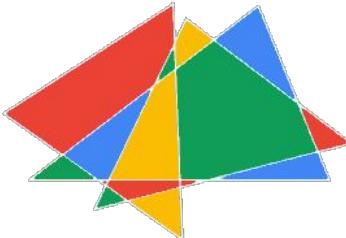




Introduction à l'OSINT

Epita Toulouse, mercredi 18 octobre 2023



Repository Github



<https://shorturl.at/jnpM0>

Sommaire

Définitions

- Ce que n'est pas l'OSINT
- Définition globale de l'OSINT
- Catégories de renseignement
 - GEOINT
 - SOCMINT
 - IMINT
 - HUMINT
 - SIGINT

Source ouvertes

- C'est quoi une source ouverte ?
- Exemples de sources fermées

GEOINT

- Définition
- Exemples
- Outils
- Cas d'application : 4Chan
- Cas d'application : Guerre en Ukraine

SOCMINT

- Définition
- Cas d'application
- Outils
 - Google Dorking
 - Scripts divers
 - Maltego
 - Réseaux sociaux
- Limites légales
- Cas d'application

IMINT

- Définition
- Cas d'application (lien avec le GEOINT) : Guerre en Ukraine
- Outils
 - Analyse visuelle et forensic
 - Analyse des métadonnées
- CTF avec OZINT.eu

SIGINT

- Stéganographie
- Cryptanalyse

Problèmes éthiques

- Utiliser correctement l'OSINT
- Problématiques légales
- Protections et précautions à prendre

Définitions

Définitions : ce que n'est PAS l'OSINT

HACKING

- Pas de récupération de source fermées / privées
- Pas de modification de l'environnement originel
- Activités légalement correctes

Définitions : ce qu'est l'OSINT ?

Faire du renseignement avec des données provenant de sources ouvertes.

- Récupérer des données brutes
- Contextualiser les données
- Analyser les données

Comment récupérer des informations, comment les transformer en renseignement ?

Définitions : Catégories de renseignement

GEOINT

- Géolocalisation d'une donnée
- Couplée à l'IMINT

IMINT

- Analyse d'image
- Contextualisation, valorisation

SOCMINT

- Récupération de données par les réseaux sociaux

HUMINT

- Données de source humaine

SIGINT

- Analyse de signaux

Sources ouvertes

C'est quoi une source ouverte ?

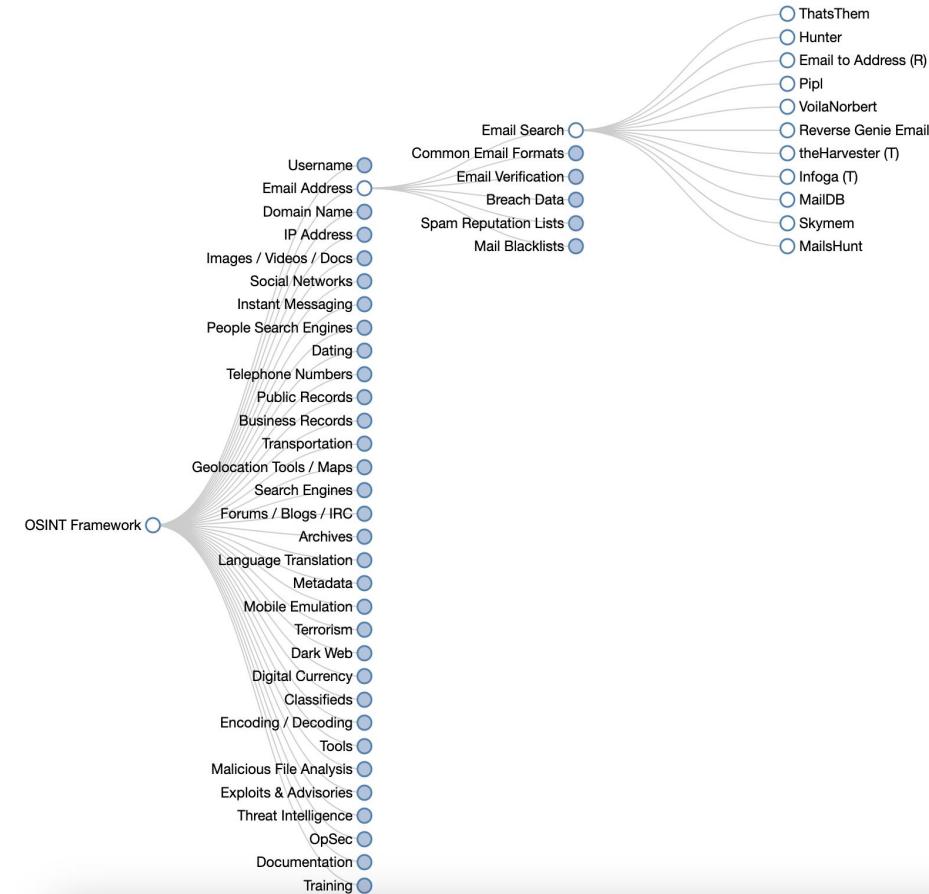
Source accessible de façon “publique” ≠ gratuite

- Magazine
- Données publiques sur internet
- Télévision
- Littérature
- Administration

Précautions importantes à prendre, ne pas laisser de traces, ne pas modifier son environnement originel.

Pas d'utilisation de données privées, confidentielles (si non accessibles), etc...

OSINT Framework



GEOINT

GEOINT

- Guerre en Ukraine
- Conflit Israélo-Palestinien

CTF de 4Chan

GEOINT

Récupération de localisation,
et contextualisation de
l'information

- Google Lens
- OpenStreetMap
- Overpass Turbo
- Ciel
- Trafic aérien(FlightRadar24)

SOCMINT

SOCMINT

- Contre terrorisme
- Recherche générale...

Attention à l'éthique

Renseignement à partir des réseaux sociaux

SOCMINT

- Maltego
- Google Dorking
- Mr Holmes
- Twitter
- LinkedIN
- WhatsMyName, UserSearch
- TheHarvester

Google Dorking

Méthode de recherche permettant d'utiliser Google avec précision

Google site:epita.fr doctype:pdf "segfault"

Images Vidéos Livres Actualités Maps Vols Finance

Environ 5 résultats (0,21 secondes)

 epita.fr https://blog.lse.epita.fr, authors, psurpury : Psurpury | LSE Blog

11 avr. 2020 — ... pdf). The usual way to get a Method Handler of a function in a class ...
segfault. Here is the code of this second step: #SECOND part : leek ...

 epita.fr https://blog.lse.epita.fr, authors : W4kfuf | LSE Blog

11 avr. 2020 — ... pdf). The usual way to get a Method Handler of a function in a class ...
segfault. Here is the code of this second step: #SECOND part : leek ...

 epita.fr https://blog.lse.epita.fr, authors : Pm | LSE Blog

11 avr. 2020 — ... pdf). The usual way to get a Method Handler of a function in a class ...
segfault. Here is the code of this second step: #SECOND part : leek ...

 epita.fr https://gitlab.lre.epita.fr, Spot, Spot : NEWS · spot-2-10-4 - GitLab - Epita

1 févr. 2022 — ... **segfault** during WDBA minimization on automata with useless states ... PDF manual. 6024. * Many bug fixes. 6025. 6026. New in spot 0.0b (2003-06 ...

Google site:epita.fr inurl:cri

Images Vidéos Définition Actualités Tableau Chat Grenouille Poule Chouette hulotte

Environ 3 210 résultats (0,38 secondes)

 epita.fr https://cri.epita.fr : Forge ID

Forge ID · Documentation · News · Maps · Fleet · Sign in · Blog CRI · Charte des SM · EPITA News · EPITA Signalement · Fleet Manager · GitLab CRI.

 epita.fr https://gitlab.cri.epita.fr : Sign in · GitLab

GitLab Enterprise Edition.

