

Bienvenue!

Conférence BRIEF-42
#00

GDB, valgrind, memory and co.

Salut! (Oui, vous êtes bien venu jusqu'à votre chaise, bravo! +0.1XP pour chacun d'entre vous.)

Mercredi 13 Avril : 14h00

Première conférence réalisée par et pour les étudiants de 42 Angoulême.

- 1 - Introduction à l'utilisation de GDB, avec *Marc*.
- 2 - Utilisation plus avancée de GDB, avec *Maël*.
- 3 - Démonstration avec GDB, avec *Sam*.
- 4 - Un peu de théorie sur la mémoire, avec *Thomas*.
- 5 - Introduction à l'utilisation de Valgrind, avec *Maxime*.
- 6 - Astuces d'utilisation de Bash, avec *Bruno*.

Si tout se passe bien* nous ferons plusieurs conférences tout au long de l'année. Pour nous organiser ensemble autour de ces projets pédagogiques nous créerons un club dédié au sein du BDE. **Présentation en fin de conférence.**

* Ce qui inclut l'absence de décès de l'un ou plusieurs des intervenants, ni de malaise vagal dans le public, ni de faillite liée au budget sucreries de la conférence. (Quel sucreries dites-vous ? Euh y'en a plus, ne lisez pas les petits caractères!)

Durée estimée: 1h30 environ*

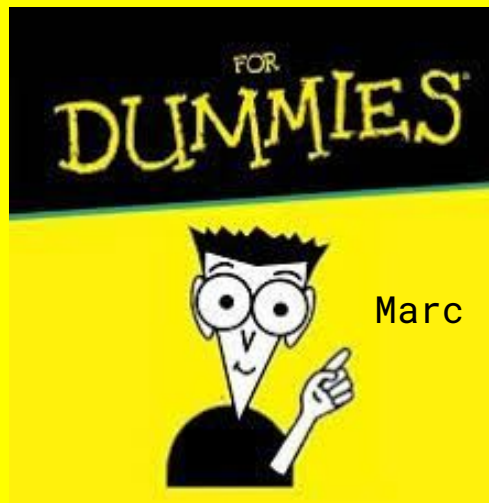
- 1 heure interventions
- 30 minutes FAQ sous forme de discussions et d'interventions libres.

00 : / 0 : 00

C'est notre première, c'est une expérience d'apprentissage dans les deux sens, please be nice. Gardez les questions et discussions pour la FAQ, SVP.

* Estimation réalisée par nos soins avec l'aide d'une horloge atomique afin de garantir une fin de conférence dans 1h30 et une marge d'erreur de très exactement 10 millièmes de secondes. (Ticket remboursé en cas de retard pour un rdv dentiste.)

1 - Introduction à GDB



G.D.B : Mais qu'est ce donc ????

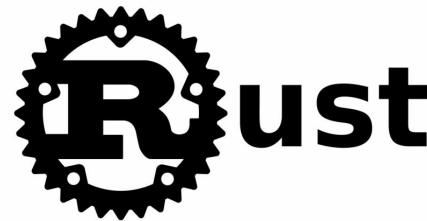
- GNU Project Debugger
- G.D.B est un debugger
- Un debugger sert à regarder ce qu'il se passe dans le programme quand il s'exécute.
- GDB créé en 1986 par Richard Stallman est un logiciel libre sous [GNU General Public License](#)



*Hésitez pas à vous
renseigner davantage
sur le projet GNU et les
début du logiciel libre.
Saint Ignucius sera content.*

G.D.B supporte :

- **Ada**
- **Assembly**
- **C**
- **C++**
- **D**
- **Fortran**
- **Go**
- **Objective-C**
- **OpenCL**
- **Modula-2**
- **Pascal**
- **Rust**



G.D.B

VS

Printf

- Utiliser un debugger fait partie des bonnes pratiques professionnelles
- Gain de temps quand on sait s'en servir
- Évite de laisser des Printf partout dans ses programmes
- Possibilité de voir l'évolution d'une variable comme par exemple dans une while
- Permet de surveiller la mémoire (stack, heap, adressage)



Déroulement:

