APK Reversing & Android Internals

REV @ RITSEC

Fall 2025

Presented by

Dudcom

Content

1 What are APKs

2 Reversing Them

3 Challenges Exp 1

4 Challenges Exp 2

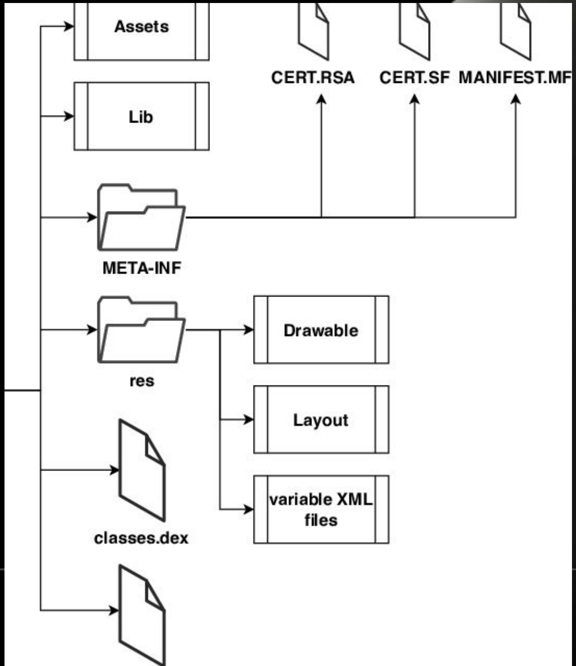
5 You Try !

6 Android Internals

APK File Format

APK - Android Package
- Java, Koltin, Dart, .Net

Really Just A Zip Archive
- Contains all source code / file assets / necessary libs for execution



Folders:
- META-INF
  - Manifest file, cert, sha1 digest
- Lib
  - Compiled code / native code
- Res
  - Not complied Resources
- Assets
  - Application assets
- AndroidManifest.xml
  - Android file describing the name, version, access right
- Classes.dex
  - Complied dex file format
- Resources.arsc
  - Precompiled resources such as binary XML

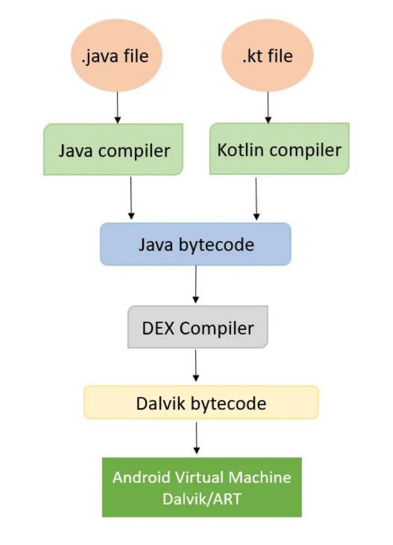
Compilation Internals

Compilation Process:

1. Java (.java) + Koltin (.kt) files, are compiled to create java class files
   a. This is java bytecode which can be ran in the JVM (java virtual machine)
2. Java files are then compiled into .dex files for the Dalvik machine code
   a. The code can now be executed in the ART (Android Runtime) / Dalvik VM

DVM / ART - Why and How?

- DVM was optimized for memory RAM, used JIT - Just in Time compilation
  - We only compile what is needed at runtime for execution
    - Saves RAM but reduced application performance
- ART was created as a result of the ever improving Android hardware
  - Uses AoT (Ahead of time) compilation
  - Dex Bytecode compiled into machine code - **.oat** files
    - Faster code, but slower install and update times since dex bytecode is converted to machine code during installation
    - Higher RAM usage



Compilation Internals Cont.

Why is AoT Bad?

- Most application aren't actively used its kinda pointless to hyper optimize them it also just wastes a large amount of space having to create machine code for every app

Profile Guided Compilation

- 2016 in API 23 JIT is brought back but with the ability to define "hot" methods similar to v8
- Default compilation method is JIT but highly used methods are cached and precompiled in by ART using AoT
  - Only problem is at the start of usage this would be rather slow since it has to build out "hot" usage