 epita.fr https://moodle-exam.cri.epita.fr : Plateforme d'examens de l'EPITA

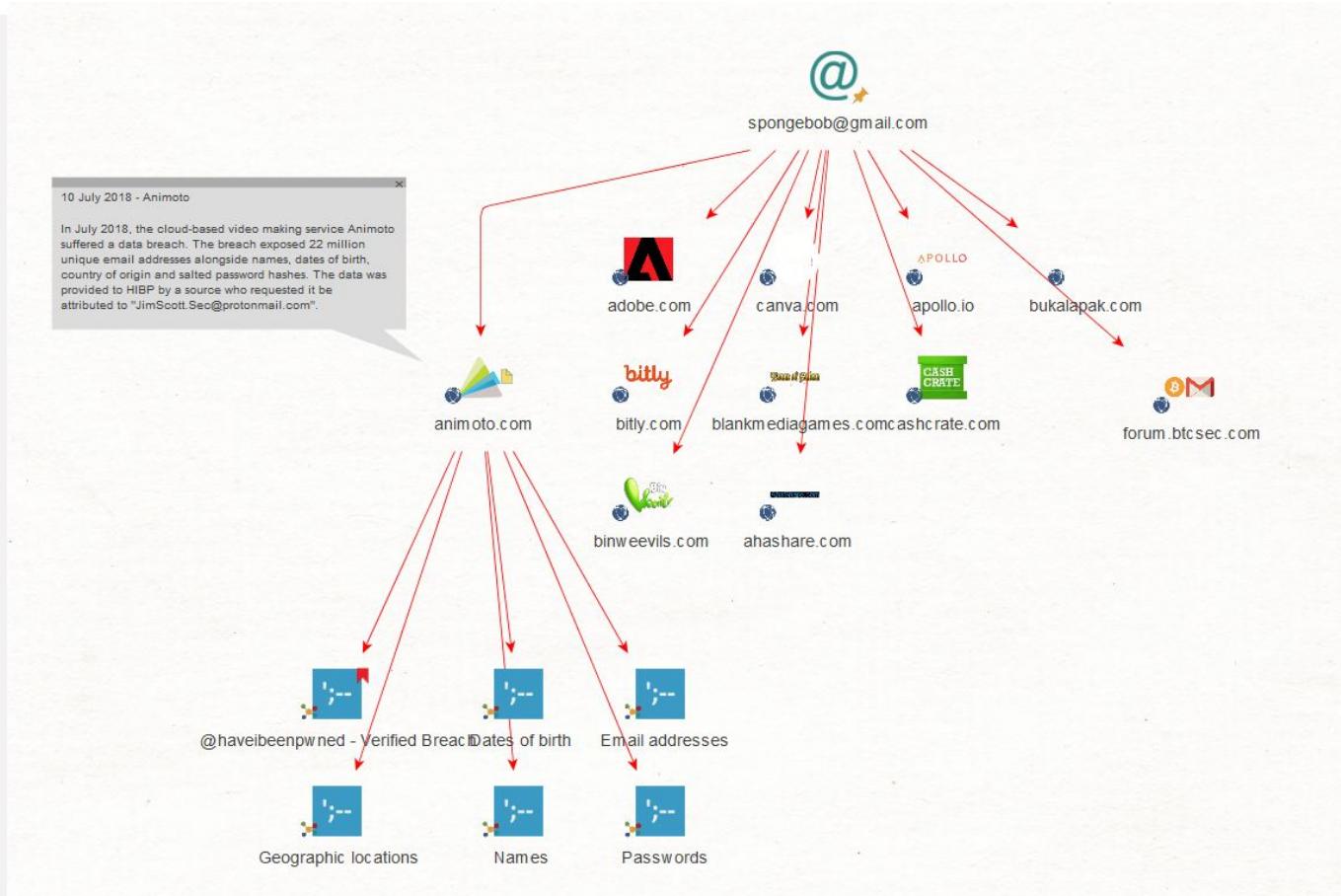
Bienvenue sur la plateforme d'examens de l'EPITA.

Maltego



MALTEGO

Maltego



Welcome to the Pipl Search API

About the Pipl Search API

Pipl Search helps you gather information on customers and contacts to ensure that you are targeting the right people with the right content. This is useful in multiple industries:

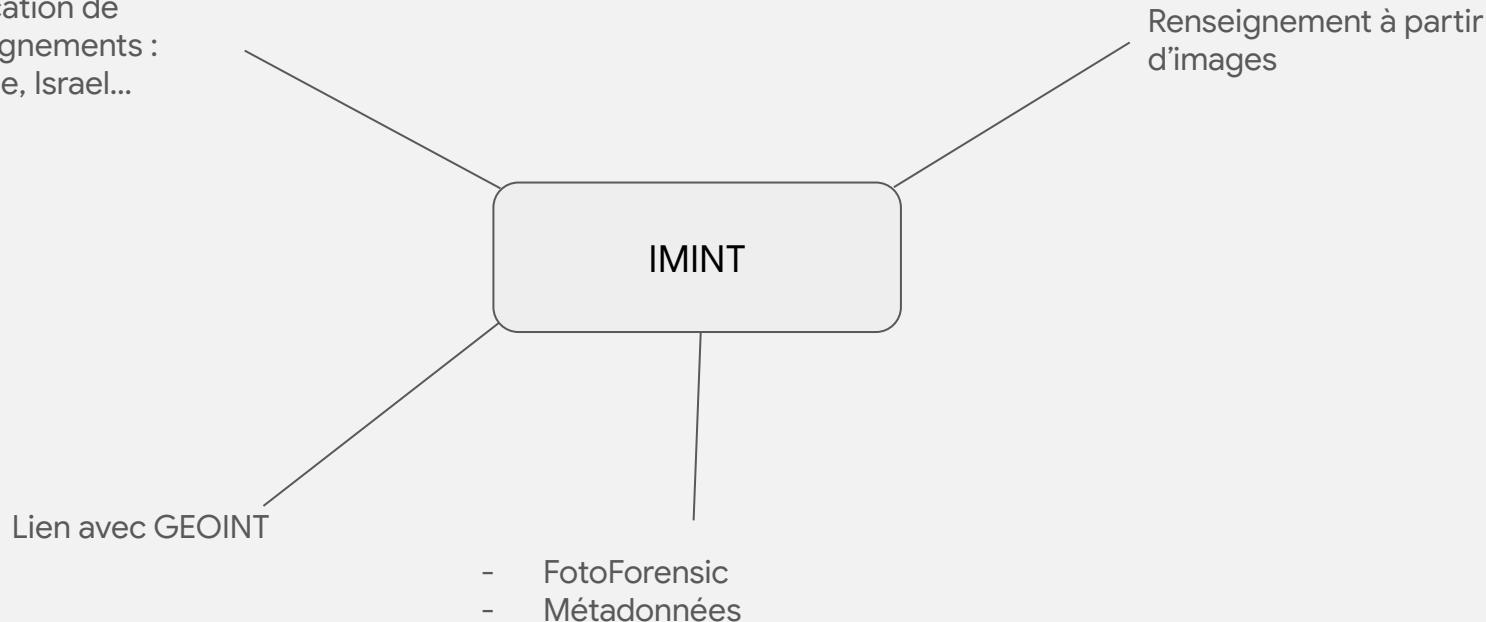
- Professional recruiting, which depends on accurate personal information to find candidates who are best suited to a position
- Hiring, financial applications and other scenarios that require proof of employment.
- Digital marketing, where the additional personal data can help match advertising to interested consumers, improving the likelihood of conversion and increased revenue

Use the Pipl Search API to automate your searches and collect results into a format that is easily consumable by your website or application. This guide walks you through first steps to help you get started. If you need detailed information on the API, see [The Pipl Search API Reference](#).

IMINT

IMINT

- Vérification de renseignements : Ukraine, Israel...



Problèmes éthiques

Problèmes éthiques

Ne pas utiliser l'OSINT (en particulier SOCMINT) à des fins malveillantes.

La communauté OSINT doit rester dans l'objectif de rendre des informations fiables, publiques. L'OSINT ne doit pas être utilisé comme menace, mais comme moyen d'avoir des informations pour comprendre le monde actuel sans manipulation de l'information et de l'opinion.

- Faire attention, prendre des précautions.
- Être à plusieurs.
- Ne pas diffuser ou enregistrer des données confidentielles mal protégées

Stay safe, then OSINT.

Logos [Chapter]

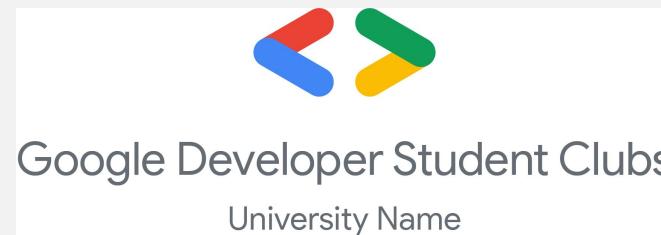
Those who have been a part of the program for a while are familiar with the GDSC logo as an acronym. The new Google Developer Student Clubs logo is an opportunity for community groups to have a stronger visible affiliation with Google.

Use the logo in these formats.

While the horizontal logo is preferred, the stacked logo can be used as an alternative when space is a limiting factor.

The full color logo lockup should only be used on either white and grey backgrounds.

The white version should only be used on top of a background color from the Google Developers primary color palette or on photographs that are not too busy.

[Download Files](#)

The bracket icon [Download](#)



Color

Use the Google Developers Student Clubs primary color palette in assets or communications.

White is the most important color in our palette. It provides simplicity and clarity to our visuals, and it's the foundation of all Google designs, illustrations, and environments. Use the primary colors to create focus.

Neutrals



Black
#000000



Grey 700
#5f6368



Grey 100
#f1f3f4



Blue 500
#4285f4



Blue 300
#8ab4f8



Green 500
#34a853



Green 300
#81c995



Yellow 600
#f9ab00



Yellow 200
#fde293



Red 500
#ea4335



Red 300
#f28b82

Chapter Logo Do's

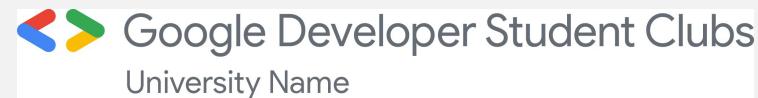


Do customize the lockup for your chapter using the official lockup generator tool (made available only to confirmed members of the platform) and following the naming guidelines indicated above.

Do refer to your chapter as “Google Developer Student Clubs [University Name]”.

Do refer to the program as “Google Developer Student Clubs”

Do name your chapter with a “University Name”



Do if you want to further customize your brand, create a visual asset that can be shown in addition to but NOT as part of the lockup. The spacing around the lockup should at a minimum match the height of “Google”.

Do describe the program as “GDSC stands for Google Developer Student Clubs and is a program offered by Google for Developers to support community-run developer groups”.

Do refer to your chapter as “a community-run developer student club supported by Google for Developers”

Chapter Logo Don'ts

Don't Localize "GDSC" or the Location within the lockup. Always use "GDSC" and "University Name" in English and localize comms instead.

Don't Name your chapter with a "Location" that is a state, country, region, or continent (e.g. California, France, EMEA, Africa).

Don't Refer to your chapter as a "Google Developer Student Club Location" or "Google Developers Student Club Location".