- Compiler avec l'argument -g
- Lancer G.D.B avec l'exécutable
- Créer un Break point
- Lancer le programme
- avancer pas à pas dans le programme
- observer le comportement des variables

```
gcc -g monProgBugger.c
```

```
gdb a.out
```


Les indispensables :

Lancer GDB avec des **arguments**

Break point

Enlever les Break point

Afficher ou en est le code

Lancer le prg

Ligne suivante

répéter la commande

rentrer dans une fct

Afficher une variable

Changer la valeur d'une variable

`gdb --args a.out "POLO" "&" "PAN"`

break avec numéros de ligne ou fct

delete

list

run

next

touche enter

step

print `nomDelaVariable`

set var `nomDelaVariable` = X

T.U.I pour y voir clair

- Text User Interface
- Pour l'activer 2 méthodes
 - Soit dans le terminal
 - Soit dans GDB



```
gdb --tui a.out  
tui enable
```

T.U.I cheat sheet

Changer de fenêtre pour scroller

focus next / preview

Afficher les commandes ASM / registre

layout asm / reg

Afficher le code src et registre

layout split

Revenir au code source

layout src

Pimp my G.D.B

Possibilité de rajouter des extensions pour GDB
en modifiant ~/.gdbinit
ou avec des surcouches python

```

1  ./sysdeps/i386/elf/start.S: no such file or directory.
2  In ./sysdeps/i386/elf/start.S
3
4  gnuB b main
5  breakpoint 1 at 0xb0483aa
6
7  [reg]
8
9  EAX: 00000000 ECX: 07FC4FC8 EAX: 07FC010C EIP: 00000001 o d i s t a n p c
10 EST: 00000000 ESP: 00000000 EBP: 00000000 ESP: 00000000 EIP: 000483aa
11 CS: 0000 FS: 0070 ES: 0070 FS: 0000 SS: 0030 SS: 0070
12
13 [stack]
14
15 00FF5F50: 00 00 00 00 F8 0F 0B 08 - 01 00 00 00 D0 82 04 08
16 00FF5F54: 70 F5 FF FF 02 00 EB 07 - 00 00 00 00 00 00 00 00
17 00FF5F58: 00 00 00 00 00 00 00 00 - 00 F5 FF FF C4 F5 FF FF
18 00FF5F5C: 00 00 00 00 F4 F5 FF FF - FC F5 FF FF 00 00 00 00
19 00FF5F60: 00 00 00 00 E0 0C 00 00 - C3 F5 FF FF 14 0E EB 07
20 00FF5F64: FC FC FF FF FC FC FF - 18 05 04 00 FC FC FC FF
21
22 [reg]
23
24 00FF5F50: FC FC FF FF FC FC FF - FC FC FF FF 18 05 04 00
25 00FF5F54: 00 00 00 00 E0 0C 00 00 - C3 F5 FF FF 14 0E EB 07
26 00FF5F58: 00 00 00 00 F4 F5 FF FF - FC F5 FF FF 00 00 00 00
27 00FF5F5C: FC FC FF FF 02 00 EB 07 - 00 00 00 00 00 00 00 00
28 00FF5F60: 00 00 00 00 F8 0F 0B 08 - 01 00 00 00 D0 82 04 08
29 00FF5F64: 00 00 00 00 A0 5A FF FF - B0 6F FF FF 78 0F 00 08
30
31 00FF5F6C: 01 00 00 00 D2 84 08 00 - F2 82 04 00 F1 82 04 00
32
33 [code]
34
35 0xb0483ac: call 0x40;          and esp,0xffffffff
36 0xb0483ae: jmp 0x40;          mov eax,0x0
37 0xb0483af: add 0x40;          add eax,0xf
38 0xb0483b0: add 0x40;          add esp,0xf
39 0xb0483b1: shl 0x40;          shl eax,0x4
40 0xb0483b2: sub 0x40;          sub esp,eax
41 0xb0483b3: mov 0x40;          mov eax,0xb04844f4
42 0xb0483b4: mov 0x20;          mov ebx,0xb04844f4
43 0xb0483b5: mov 0x20;          mov ebx,0xb04844f4
44 0xb0483b6: mov 0x20;          mov ebx,0xb04844f4
45 0xb0483b7: mov 0x20;          mov ebx,0xb04844f4
46 0xb0483b8: mov 0x20;          mov ebx,0xb04844f4
47 0xb0483b9: mov 0x20;          mov ebx,0xb04844f4
48 0xb0483ba: mov 0x20;          mov ebx,0xb04844f4
49 0xb0483bb: mov 0x20;          mov ebx,0xb04844f4
50 0xb0483bc: mov 0x20;          mov ebx,0xb04844f4
51 0xb0483bd: mov 0x20;          mov ebx,0xb04844f4
52 0xb0483be: mov 0x20;          mov ebx,0xb04844f4
53 0xb0483bf: mov 0x20;          mov ebx,0xb04844f4
54 0xb0483c0: mov 0x20;          mov ebx,0xb04844f4
55 0xb0483c1: mov 0x20;          mov ebx,0xb04844f4
56 0xb0483c2: mov 0x20;          mov ebx,0xb04844f4
57 0xb0483c3: mov 0x20;          mov ebx,0xb04844f4
58 0xb0483c4: mov 0x20;          mov ebx,0xb04844f4
59 0xb0483c5: mov 0x20;          mov ebx,0xb04844f4
60 0xb0483c6: mov 0x20;          mov ebx,0xb04844f4