Profiles in the cloud

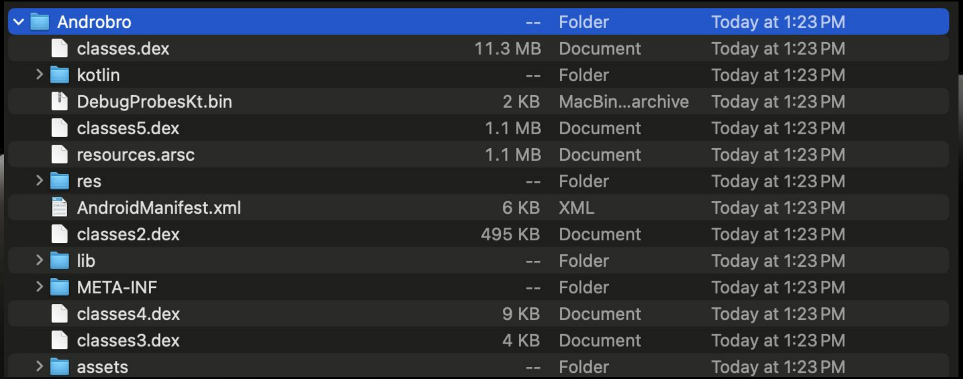
- Simple idea is to store usage data across many users so default "hot" methods exists

Resources

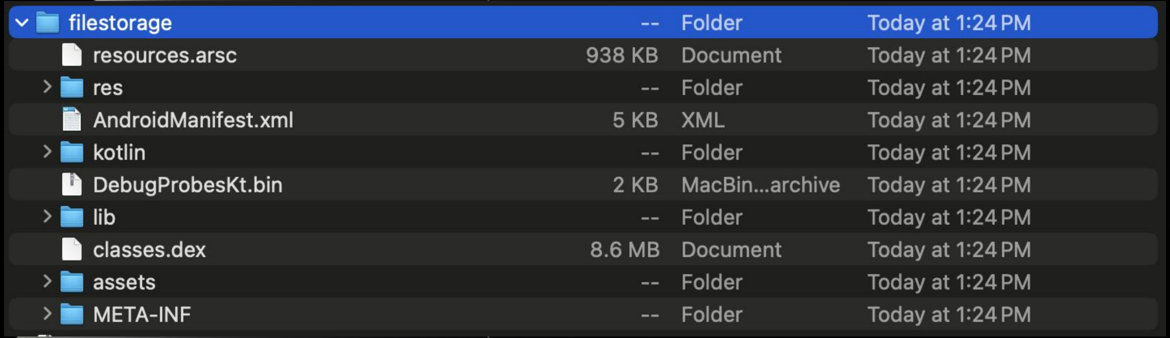
- https://source.android.com/docs/core/runtime
- https://developer.android.com/guide/components/fundamentals
- https://me-abhishek92.medium.com/understanding-android-runtime-and-dalvik-7d8df2b0754b

Opening it up !

File → set to .zip → profit



Androbro	--	Folder	Today at 1:23 PM
classes.dex	11.3 MB	Document	Today at 1:23 PM
kotlin	--	Folder	Today at 1:23 PM
DebugProbesKt.bin	2 KB	MacBin...archive	Today at 1:23 PM
classes5.dex	1.1 MB	Document	Today at 1:23 PM
resources.arsc	1.1 MB	Document	Today at 1:23 PM
res	--	Folder	Today at 1:23 PM
AndroidManifest.xml	6 KB	XML	Today at 1:23 PM
classes2.dex	495 KB	Document	Today at 1:23 PM
lib	--	Folder	Today at 1:23 PM
META-INF	--	Folder	Today at 1:23 PM
classes4.dex	9 KB	Document	Today at 1:23 PM
classes3.dex	4 KB	Document	Today at 1:23 PM
assets	--	Folder	Today at 1:23 PM



filestorage	--	Folder	Today at 1:24 PM
resources.arsc	938 KB	Document	Today at 1:24 PM
res	--	Folder	Today at 1:24 PM
AndroidManifest.xml	5 KB	XML	Today at 1:24 PM
kotlin	--	Folder	Today at 1:24 PM
DebugProbesKt.bin	2 KB	MacBin...archive	Today at 1:24 PM
lib	--	Folder	Today at 1:24 PM
classes.dex	8.6 MB	Document	Today at 1:24 PM
assets	--	Folder	Today at 1:24 PM
META-INF	--	Folder	Today at 1:24 PM