Google Developer Student Clubs

GDSC Location

Don't Use the Google for Developers name or lockup to represent your chapter. Always use your custom Google Developer Student Club [University Name] lockup OR the main GDSC lockup instead (but don't use both at the same time!).



Don't Alter or distort the official lockup in any way, including altering fonts, colors, shapes, proportions, or rotating/flipping it in any direction.



Don't Use the lockup on a poorly contrasting or busy background.

Don't Overlap or crowd the lockup with other custom elements including text or artwork.

Photography

Use photography to communicate Google's values of inclusivity, empowerment and strength in community.

Prioritize and focus on individuals.

Capture smiling faces.

Focus on actions that communicate what Google Developers is about (people coding together, working on laptops, listening to talks, giving talks, networking).

Avoid focusing on "party" photos.

Make sure photos are clear, with good lighting and of high resolution. Avoid sharing blurry photos.

Integrate the developer line art style as needed to reiterate Google's developer-centric branding.



Typography

Please use Google Sans Bold for headlines, and Google Sans Regular for subheads and body copy. If smaller text is necessary such as for annotations, footnotes, or small labels, please use Open Sans or Roboto Mono.

Google Sans Bold

Headline

Roboto Mono Normal

Subhead

Google Sans Regular

Body Copy

Open Sans Normal

Alternate Body Copy

Typography: Do's

Use a ratio of $1\frac{1}{2} : 1$ for setting the size of a header to the body copy. (Example: if your body copy 12pt in size, please set the header to 18 ($12/2 = 6$; $12+6=18$).

Use a line spacing of between 1.15-1.5.

Add a paragraph break that is $\frac{1}{2}$ the height of the header. (Example: if the header is 24pt in size, add at least a 12pt paragraph break between the header and body copy below.)

Use color to draw attention to key messages in the typography.

Applications closing soon.

Submit your information by October 1 to be considered.

Do

Left align text and ensure comfortable spacing between lines

Subtitle Text

Another example of a header.

Submit your information by October 1 to be considered.

Do

Apply Roboto Mono Normal to the subheaders to create appropriate hierarchy.

Typography: Don'ts

Applications closing soon.

Submit your information by October 1 to be considered.

Don't

Do not use bold for subheadings or body copy.

Applications closing soon.

Submit your information by October 1 to be considered.

Don't

Do not use multiple colors for a full body of text. Reserve color usage to the key element of a message that deserves the most attention

Applications closing soon.

Submit your information by October 1 to be considered.

Don't

Do not use highlights or any other typographic treatment for headers. Lean on Google Sans bold and accents of color to draw attention to content when necessary.

Typography: Don'ts

APPLICATIONS CLOSING SOON.

Submit your information by
October 1 to be considered.

Don't

Do not use all caps for headlines, or underline text (unless an underline is needed for a link)

Applications closing soon.

Submit your information by
October 1 to be considered.

Don't

Do not apply colors outside of the brand guidelines to any typography.

Applications closing soon.

S i g n u p t o d a y !

Don't

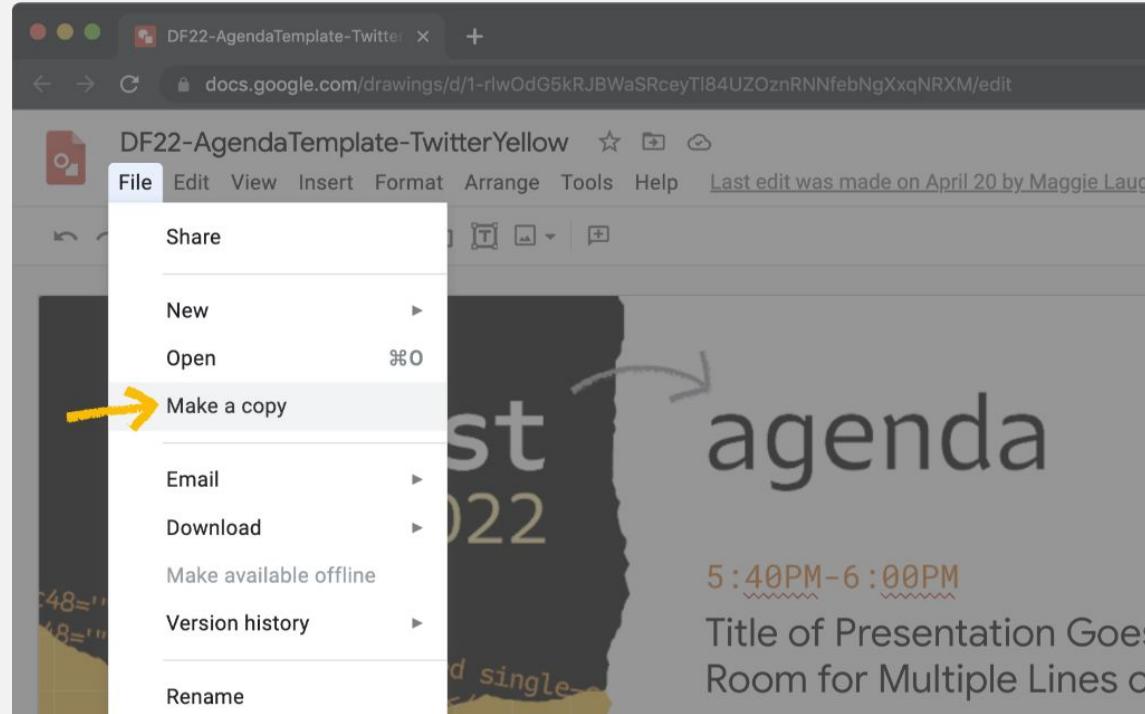
Do not use italics or adjust the letter spacing of the text

How-to Use Google Drawings

How to use Google Drawings: Create

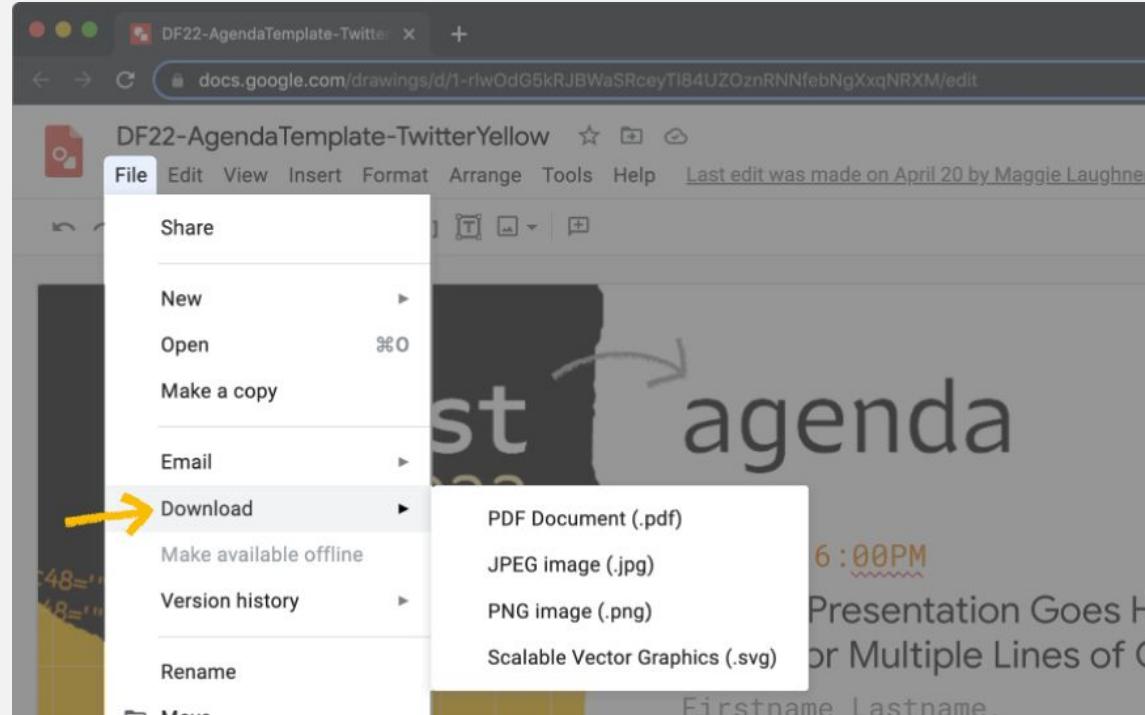
To create your own asset, simply make a copy of the Google Drawing you are looking to recreate.

Once you have made your own copy of the asset, you can edit the location, information, and photos to your liking. Keeping within the guidelines noted in this document will ensure your version is on-brand.