61 0xb0483c7: mov 0x20;          mov ebx,0xb04844f4
62 0xb0483c8: mov 0x20;          mov ebx,0xb04844f4
63 0xb0483c9: mov 0x20;          mov ebx,0xb04844f4
64 0xb0483ca: mov 0x20;          mov ebx,0xb04844f4
65 0xb0483cb: mov 0x20;          mov ebx,0xb04844f4
66 0xb0483cc: mov 0x20;          mov ebx,0xb04844f4
67 0xb0483cd: mov 0x20;          mov ebx,0xb04844f4
68 0xb0483ce: mov 0x20;          mov ebx,0xb04844f4
69 0xb0483cf: mov 0x20;          mov ebx,0xb04844f4
70 0xb0483d0: mov 0x20;          mov ebx,0xb04844f4
71 0xb0483d1: mov 0x20;          mov ebx,0xb04844f4
72 0xb0483d2: mov 0x20;          mov ebx,0xb04844f4
73 0xb0483d3: mov 0x20;          mov ebx,0xb04844f4
74 0xb0483d4: mov 0x20;          mov ebx,0xb04844f4
75 0xb0483d5: mov 0x20;          mov ebx,0xb04844f4
76 0xb0483d6: mov 0x20;          mov ebx,0xb04844f4
77 0xb0483d7: mov 0x20;          mov ebx,0xb04844f4
78 0xb0483d8: mov 0x20;          mov ebx,0xb04844f4
79 0xb0483d9: mov 0x20;          mov ebx,0xb04844f4
80 0xb0483da: mov 0x20;          mov ebx,0xb04844f4
81 0xb0483db: mov 0x20;          mov ebx,0xb04844f4
82 0xb0483dc: mov 0x20;          mov ebx,0xb04844f4
83 0xb0483dd: mov 0x20;          mov ebx,0xb04844f4
84 0xb0483de: mov 0x20;          mov ebx,0xb04844f4
85 0xb0483df: mov 0x20;          mov ebx,0xb04844f4
86 0xb0483e0: mov 0x20;          mov ebx,0xb04844f4
87 0xb0483e1: mov 0x20;          mov ebx,0xb04844f4
88 0xb0483e2: mov 0x20;          mov ebx,0xb04844f4
89 0xb0483e3: mov 0x20;          mov ebx,0xb04844f4
90 0xb0483e4: mov 0x20;          mov ebx,0xb04844f4
91 0xb0483e5: mov 0x20;          mov ebx,0xb04844f4
92 0xb0483e6: mov 0x20;          mov ebx,0xb04844f4
93 0xb0483e7: mov 0x20;          mov ebx,0xb04844f4
94 0xb0483e8: mov 0x20;          mov ebx,0xb04844f4
95 0xb0483e9: mov 0x20;          mov ebx,0xb04844f4
96 0xb0483ea: mov 0x20;          mov ebx,0xb04844f4
97 0xb0483eb: mov 0x20;          mov ebx,0xb04844f4
98 0xb0483ec: mov 0x20;          mov ebx,0xb04844f4
99 0xb0483ed: mov 0x20;          mov ebx,0xb04844f4
100 0xb0483ee: mov 0x20;          mov ebx,0xb04844f4
101 0xb0483ef: mov 0x20;          mov ebx,0xb04844f4
102 0xb0483f0: mov 0x20;          mov ebx,0xb04844f4
103 0xb0483f1: mov 0x20;          mov ebx,0xb04844f4
104 0xb0483f2: mov 0x20;          mov ebx,0xb04844f4
105 0xb0483f3: mov 0x20;          mov ebx,0xb04844f4
106 0xb0483f4: mov 0x20;          mov ebx,0xb04844f4
107 0xb0483f5: mov 0x20;          mov ebx,0xb04844f4
108 0xb0483f6: mov 0x20;          mov ebx,0xb04844f4
109 0xb0483f7: mov 0x20;          mov ebx,0xb04844f4
110 0xb0483f8: mov 0x20;          mov ebx,0xb04844f4
111 0xb0483f9: mov 0x20;          mov ebx,0xb04844f4
112 0xb0483fa: mov 0x20;          mov ebx,0xb04844f4
113 0xb0483fb: mov 0x20;          mov ebx,0xb04844f4
114 0xb0483fc: mov 0x20;          mov ebx,0xb04844f4
115 0xb0483fd: mov 0x20;          mov ebx,0xb04844f4
116 0xb0483fe: mov 0x20;          mov ebx,0xb04844f4
117 0xb0483ff: mov 0x20;          mov ebx,0xb04844f4
118 0xb048400: mov 0x20;          mov ebx,0xb04844f4
119 0xb048401: mov 0x20;          mov ebx,0xb04844f4
120 0xb048402: mov 0x20;          mov ebx,0xb04844f4
121 0xb048403: mov 0x20;          mov ebx,0xb04844f4
122 0xb048404: mov 0x20;          mov ebx,0xb04844f4
123 0xb048405: mov 0x20;          mov ebx,0xb04844f4
124 0xb048406: mov 0x20;          mov ebx,0xb04844f4
125 0xb048407: mov 0x20;          mov ebx,0xb04844f4
126 0xb048408: mov 0x20;          mov ebx,0xb04844f4
127 0xb048409: mov 0x20;          mov ebx,0xb04844f4
128 0xb04840a: mov 0x20;          mov ebx,0xb04844f4
129 0xb04840b: mov 0x20;          mov ebx,0xb04844f4
130 0xb04840c: mov 0x20;          mov ebx,0xb04844f4
131 0xb04840d: mov 0x20;          mov ebx,0xb04844f4
132 0xb04
```