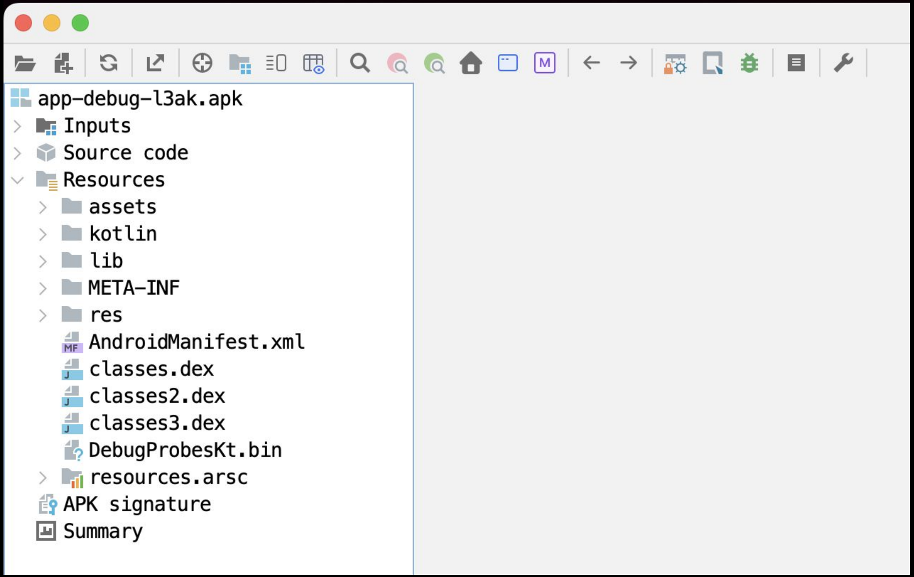
Jadxd

Install:

- sudo pacman -S jadx
- brew install jadx
- flatpak install flathub com.github.skylot.jadx

CLI vs GUI

- Most people tend to use the GUI version there is CLI functionality
- Jadx - cli tool
- Jadx-gui - gui

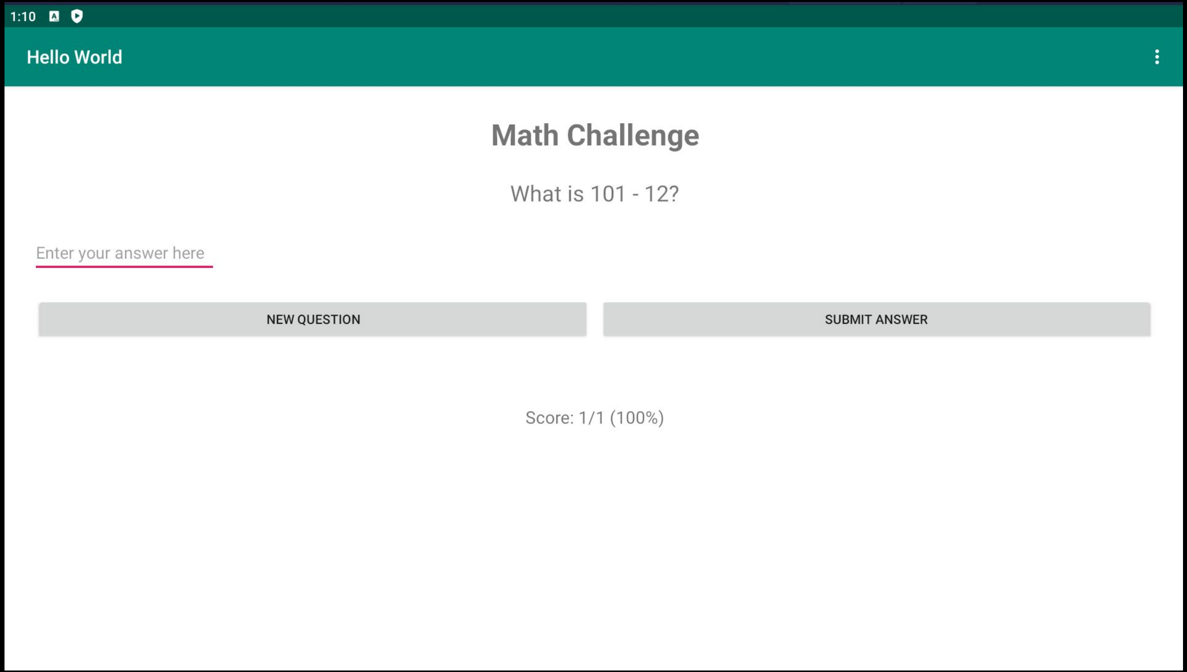


```
app-debug-l3ak.apk
  > Inputs
  > Source code
  v Resources
      > assets
      > kotlin
      > lib
      > META-INF
      > res
        AndroidManifest.xml
        classes.dex
        classes2.dex
        classes3.dex
        DebugProbesKt.bin
      > resources.arsc
    APK signature
    Summary
```