How to use Google Drawings: Export

To export your customized DevFest asset, go to File > Download > and select the preferred file type. In most cases, this will either by .jpg or .png



Video

Intro Animation

[Download Files](#)

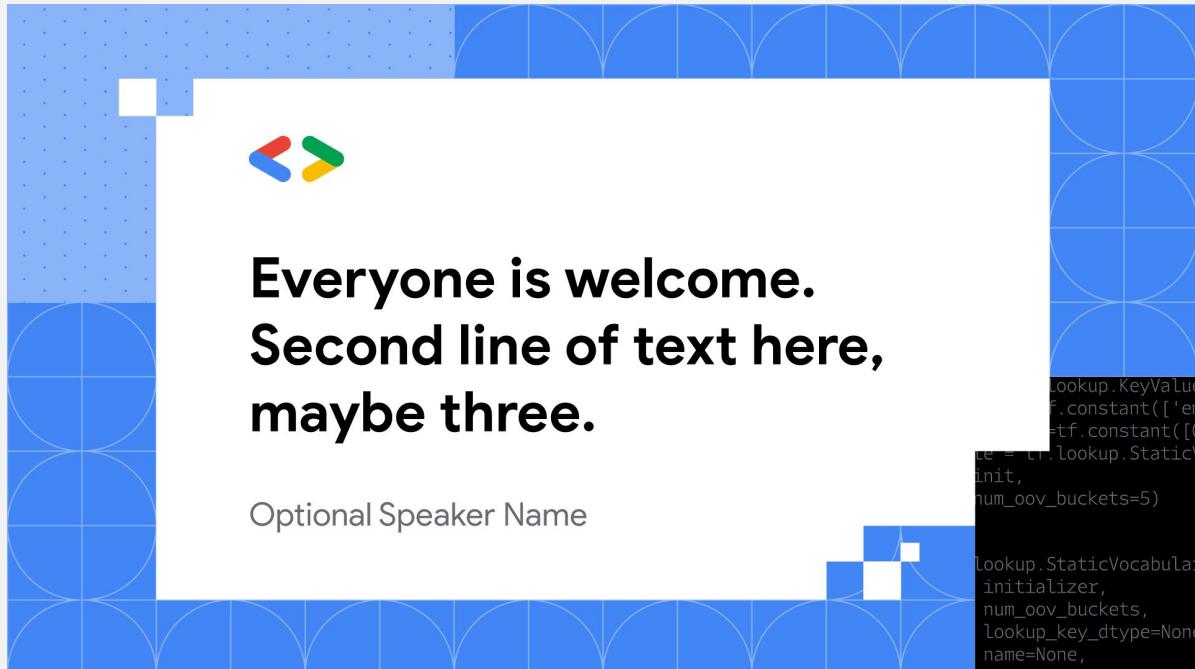


Intro Animation with Title

[Download Files](#)



Title Card

[Download Files](#)

Section Title

[Download Files](#)



Transitions

[Download Files](#)



End Card

[Download Files](#)



Lower Thirds

[Download Files](#)

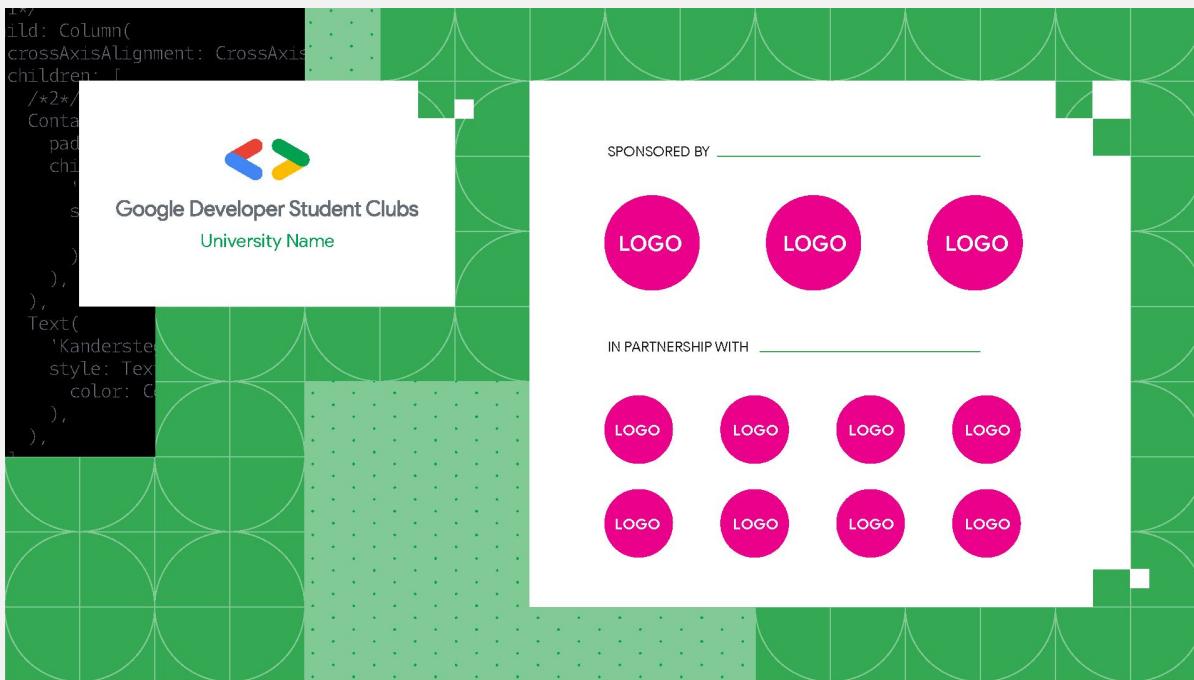


YouTube Thumbnail

[Download Files](#)

Holding Slides: GDSC Logo / Sponsors & Partners

Download Files



Digital

Website: Landing Page Header

[Download Files](#)



2650x500



640x500

1440x500

Website: Bevy Landing Page Header

Download Files



2560x650

Website Banners

[Download Files](#)



2650x500



640x500



1440x500

Blog Post Banners

[Download Files](#)



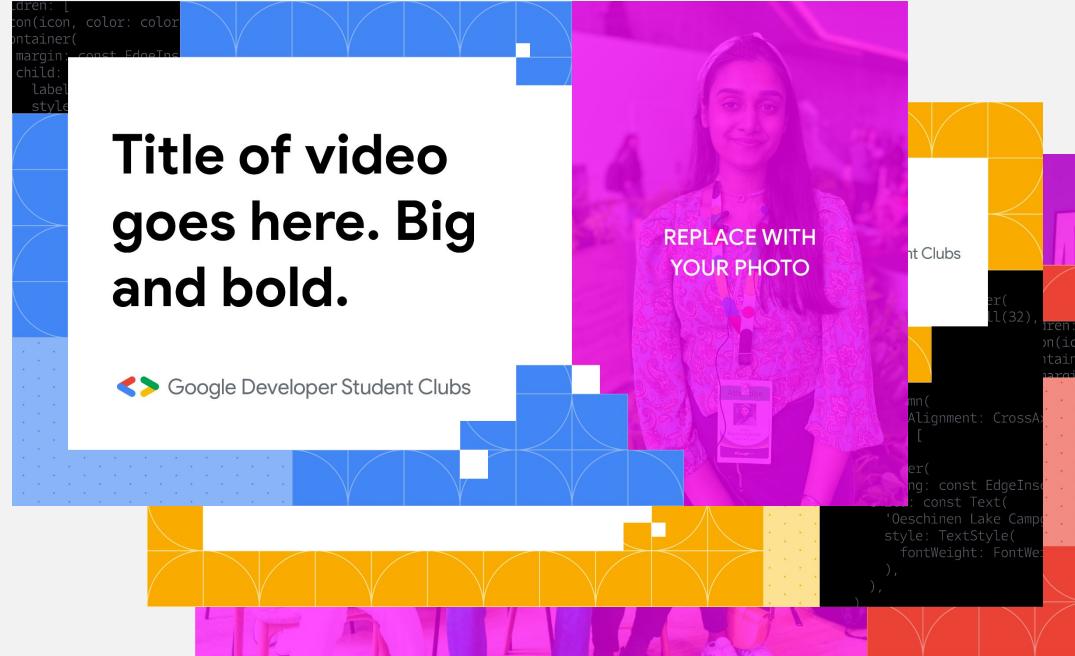
4209x1253



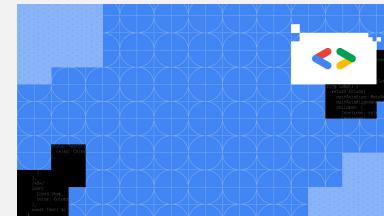
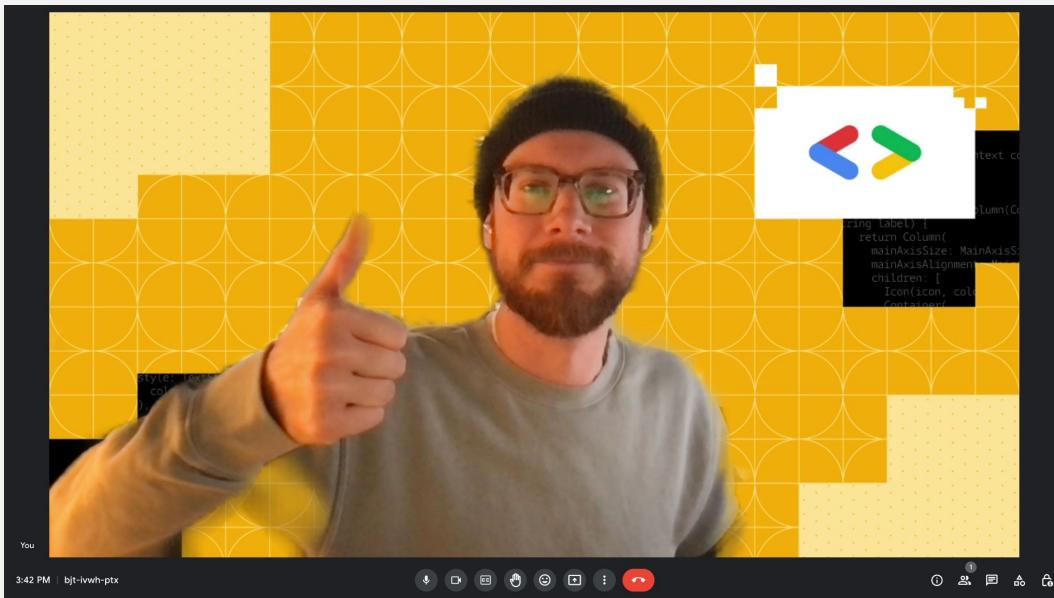
1024x512

