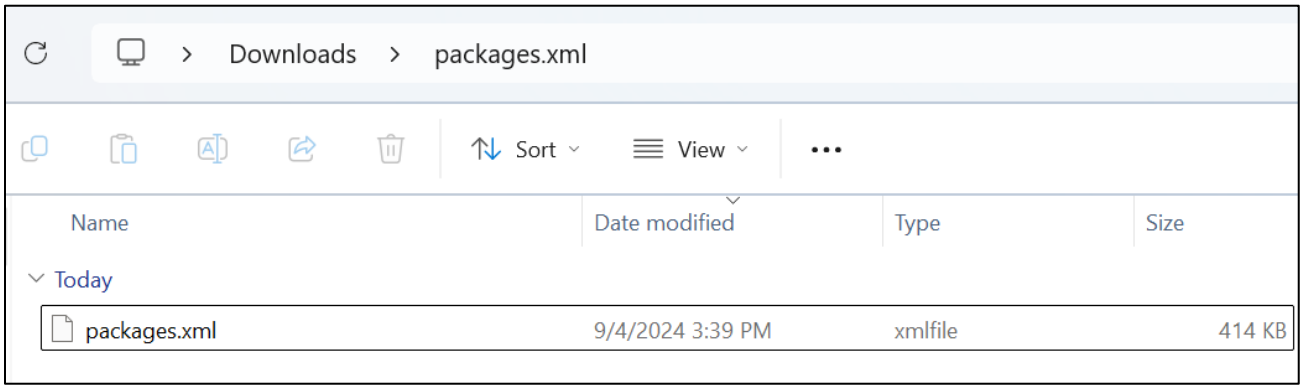
Assignment/Work by

Jeel Khatiwala

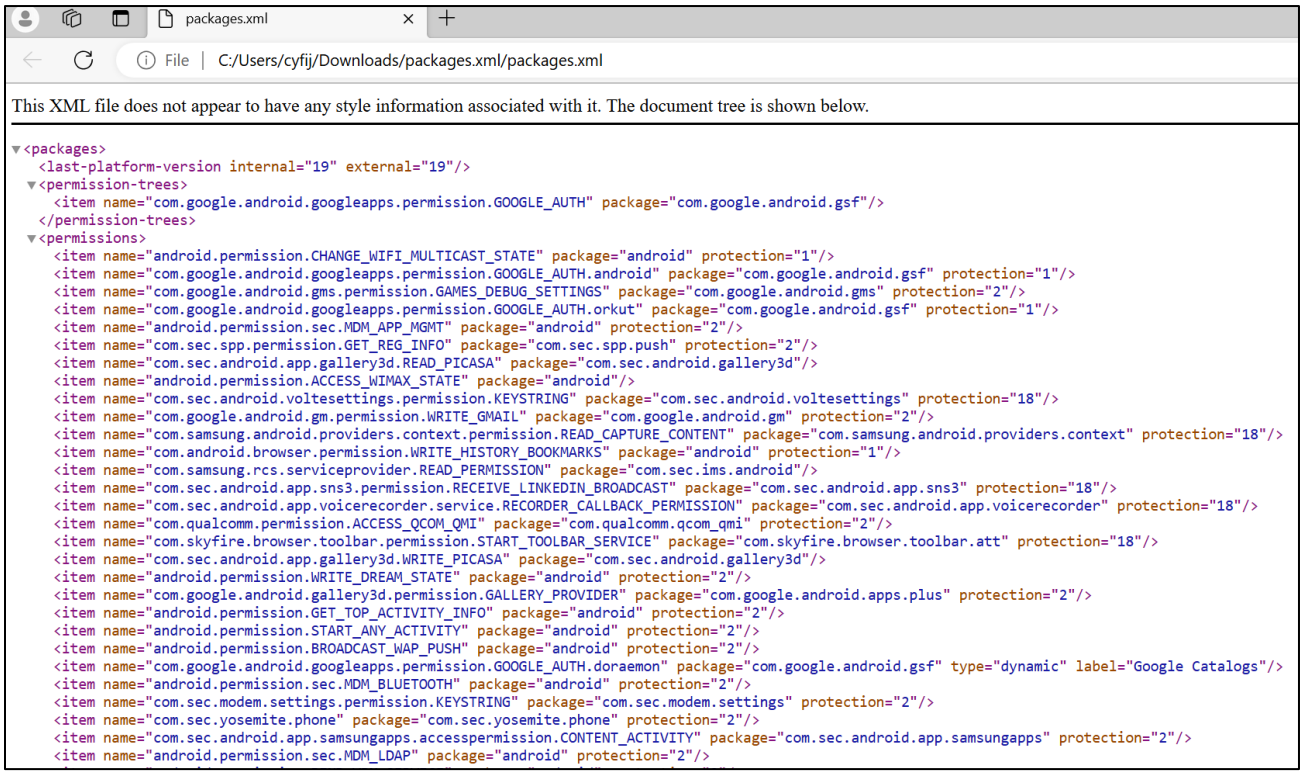
❖ Examination of Packages.xml from an Android Phone