Your first challenge ! https://2025.imaginaryctf.org/files/weird-app/weird.zip

Babies Second Challenge !

https://github.com/L3AK-TEAM/L3akCTF-2025-public/blob/main/mobile/BrainCalc/dist/app-debug.apk



Hello World

Math Challenge

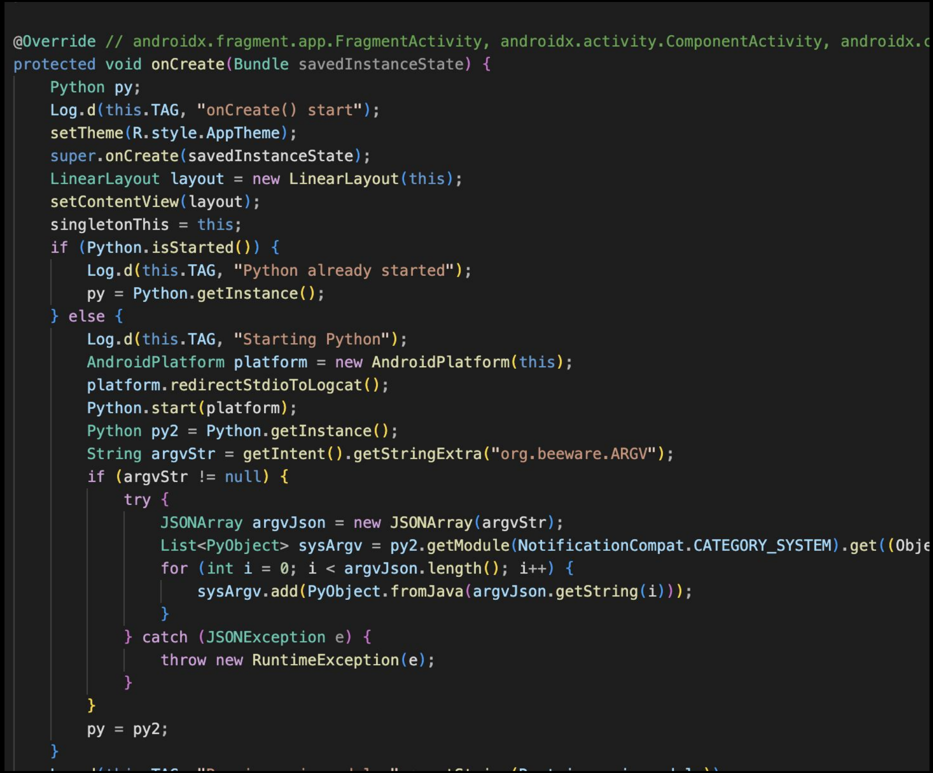
What is 101 - 12?

Enter your answer here

Score: 1/1 (100%)

Finding the Primary logic?

- MainActivity.java



```java
@Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.c
protected void onCreate(Bundle savedInstanceState) {
    Python py;
    Log.d(this.TAG, "onCreate() start");
    setTheme(R.style.AppTheme);
    super.onCreate(savedInstanceState);
    LinearLayout layout = new LinearLayout(this);
    setContentView(layout);
    singletonThis = this;
    if (Python.isStarted()) {
        Log.d(this.TAG, "Python already started");
        py = Python.getInstance();
    } else {
        Log.d(this.TAG, "Starting Python");
        AndroidPlatform platform = new AndroidPlatform(this);
        platform.redirectStdioToLogcat();
        Python.start(platform);
        Python py2 = Python.getInstance();
        String argvStr = getIntent().getStringExtra("org.beeware.ARGV");
        if (argvStr != null) {
            try {
                JSONArray argvJson = new JSONArray(argvStr);
                List<PyObject> sysArgv = py2.getModule(NotificationCompat.CATEGORY_SYSTEM).get((Obje
                for (int i = 0; i < argvJson.length(); i++) {
                    sysArgv.add(PyObject.fromJava(argvJson.getString(i)));
                }
            } catch (JSONException e) {
                throw new RuntimeException(e);
            }
        }
        py = py2;
    }
```

What the fuck is going on here?