Presentation Slides Template

[Download Files](#)



Video Chat Digital Background

[Download Files](#)

Email Template: Google Docs

[Download Files](#)



Headline One

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt. [Link lorem ipsum](#)

Email Signature

Download Files

Michaelangelo Muchlongername

Title at Company

Subheading text here

P 111.111.1111

editableurl.com



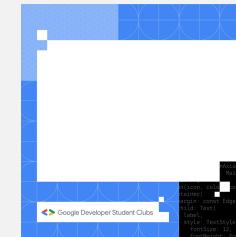
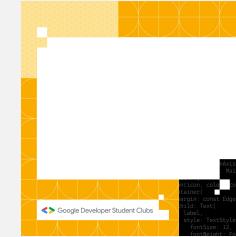
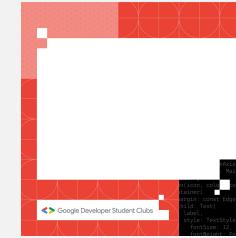
Social

Instagram: Promo Stickers (GIFs)

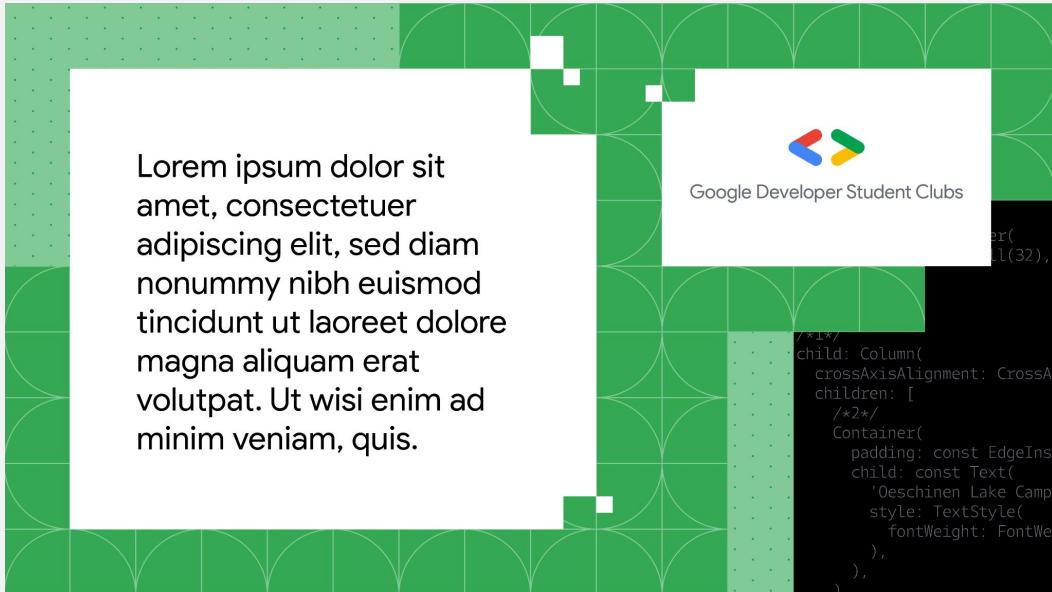
[Download Files](#)



1:1 Background Template

[Download Files](#)

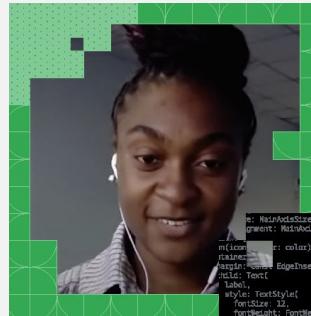
16:9 Background Template

[Download Files](#)

Avatar Template

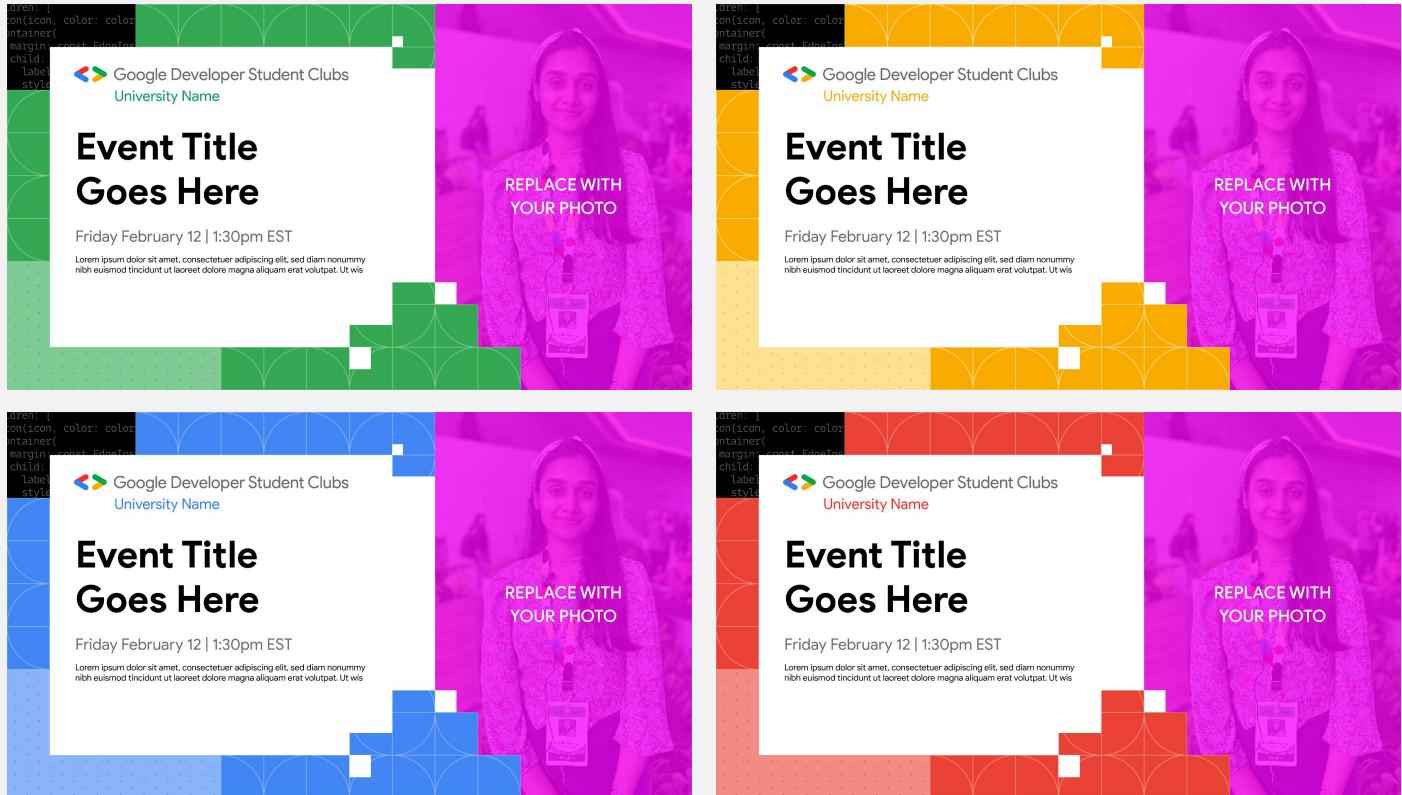
[Download Files](#)

Photo Frames

[Download Files](#)

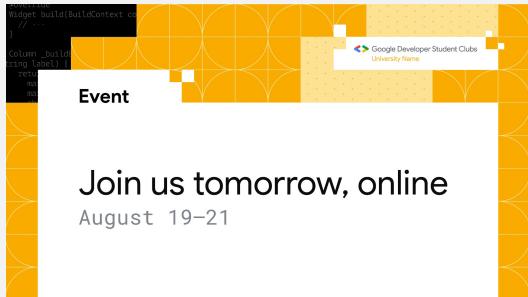
Social Media Event Promo

Download Files

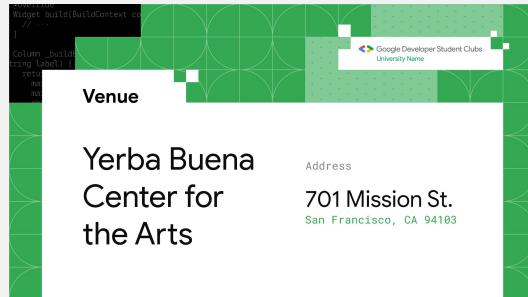


Announcement Templates: Event, Venue, Activity

[Download Files](#)



Event Announcement



Venue Announcement



Activity Announcement



Agenda Template

[Download Files](#)

```
override  
Widget build(BuildContext co  
    // ...  
}  
  
Column _buildD  
string label) {  
    return  
        ma  
        ma  
        sh  
  
    Event
```