- **Instruction steps:**

Download and extract the file packages.xml from the compressed file and place it on the desktop:



View the XML File on browser




```
<packages>
  <last-platform-version internal="19" external="19"/>
  <permission-trees>
    <item name="com.google.android.googleapps.permission.GOOGLE_AUTH" package="com.google.android.gsf"/>
  </permission-trees>
  <permissions>
    <item name="android.permission.CHANGE_WIFI_MULTICAST_STATE" package="android" protection="1"/>
    <item name="com.google.android.googleapps.permission.GOOGLE_AUTH.android" package="com.google.android.gsf" protection="1"/>
    <item name="com.google.android.gms.permission.GAMES_DEBUG_SETTINGS" package="com.google.android.gms" protection="2"/>
    <item name="com.google.android.googleapps.permission.GOOGLE_AUTH.orkut" package="com.google.android.gsf" protection="1"/>
    <item name="android.permission.sec.MDM_APP_MGMT" package="android" protection="2"/>
    <item name="com.sec.spp.permission.GET_REG_INFO" package="com.sec.spp.push" protection="2"/>
    <item name="com.sec.android.app.gallery3d.READ_PICASA" package="com.sec.android.gallery3d"/>
    <item name="android.permission.ACCESS_WIMAX_STATE" package="android"/>
    <item name="com.sec.android.voltesettings.permission.KEYSTRING" package="com.sec.android.voltesettings" protection="18"/>
    <item name="com.google.android.gm.permission.WRITE_GMAIL" package="com.google.android.gm" protection="2"/>
    <item name="com.samsung.android.providers.context.permission.READ_CAPTURE_CONTENT" package="com.samsung.android.providers.context" protection="18"/>
    <item name="com.android.browser.permission.WRITE_HISTORY_BOOKMARKS" package="android" protection="1"/>
    <item name="com.samsung.rcs.serviceprovider.READ_PERMISSION" package="com.sec.ims.android"/>
    <item name="com.sec.android.app.sns3.permission.RECEIVE_LINKEDIN_BROADCAST" package="com.sec.android.app.sns3" protection="18"/>
    <item name="com.sec.android.app.voicerecorder.service.RECORDER_CALLBACK_PERMISSION" package="com.sec.android.app.voicerecorder" protection="18"/>
    <item name="com.qualcomm.permission.ACCESS_QCOM_QMI" package="com.qualcomm.qcom_qmi" protection="2"/>
    <item name="com.skyfire.browser.toolbar.permission.START_TOOLBAR_SERVICE" package="com.skyfire.browser.toolbar.att" protection="18"/>
    <item name="com.sec.android.app.gallery3d.WRITE_PICASA" package="com.sec.android.gallery3d"/>
    <item name="android.permission.WRITE_DREAM_STATE" package="android" protection="2"/>
    <item name="com.google.android.gallery3d.permission.GALLERY_PROVIDER" package="com.google.android.apps.plus" protection="2"/>
    <item name="android.permission.GET_TOP_ACTIVITY_INFO" package="android" protection="2"/>
    <item name="android.permission.START_ANY_ACTIVITY" package="android" protection="2"/>
    <item name="android.permission.BROADCAST_WAP_PUSH" package="android" protection="2"/>
    <item name="com.google.android.googleapps.permission.GOOGLE_AUTH.doraemon" package="com.google.android.gsf" type="dynamic" label="Google Catalogs"/>
    <item name="android.permission.sec.MDM_BLUETOOTH" package="android" protection="2"/>
    <item name="com.sec.modem.settings.permission.KEYSTRING" package="com.sec.modem.settings" protection="2"/>
    <item name="com.sec.yosemite.phone" package="com.sec.yosemite.phone" protection="2"/>
    <item name="com.sec.android.app.samsungapps.accesspermission.CONTENT_ACTIVITY" package="com.sec.android.app.samsungapps" protection="2"/>
    <item name="android.permission.sec.MDM_LDAP" package="android" protection="2"/>
```

Permission for com.surpax.ledflashlight.panel

Normal Permission:

- **android.permission.FLASHLIGHT:** Necessary for controlling the device's flashlight, typical for a flashlight app.
- **android.permission.CAMERA:** Required to access the camera hardware, which often controls the flashlight.
- **android.permission.WAKE_LOCK:** Prevents the device from sleeping while the flashlight is in use, ensuring continuous operation.