- Its java that initialization python code and objects using Chaquopy
    - If you ask AI it more or less tells you this:
        - boostrops a embed python interpreter
        - Runs a designated python module
        - When specific actions are triggered "onCreate" and "onPause" calls python object so it can run python code

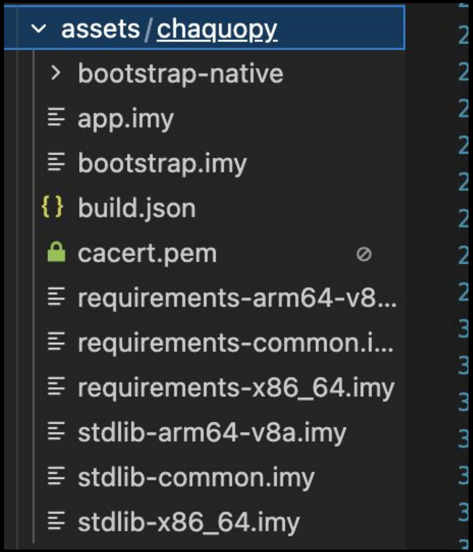
Next steps?

- Where is the python file?
- How does it work?
- Where is our "flag"?

Finding the Python Code !

Chaquopy

- Chaquopy will put its embed code into the assets folder



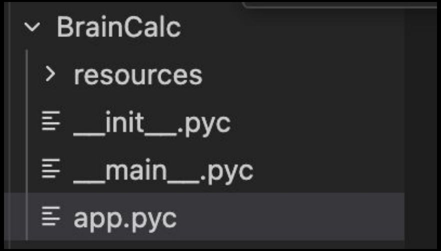
```
assets / chaquopy
  > bootstrap-native
    app.imy
    bootstrap.imy
    build.json
    cacert.pem
    requirements-arm64-v8...
    requirements-common.i...
    requirements-x86_64.imy
    stdlib-arm64-v8a.imy
    stdlib-common.imy
    stdlib-x86_64.imy
```

Well Where is the python?

- The app.imy file !

What is it? If we do file on it we figure out its a Zip Archive

After unzipping it we see our "BrainCalc" folder



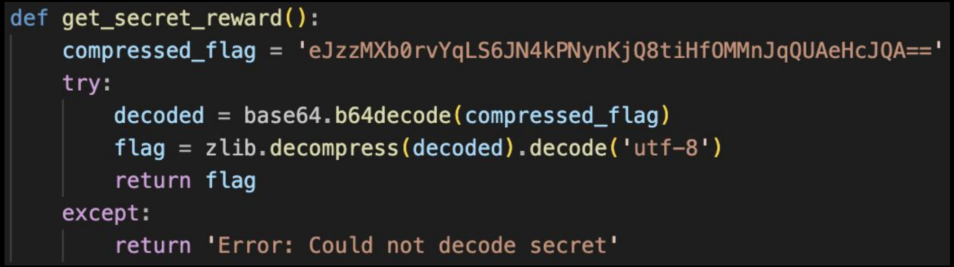
```
BrainCalc
  > resources
    __init__.pyc
    __main__.pyc
    app.pyc
```

https://pylingual.io

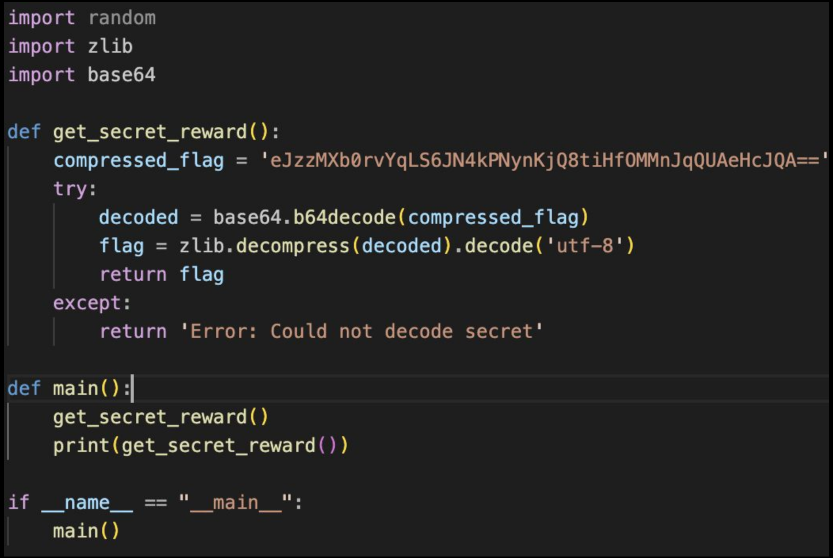
- We are given compiled python (pyc) so use a decomplier to get out the raw python bytecode/source code

Flag?