Notice from NickServ
This nickname is registered. Please
choose a different nickname, or

<https://stackoverflow.com/questions/209534/how-to-highlight-and-color-gdb-output-during-interactive-debugging/17341335#17341335>

2 - Utilisation de GDB

Maël



hackerman tips : `bash -c "$(curl -fsSL http://gef.blah.cat/sh)"` -
to install GDB-GEF and became *pimped hackerman*

Summary of regularly shorted used gdb command

- ❖ breakpoint -> b
- ❖ watchpoint -> watch
- ❖ run -> r
- ❖ continue -> c
- ❖ next -> n
- ❖ step -> s
- ❖ list -> l
- ❖ print -> p
- ❖ backtrace -> bt
- ❖ info -> i

'print' and 'x' like a rockstar

❖ **print** - *like printf u know*

use it as : **print** **optType1** **targetName** **optType2**

- **optType1** is an 'in-case' type to format target
- **targetName** can be a pointer, an address or a variable name
- **optType2** another 'in-case' type formatter

example : **p** ***toto@100** - *print 100 first formatted element of toto*

❖ **x** - *examine at a certain memory address like printf++*

use it as : **x/nbrToShow** **optType1** **targetAddress**

- **optType1** can be : d (dec-10), a (ptr), c (char), s (char *), x(hex), o (oct-8)
- **nbrToShow** is the number of **optType1** that you want to show from **targetAddress**

example : **x/16c** **&toto** - *show 16 formatted char from toto address*

'set' like a rockstar

❖ **set** - *like '=' u know*

use it as : **set** **optTarget1** **targetName** = **myCoolValue**

➤ **optTarget1** can be lot of things, first thing
first : var

➤ **targetName** is the name of the object

➤ **myCoolValue** is what you want to write in target

example : **set** **var** **toto** = "tutu"