Unusual Permission for flashlight:

- **android.permission.READ_PHONE_STATE:** Unusual for a flashlight app; allows access to phone status, possibly for tracking or data collection.
- **android.permission.READ_EXTERNAL_STORAGE and android.permission.WRITE_EXTERNAL_STORAGE:** Allows the app to read and write files on the device’s storage, which is not typically needed for a flashlight.
- **android.permission.INTERNET & android.permission.ACCESS_NETWORK_STATE:** Provides internet access, which is suspicious for a flashlight app unless it's ad-supported.
- **android.permission.GET_TASKS:** Enables the app to monitor running tasks, potentially for tracking user activity, which is concerning.
- **Custom Permissions (com.surpax.ledflashlight.panel.permission.C2D_MESSAGE, com.google.android.c2dm.permission.RECEIVE):** Related to receiving push notifications, which is unusual for a basic flashlight app.

Additional Exercise:

Examine the Packages.xml file. What are the permissions associated with com.roidapp.photogrid?

Permissions:

- **android.permission.READ_EXTERNAL_STORAGE:** Grants the app access to photos and other files on the device, which is common for an app that edits or organizes images.
- **android.permission.GET_TASKS:** This permission allows the app to view active or recently closed apps, which is atypical for a photo editing app and could suggest potential user activity tracking.

  This permission allows the app to view information about currently or recently running apps on the device. While not inherently malicious, it's unusual for a photo editing app to need this level of access, as it's not directly related to its core functionality. This could indicate that the app is monitoring user activity, which could be seen as an overreach or a privacy concern.

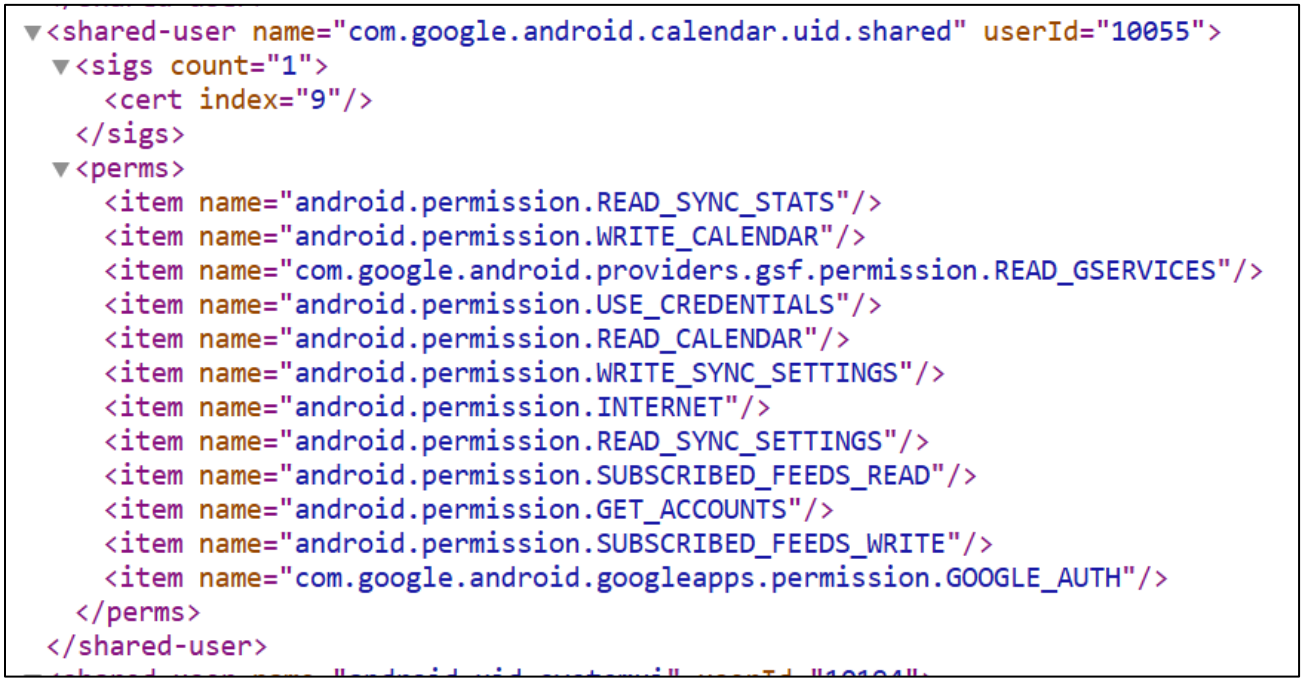
- **com.android.vending.BILLING:** Necessary for processing in-app purchases, which is typical for apps offering paid features or content.
- **android.permission.WRITE_EXTERNAL_STORAGE:** Lets the app save edited images and other data to the device, expected functionality for a photo editing tool.
- **android.permission.INTERNET:** Needed for downloading resources, syncing, or sharing content online, which aligns with common features in photo apps.