After we decomp and get the real py files we see that the real code is actually rather simple and doesn't do much interesting just a hidden "print" flag func edit the code a bit as shown on the right ⇒



```python
def get_secret_reward():
    compressed_flag = 'eJzzMXb0rvYqLS6JN4kPNynKjQ8tiHfOMMnJqQUAeHcJQA=='
    try:
        decoded = base64.b64decode(compressed_flag)
        flag = zlib.decompress(decoded).decode('utf-8')
        return flag
    except:
        return 'Error: Could not decode secret'
```



```python
import random
import zlib
import base64

def get_secret_reward():
    compressed_flag = 'eJzzMXb0rvYqLS6JN4kPNynKjQ8tiHfOMMnJqQUAeHcJQA=='
    try:
        decoded = base64.b64decode(compressed_flag)
        flag = zlib.decompress(decoded).decode('utf-8')
        return flag
    except:
        return 'Error: Could not decode secret'

def main():
    get_secret_reward()
    print(get_secret_reward())

if __name__ == "__main__":
    main()
```

L3AK{Just_4_W4rm_Up_Ch4ll}

Our accomplishments

Highlight your company's growth, metrics, awards, and achievements.

Industry award
Product or campaign

00%
Market share

#00
Rank in the industry

Certifications

"Quote from published media coverage about your company"

Link to article

Our values

Write a statement about the core principles that guide your company's actions.

1

Add a value or belief
Define this value and explain how it reflects your company's culture or business aspirations.

2

Add a value or belief
Examples of company values or beliefs might include teamwork, innovation, or customer focus.

3

Add a value or belief
For each value, describe how it makes your company desirable as a business partner.

Our customers

Customer segment title

"Summarize your key values, as if you were speaking directly to your customer segment."

Introduce your customer segment. Include demographic information, such as age range or location. Mention their needs, aspirations, and pain points.

Explain how your product or service solves these pain points and realizes your customers' goals.

Our customers

Customer segment title

Age range: 00-00
Education level: Highest education
Status: Marital status
Location: City or state
Archetype: Tech-savvy

Needs and motivations

- What does this segment want?
- What motivates them?
- What kind of products or services are they looking for?

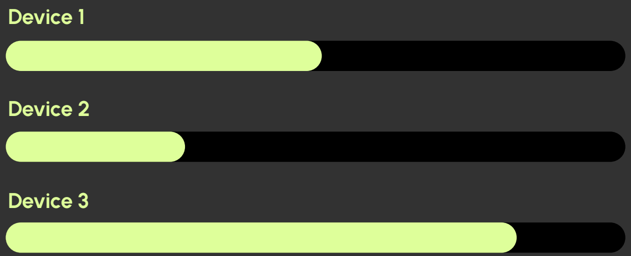
Pain points

- What interferes with their needs, goals, and motivations?
- What frustrates them in their daily life?

Favorite channels

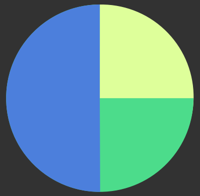
Logo Logo Logo

Technical skills



Purchasing habits

🟦 Online store
🟩 Social media
🟩 Physical store



Our successful partnerships

Celebrate what your company achieved with this partner.

Introduce one of your current partners. Mention their industry or sector, then describe what you accomplished together. Include key initiatives and outcomes.

Learn more

Our successful partnerships

Partnership 1

Quarter, Year

Introduce one of your current partners. Mention their industry or sector, then describe what you accomplished together. Include key initiatives and outcomes.

Learn more

Partnership 2

Quarter, Year

Introduce one of your current partners. Mention their industry or sector, then describe what you accomplished together. Include key initiatives and outcomes.

Learn more

Our successful partnerships

Partnership 1

Quarter, Year

LOGO

Introduce one of your current partners. Mention their industry or sector, then describe what you accomplished together. Include key initiatives and outcomes.

Partnership 2

Quarter, Year

LOGO

Introduce one of your current partners. Mention their industry or sector, then describe what you accomplished together. Include key initiatives and outcomes.