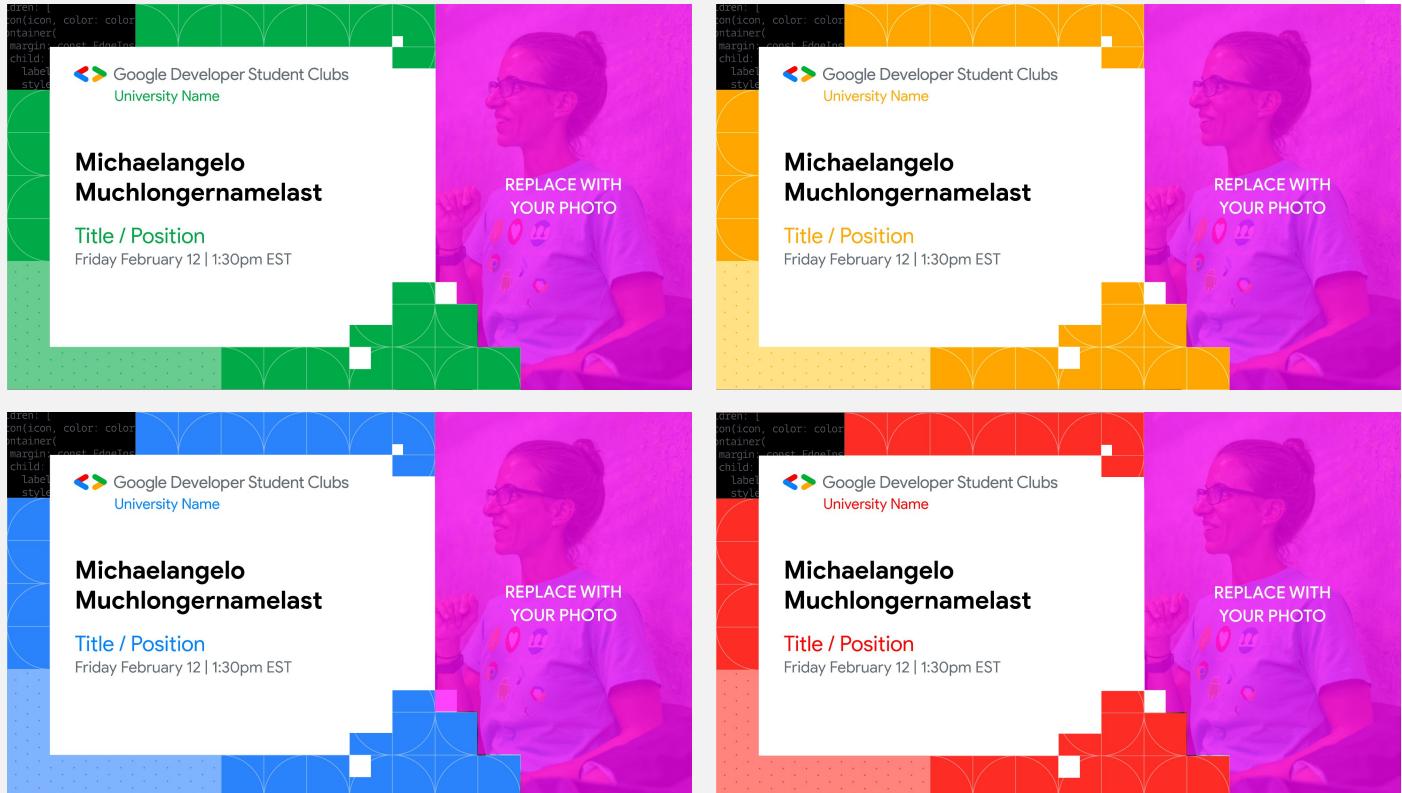


Join us tomorrow, online

August 19–21

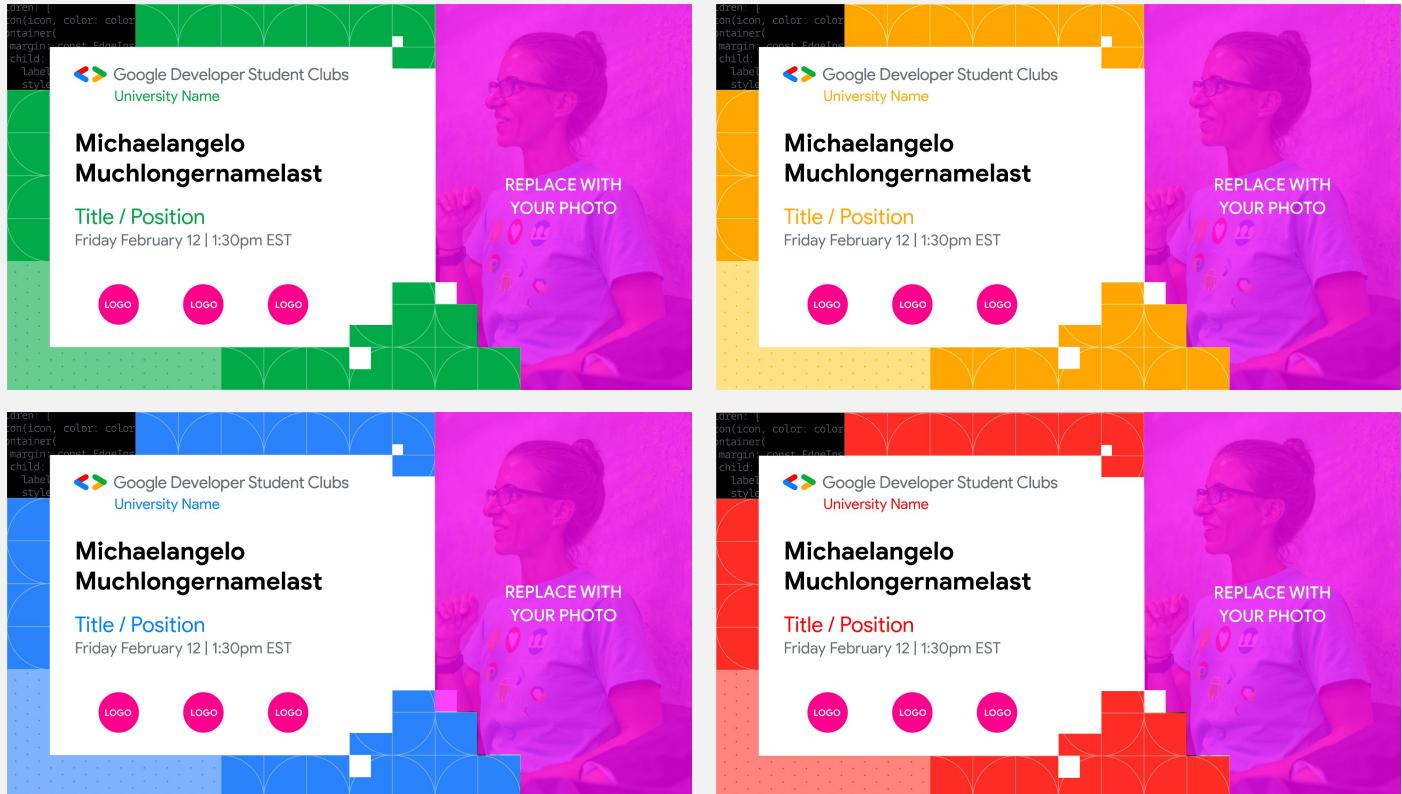
Speaker Promo

Download Files



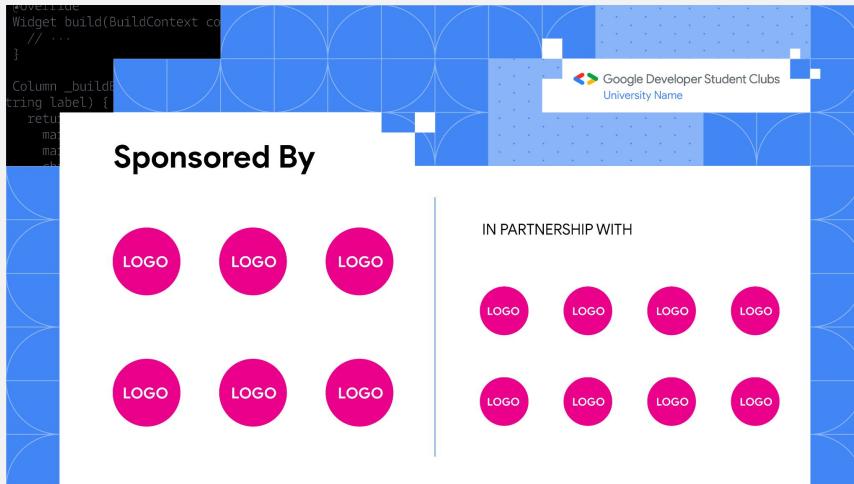
Speaker Promo: Co-branded

Download Files



Sponsor/Partner Announcement Template

Download Files



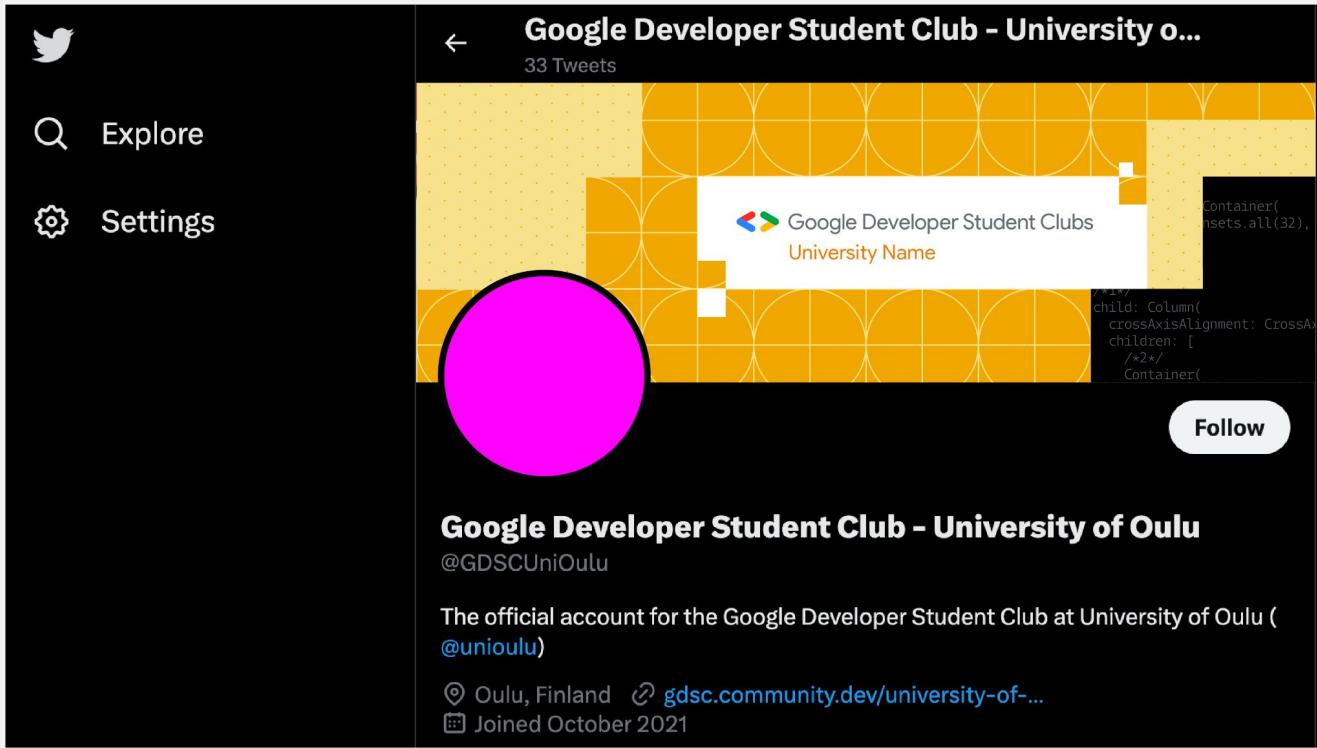
16:9



1:1

Twitter Banner

Download Files



The image shows a Twitter profile banner for the Google Developer Student Club at the University of Oulu. The banner features a yellow background with a geometric pattern of overlapping circles and squares. In the center, there is a white rectangular box containing the Google Developer Student Clubs logo and the text "University Name". Below the banner, the profile information is displayed:

Google Developer Student Club - University o...
33 Tweets

Follow

Google Developer Student Club - University of Oulu
@GDSCUniOulu

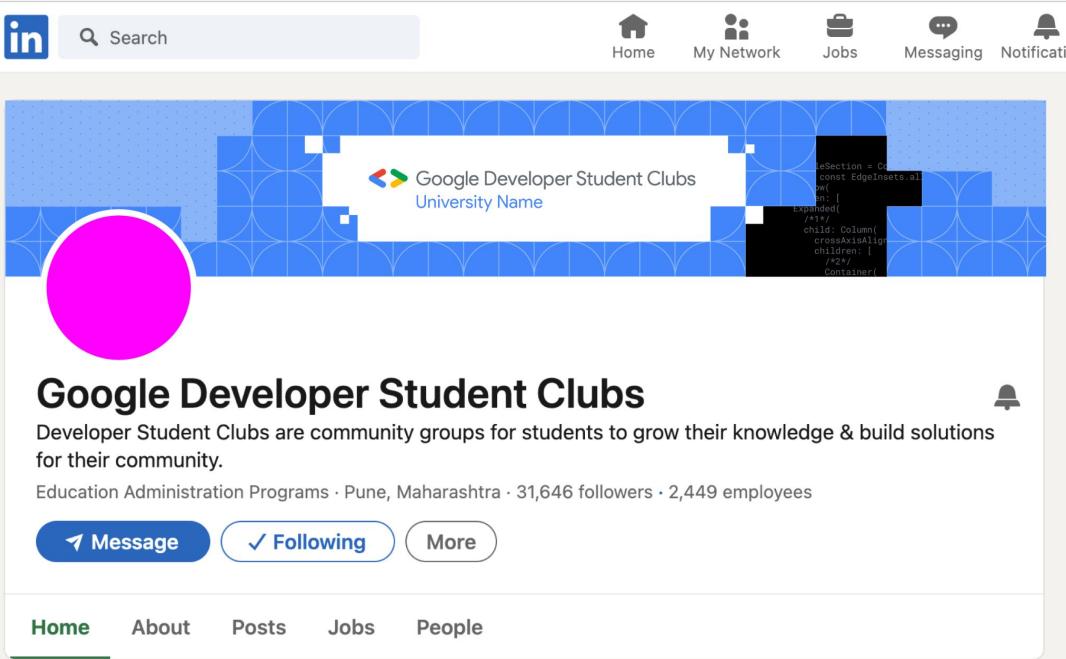