- **android.permission.VIBRATE:** Controls the device's vibration feature, likely used for providing feedback during interactions like saving or sharing photos.
- **android.permission.ACCESS_WIFI_STATE:** Allows the app to check Wi-Fi connectivity, which helps manage network usage for online features like uploading photos.
- **android.permission.ACCESS_NETWORK_STATE:** Enables the app to monitor network connectivity, which is useful for determining when to perform online operations.

Conclusion:

While most of the permissions for **com.roidapp.photogrid** are standard and align with its purpose as a photo editing and sharing app, the **GET_TASKS** permission is unusual. This permission might indicate that the app is tracking user activity, which could be a privacy issue. It's worth investigating this permission further to ensure it's not being misused.

Examine the packages.xml file. What permissions would an app have if it accessed com.google.android.calendar.uid.shared (user ID 10055)?



```
<shared-user name="com.google.android.calendar.uid.shared" userId="10055">
  <sigs count="1">
    <cert index="9"/>
  </sigs>
  <perms>
    <item name="android.permission.READ_SYNC_STATS"/>
    <item name="android.permission.WRITE_CALENDAR"/>
    <item name="com.google.android.providers.gsf.permission.READ_GSERVICES"/>
    <item name="android.permission.USE_CREDENTIALS"/>
    <item name="android.permission.READ_CALENDAR"/>
    <item name="android.permission.WRITE_SYNC_SETTINGS"/>
    <item name="android.permission.INTERNET"/>
    <item name="android.permission.READ_SYNC_SETTINGS"/>
    <item name="android.permission.SUBSCRIBED_FEEDS_READ"/>
    <item name="android.permission.GET_ACCOUNTS"/>
    <item name="android.permission.SUBSCRIBED_FEEDS_WRITE"/>
    <item name="com.google.android.googleapps.permission.GOOGLE_AUTH"/>
  </perms>
</shared-user>
```

Permissions granted to applications with this user ID 10055 are:

- **android.permission.READ_SYNC_STATS**: Allows access to synchronization statistics, which helps in monitoring and managing sync operations.
- **android.permission.WRITE_CALENDAR**: Grants the ability to write or modify calendar events, essential for apps that need to create or update calendar entries.
- **com.google.android.providers.gsf.permission.READ_GSERVICES**: Provides access to Google services configuration, used to read settings or configurations from Google's services framework.
- **android.permission.USE_CREDENTIALS**: Enables the app to access the user's credentials, which is necessary for authentication or managing account-related information.
- **android.permission.READ_CALENDAR**: Allows reading calendar events, which is crucial for applications that need to view or interact with calendar data.
- **android.permission.WRITE_SYNC_SETTINGS**: Grants the ability to modify synchronization settings, enabling control over sync behavior and preferences.
- **android.permission.INTERNET**: Provides internet access, which is commonly required for communication with external servers or online services.
- **android.permission.READ_SYNC_SETTINGS**: Allows reading synchronization settings, which is necessary to check and manage sync configurations.
- **android.permission.SUBSCRIBED_FEEDS_READ**: Grants permission to read subscribed feeds, typically used for apps that manage or display RSS or similar feeds.
- **android.permission.GET_ACCOUNTS**: Allows access to the list of accounts on the device, used for account management and authentication.
- **android.permission.SUBSCRIBED_FEEDS_WRITE**: Provides the ability to write to subscribed feeds, which is used for managing or updating RSS feeds.
- **com.google.android.googleapps.permission.GOOGLE_AUTH**: Allows access to Google authentication services, necessary for integrating with Google's authentication mechanisms.

Conclusion:

Applications accessing the shared **user ID 10055 com.google.android.calendar.uid.shared** are granted a range of permissions primarily focused on calendar management, synchronization settings, and Google service integrations. While most permissions are typical for calendar-related applications, the combination of permissions like GET_ACCOUNTS, USE_CREDENTIALS, and GOOGLE_AUTH indicates a significant level of access to user credentials and account information. This setup suggests that apps using this shared user ID have extensive capabilities related to calendar management and integration with Google services, which should be carefully managed to protect user privacy and data security.