Partnership 3

Quarter, Year

LOGO

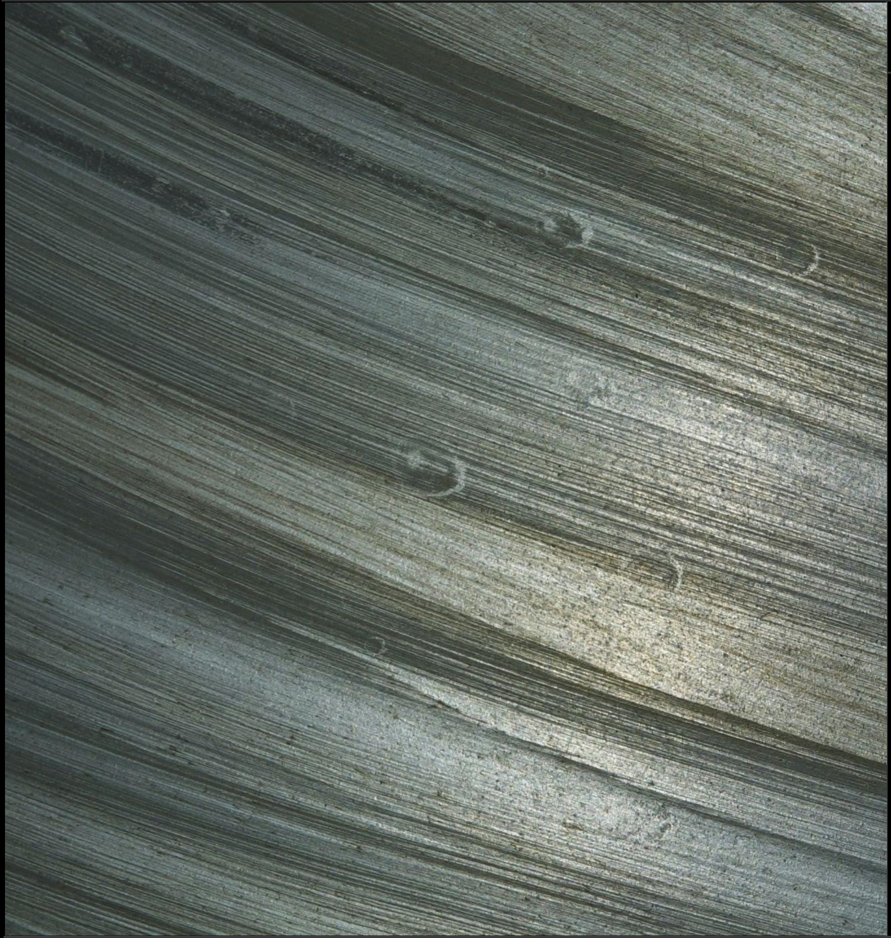
Introduce one of your current partners. Mention their industry or sector, then describe what you accomplished together. Include key initiatives and outcomes.

Partnership 4

Quarter, Year

LOGO

Introduce one of your current partners. Mention their industry or sector, then describe what you accomplished together. Include key initiatives and outcomes.