The official account for the Google Developer Student Club at University of Oulu ([@unioulu](#))

 Oulu, Finland  gdsc.community.dev/university-of-...
 Joined October 2021

A large pink circle is overlaid on the left side of the profile banner.

LinkedIn Banner

Download Files



The LinkedIn profile banner features a blue background with a white rectangular overlay containing the Google Developer Student Clubs logo and the text "University Name". A large pink circular placeholder image is on the left. The LinkedIn navigation bar is visible at the top.

Google Developer Student Clubs

Developer Student Clubs are community groups for students to grow their knowledge & build solutions for their community.

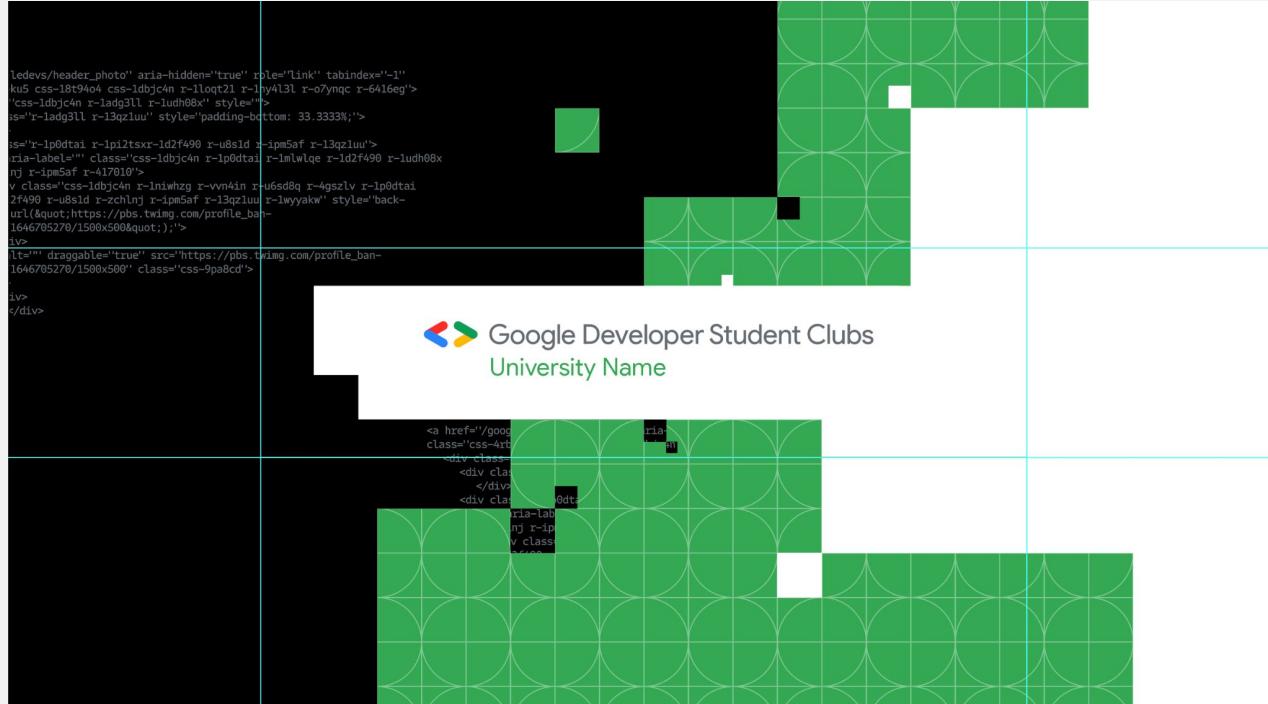
Education Administration Programs · Pune, Maharashtra · 31,646 followers · 2,449 employees

[Message](#) [Following](#) [More](#)

[Home](#) [About](#) [Posts](#) [Jobs](#) [People](#)