'break' and 'watch' to stop the damn process

- ❖ **break** - *insert breakpoint into an instruction*

use it as : **b** * **target**

➤ **target** can be an address, a line or a call to a function,

example : **b** * 15 (break line 15), **b** * 0xdeadbeef (break at 0xdeadbeef address), **b** * main (break when main is called to the stack)

- ❖ **watch** - *insert a watchpoint into an instruction*

this command work like breakpoints in any point except that you need to use watch command and this will break if targeted value has changed.

BONUS tips

- ❖ **whatis** - *what's the type of ?*

useful command to see a type of variable

- ❖ **set \$pc** = 0xdeadbeef - *jump EVERYWHERE*

super useful command to jump to 0xdeadbeef address

- ❖ *logical condition*

you can choose to add logical conditions in your gdb statement like
b * 0xdeadbeef if (i == 2)

- ❖ **define**

define is a command that allow you to create macro-like in gdb

3 - Démo GDB

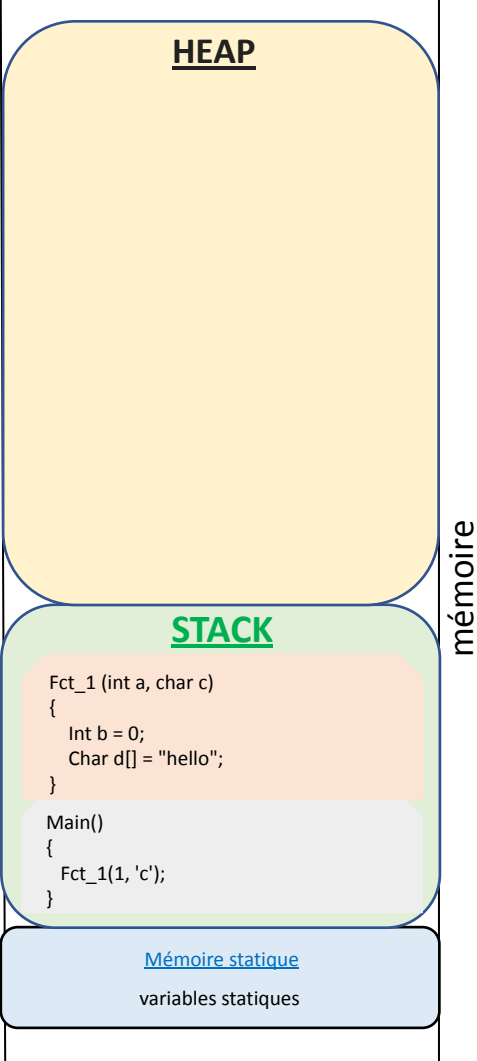
Sam

4 - Un peu de théorie sur la mémoire

Thomas

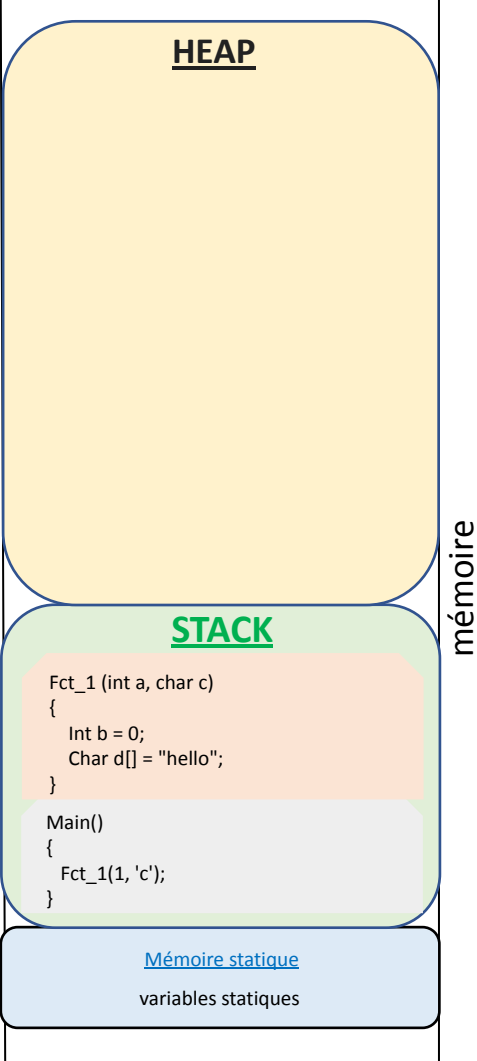
```
Fct_1(int a, char c)
{
    Int b = 0;
    Char d[] =
"hello";
}
```