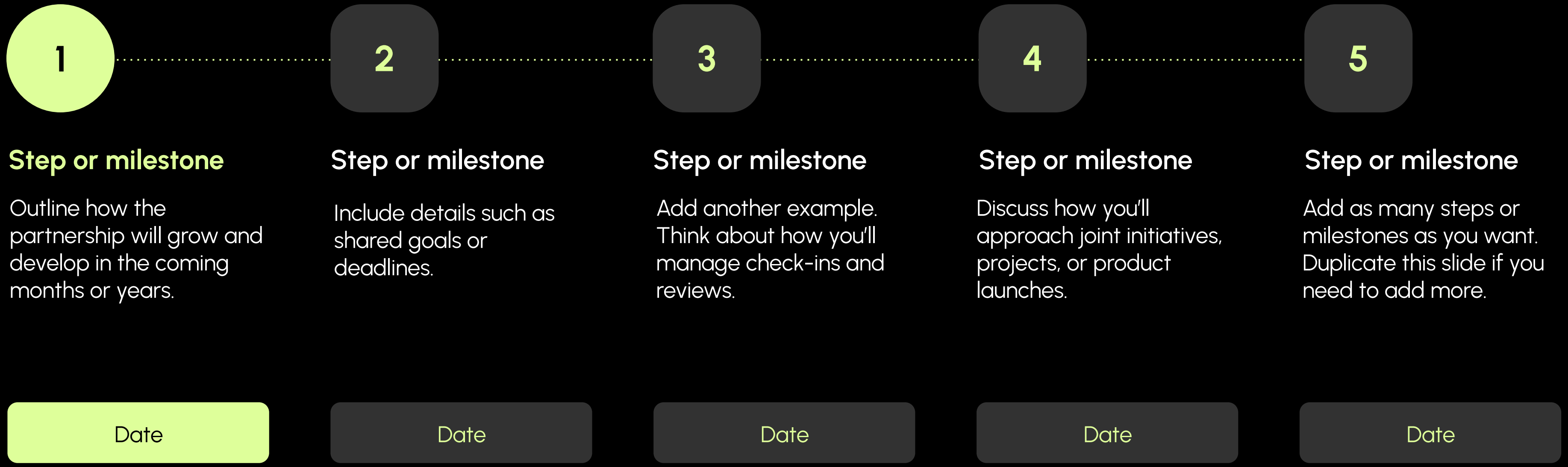


What we can do together

Write a statement about why you want to work with this partner.

Summarize why this partnership would be beneficial for both parties. Show how your values and goals align, and explain how the partnership could help you realise these goals.

How the partnership will work



1

Step or milestone

Outline how the partnership will grow and develop in the coming months or years.

Date

2

Step or milestone

Include details such as shared goals or deadlines.

Date

3

Step or milestone

Add another example. Think about how you'll manage check-ins and reviews.

Date

4

Step or milestone

Discuss how you'll approach joint initiatives, projects, or product launches.

Date

5

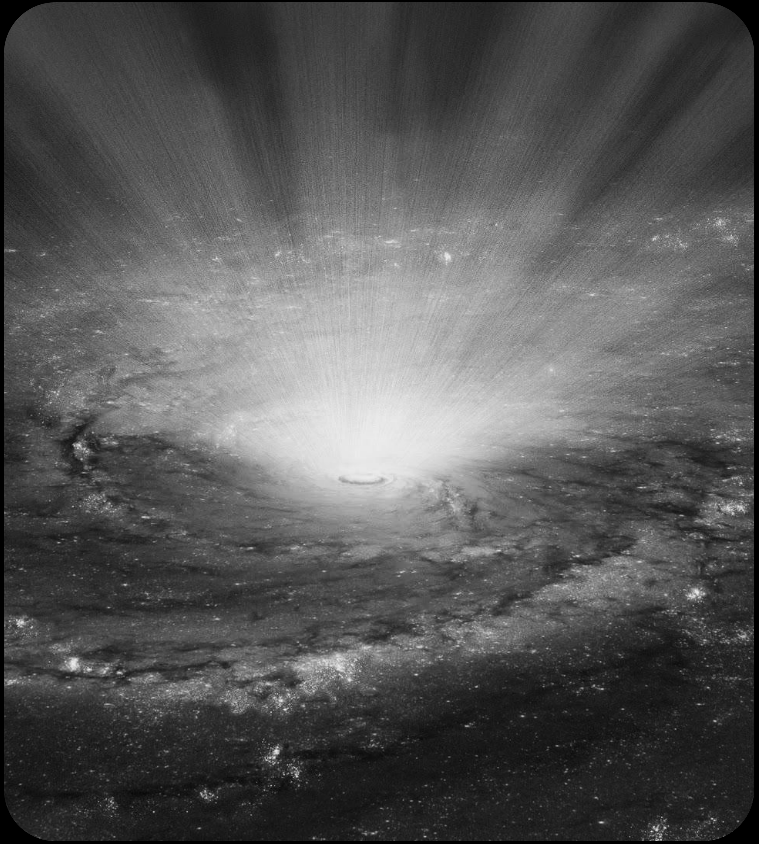
Step or milestone

Add as many steps or milestones as you want. Duplicate this slide if you need to add more.

Date

Let's work together

Invite your potential partner to join your business.



- Mention 3 or 4 partnership benefits
- Each benefit should build on the information outlined in the previous slides
- Include key performance indicators that support your proposal, such as the projected return on investment (ROI) for both parties

Agenda

Timeline

1

Quarter, Year

Outline the next steps of the partnership plan.

2

Quarter, Year

Set a deadline for drafting a partnership agreement, for example.

3

Quarter, Year

Deliver the implementation plan for the partnership.

4

Quarter, Year

Allocate resources and decide on communication channels.

Thank you

Ready for what's next?

Let's talk

Full Name (of the point of contact)
Email
Phone number