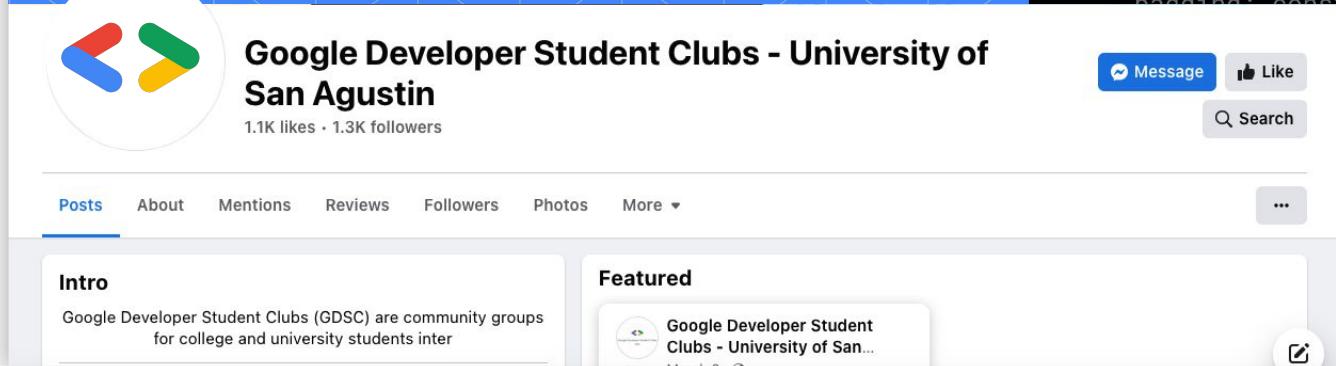
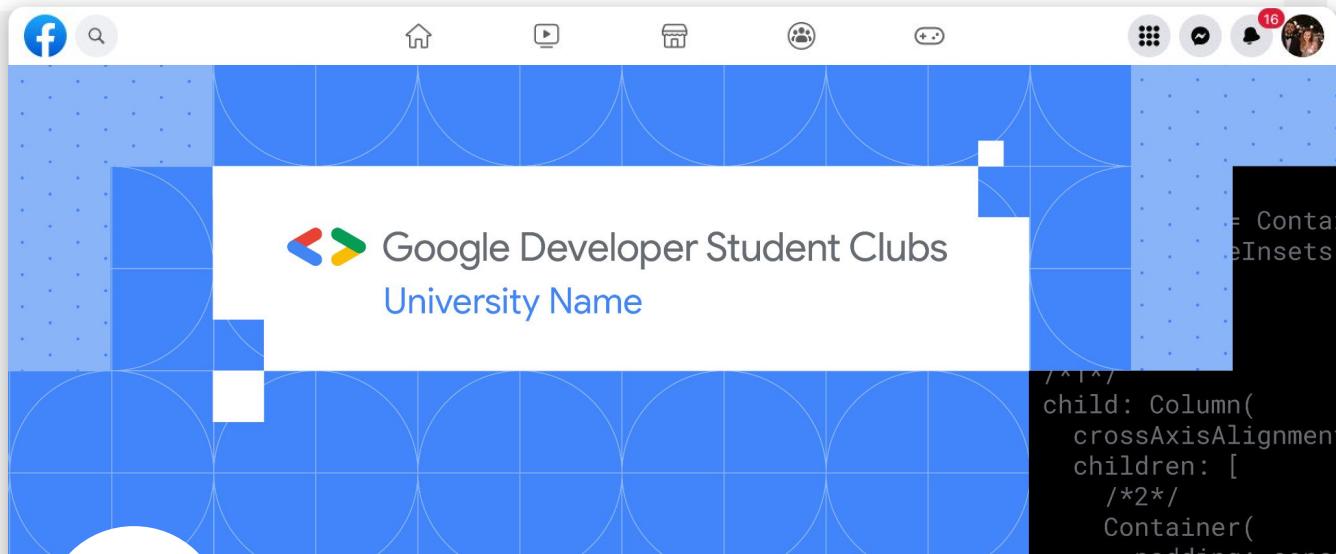
YouTube Banner

If you have a social media channel(s) for your chapter, you may use these homepage header graphics.

[Download Files](#)

Facebook Banner

If you have a social media channel(s) for your chapter, you may use these homepage header graphics. Replace the photograph(s) as desired.

[Download Files](#)

Google Developer Student Clubs - University of San Agustin
1.1K likes • 1.3K followers

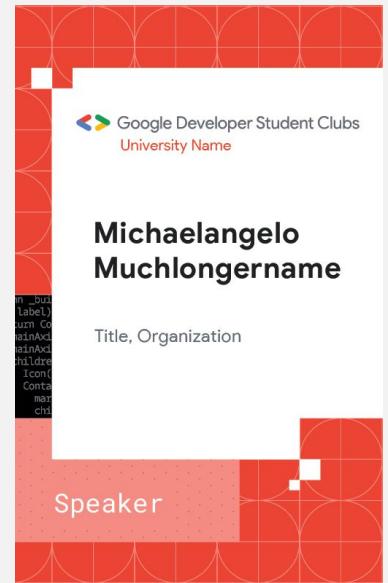
Posts About Mentions Reviews Followers Photos More ...

Intro
Google Developer Student Clubs (GDSC) are community groups for college and university students inter...

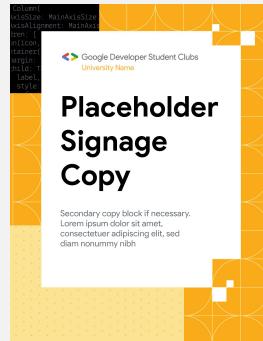
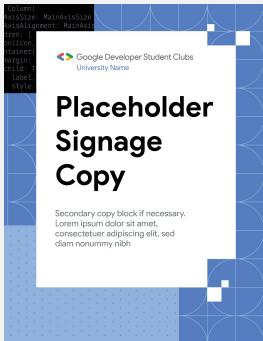
Featured
Google Developer Student Clubs - University of San...

Events

Badges & Lanyard: 3.5x5.5"

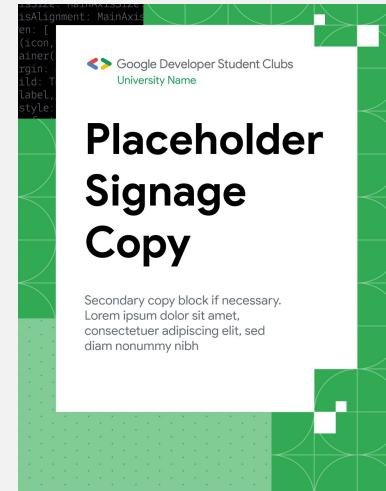
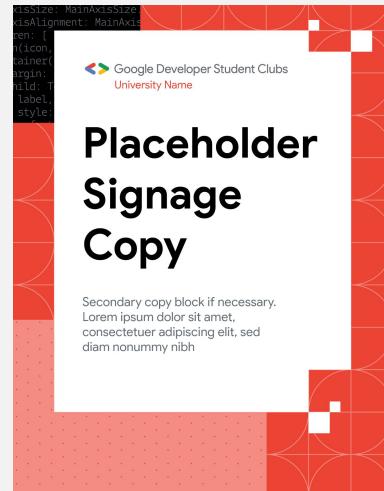
[Download Files](#)[Download Files](#)

Signage: Letter / 8.5x11"

[Download Files](#)

Signage: Poster / 18x24"

Download Files

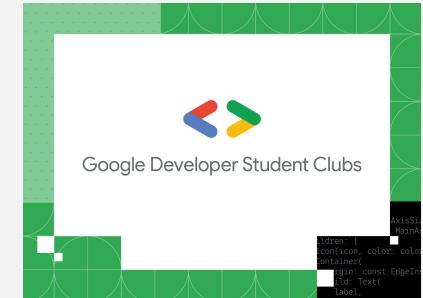
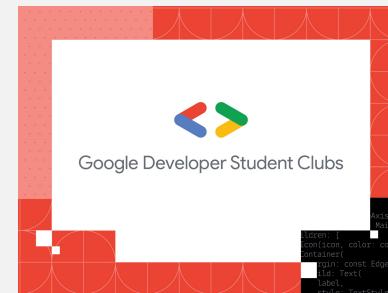
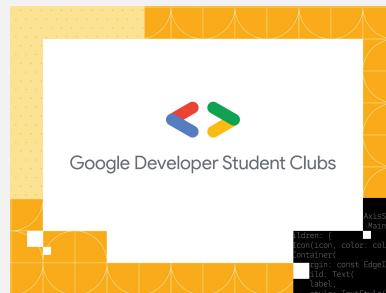
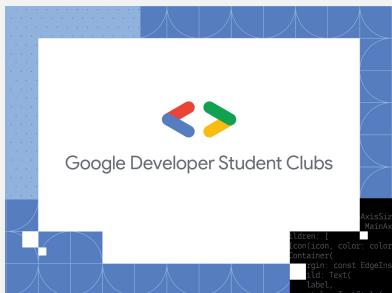


Signage: Meterboard / 46x95"

[Download Files](#)

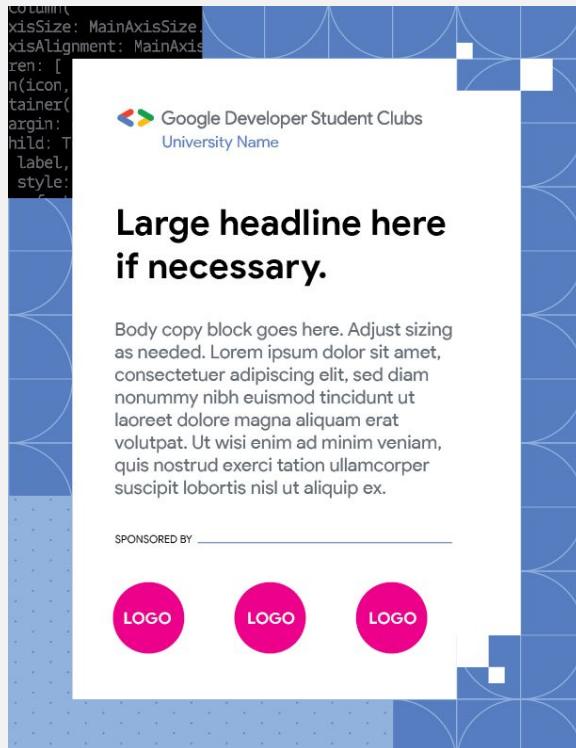
Scale reference: 72" figure

Signage: Podium / 24x18"

[Download Files](#)

One Sheet: Editable template for GDG community (8.5x11")

Download Files



Swag Kit

Stickers - Diecut

[Download Files](#)

Stickers - Rectangle

[Download Files](#)

T-shirt

[Download Files](#)

Model wearing Bella + Canvas 3413
Unisex Triblend: Charcoal-Black



Model wearing Bella + Canvas 6413
Women's Relaxed Triblend: Charcoal-Black