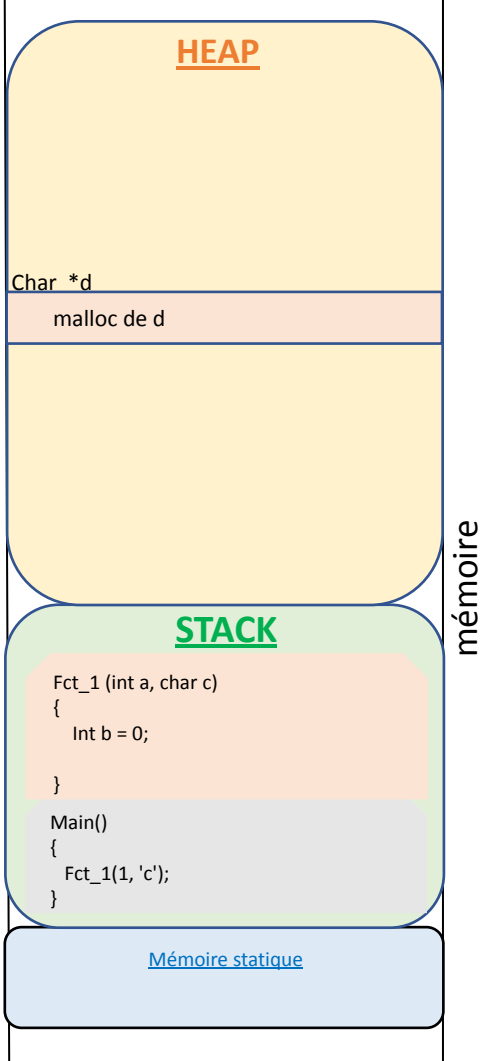
```
Main()
{
    Fct_1(1, 'c');
}
```



```
Fct_1(int a, char c)
{
    Int b = 0;
    Char d[] =
"hello";
}
```

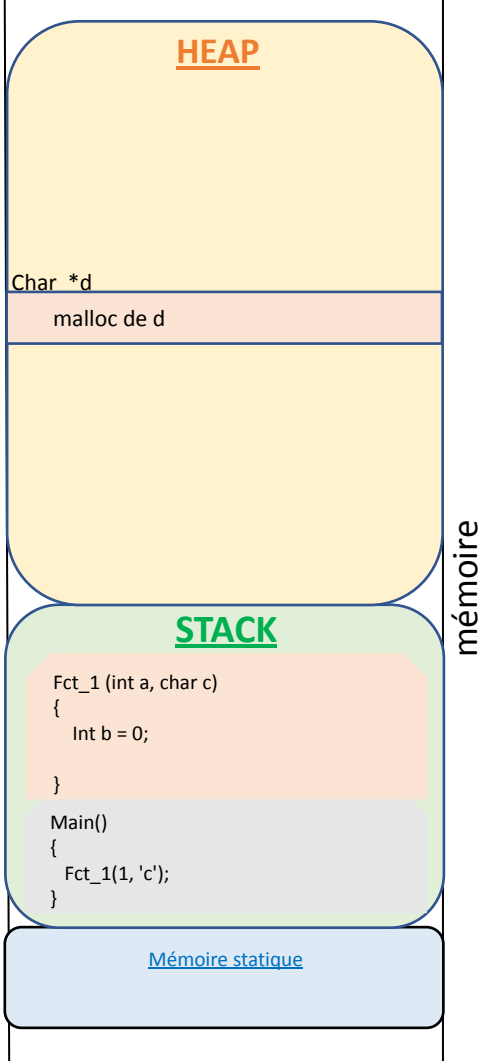
```
Main()
{
    Fct_1(1, 'c');
}
```





```
Fct_1(int a, char c)
{
    Int b = 0;
    Char *d;
    d = malloc....;
}
```

```
Main()
{
    Fct_1(1, 'c');
}
```

```
Fct_1(int a, char c)
{
    Int b = 0;
    Char *d;
    d = malloc....;
}
```

```
Main()
{
    Fct_1(1, 'c');
}
```

5 - Introduction à Valgrind

Maxime

SOMMAIRE

SYNTAXES MEMORY IN C

VAR GLOBAL ET STATIC

POURQUOI MALLOC ET FREE ()?

LES TYPES D'ERREURS DANS VALGRIND !

6 - Time for some Bash

Bruno



Command interpreter history

- a. Shell
- b. Bash
- c. Zsh

How to “chain” command

- a. Flux and piping
- b. ‘&&’ / AND operator
- c. ‘||’ / OR operator

Brace Expansion + BONUS

- a. basic of list exp
- b. Search and replace
- c. dir stack :)

Bonus Track: Présentation TED-42

Bon et bien au revoir, merci d'être venu! (-666XP si vous vous levez maintenant traîtres!)

TED-42 copyright (ou **BRIEF** copyleft)

TEchnology + **ED**ucation

(malheureusement ça marche qu'avec TED sinon Bière Ristournes Identité Embrouilles et F...)

Projet de club du BDE pour accompagner à la création et à la diffusion de conférences et de rencontres pour les étudiants de **42** Angoulême.

Oula c'est sérieux là, aucune images, documents noir et blanc. (et rien à manger en attendant, désolé la prod est parti avec la cais...)

Mais avant tout, une petite mise au point entre nous.



Chacun avance à son rythme.

Si on perd un wagon, on perd le principe du pair à pair.

Et on entre sur un autre principe, celui du chacun pour soi.

Ce n'est pas un jugement, c'est nous qui décidons ce que nous faisons de cette école.

Alors la question qu'on se pose ensemble c'est, on fait quoi ?

Bon ok deux images en couleur, pas plus, on va nous tomber dessus pour les droits intellectuels. :(

Objectifs :

- 1 . Apprendre à travailler ensemble** autour de la création et le partage d'outils et de contenu pédagogiques qui s'inscrivent sur le long du cursus 42 Angoulême: tronc commun, spécialités et autres selon les besoins de chacun.
- 2 . Accompagner** dans une forme ouverte tout les étudiants d'aujourd'hui et de demain sans discrimination de niveau technique, de promo ou même de coalition pour permettre un flux de communication à travers toute l'école et afin de **diffuser et structurer un savoir commun.**
- 3 . Tisser des liens** entre étudiants mais aussi avec des professionnels extérieurs pour aller plus loin dans l'exploration de ses connaissances et pratiques afin d'aider à l'élaboration de son projet personnel.

Rejoignez nous pour:

- Vous entraîner à consolider davantage vos connaissances pour vous même tout en les partageant avec nous autres, et tout en acquérant des “soft skills” de communication.
- Travailler avec le club pour apprendre avec nous comment construire un réseau qui connectera des ponts entre les étudiants et des professionnels du milieu tech.
- Participer à un projet pédagogique pair à pair innovant et ambitieux afin de suivre son évolution au fur et à mesure de ses itérations.
- Ou simplement venir discuter et partager vos critiques constructives, vos besoins ou vos idées pour de futurs conférences et projets.

Contactez nous sur le discord du futur club: [lien ici?](#)

Prochaine conférence:
dans 3 semaines "environ"

BRIEF-42: Conf#01
Le thème sera décidé ensemble!

Venez en discuter, la préparer et la construire avec nous.

Non, il n'est pas sur l'écran, il est sur le Discord de la promo dans 3, 2, 1...

Au revoir!

FAQ

Pour ceux qui le souhaitent.