

Debugovanje u LLDB-u

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Momir Adžemovic, Miloš Miković, Marko Spasić,
Mladen Dobrašinović

momir.adzemovic@gmail.com, spaskeasm@gmail.com,
milos.mikovicpos@gmail.com, dobrasinovic.mladen@gmail.com

1. april 2020.

Sažetak

Ovaj rad predstavlja grupni projekat u okviru kursa Metodologija stručnog i naučnog rada. Ovo je dobra prilika da podelimo sa kolegama naša znanja koja smo stekli ovim istraživanjem koje ima velike primene u praksi. Rad većinom pokriva interesatne informacije o debageru LLDB kao jednom od produžetaka LLVM-a, način korišćenja LLDB i poređenje sa ostalim debagerima.

Sadržaj

1	Uvod	2
2	Šta je debugovanje	2
2.1	Bagovi uopšteno	2
2.2	Metode debugovanja	2
2.3	Tehnike za prevenciju bagova	3
2.4	Debager	4
2.5	Lista debagera	4
3	Upoznavanje sa LLDB-om	4
3.1	LLDB interfejs komandne linije	5
4	Gde se on koristi i za koje jezike?	5
5	Koja razvojna okruženja podržavaju upotrebu ovog debagera i kako?	7
5.1	Visual Studio Code	7
5.2	Eclipse	7
5.3	CLion	7
5.4	Xcode 5	8
6	Poređenje sa drugim popularnim debagerima	8
6.1	Poređenje: GDB i LLDB	8
6.2	Visual Studio Debugger i LLDB	9
7	Zaključak	9
	Literatura	9

1 Uvod

Nakon pročitano g rada čitalac će biti upoznat sa osnovnim tehnikama debagovanja i specifičnostima debagovanja sa LLDB-om. Predstavljena su poređenja LLDB-a sa drugim debagerima kako bi čitalac lakše mogao da donese odluku da li je LLDB pravi izbor za posao kojim se bavi u zavisnosti od platforme na kojoj radi. Za one koji preferiraju rad u integrisanom razvojonom okruženju poglavlje 5

2 Šta je debagovanje

Debagovanje je proces identifikacije pravog problema i njegovo ispravljanje. "Debagovanje je duplo teže od kodiranja, ako napisete kod na najlukaviji (odnosno najkomplikovaniji) način, po definiciji niste dovoljno pametni da ga debagujete. (Brian w. Keringhan) [2]
Koraci pri debagovanju[12]:

1. uočavanje da postoji greška
2. razumevanje greške
3. lociranje greške
4. ispravljanje greške

Često je najteži deo ispravno razumevanje i rano otkrivanje greške, kada se greška locira, ispravljanje najčešće nije veliki problem.

2.1 Bagovi uopšteno

Postojanje grešaka(bagova) se često neopravdano poistovećuje sa propustima u programiranju. U širem kontekstu bag, greška, defekt ili propust se odnosi na bilo koju vrstu problema u bilo kojoj fazi procesa razvoja kao što su greške u projektovanju, planiranju, arhitekturi, dizajnu... Zato se često termini propust i greška koriste u širem kontekstu razvoja a termin bag u užem i vezan je za propuste u programiranju.

Jedna od najčešćih klasifikacija bagova prema načinu ispoljavanja obuhvata:

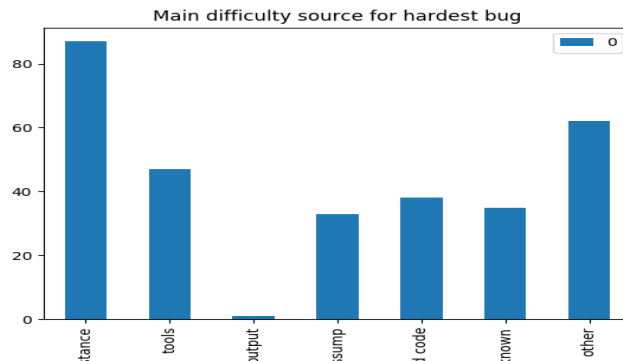
1. **Nekonzistentnosti u korisničkom interfejsu:** često je slučaj da se komanda `ctr+f` koristi za pretraživanje dokumenta, Outlook koristi tu komandu za prosleđivanje poruke
2. **Neispunjena očekivanja:** dobijanje neočekivanog(pogrešnog) rezultata
3. **Slabe performanse:** stalno ili povremeno čekanje rezultata zbog lošeg odziva sistema, takvi programi su često ne upotrebljivi
4. **Padovi sistema i oštećenja podataka:** predstavljaju najopasniji vid bagova, mogu trajno oštetiti sistem i podatke

Bagovi su jako neugodni i treba ih sistematski otklanjati čestim refaktorisanjem i planskim gradjenjem koda. Jedne od okolnosti koje pogoduju nastajanju bagova su nedovoljna stručnost razvojnog tima i povećan stres na poslu, a informisanost, sistematičnost i redovnost ih suzbijaju. [12]

Sa slike (1) vidimo da su najčešći razlozi za teške bagove upravo rastojanje od izvora greške do neočekivanog ponašanja. U ovim situacijama su veoma bitne metode debagovanja, pa i alati koji se koriste za debagovanje (debageri).

2.2 Metode debagovanja

1. **Neformalno debagovanje:** Neformalno debagovanje predstavlja jednostavan i površan pristup i čine ga dva koraka.
(a) Pokušati sa nekom jednostavnom popravkom;



Slika 1: Glavni razlozi najtežih bagova[?]

- (b) Ponavljati korak (a) dok se problem ne reši.

Ovaj metod se ne preporučuje u praksi i često može da proizvede nove probleme, pogotovo ako vršimo puno sitnih popravki za koje nismo sigurni da će rešiti problem. Ponekad, ako su u pitanju sitne greške, ovaj metod se može oprezno koristiti jer dovodi do brzog rešenja problema.[12]

2. **Empirijski naučni metod:** Ovaj postupak je sličan uobičajenom istraživačkom metodu u prirodnim naukama. Čine ga sledeći koraci:

- (a) Posmatrati uočen problem;
- (b) Postaviti hipoteze o uzroku problema;
- (c) Na osnovu hipoteza napraviti predviđanje;
- (d) ponašanja;
- (e) Eksperimentalno proveriti ispravnost predviđanja Ponavljati prethodne korake uz popravljjanje ili menjanje hipoteze, sve dok se ne potvrdi ispravnost hipoteze ili ne ponestanu mogućnosti za njeno dalje unapređivanje.

Uopšteno gledano ovo je najbolji pristup debugovanju. Često je jako zahtevan i oduzima dosta vremena ali je sa druge strane je temeljan i koncizan.[12]

3. **Heurističko debugovanje:** Ova vrsta debugovanja podrazumeva postojanje heuristike(skup pravila) koja olakšava brže i efikasnije pronalaženje grešaka. Često se za određene skupove problema prave različite heuristike, koje se testiraju u praksi i kasnije koriste kao pravila pri otklanjanju određenih vrsta bagova. Ovakve heuristike odlikuje izbegavanje pravljenja previda pri posmatranju, sužavanje skupa kandidata za iskazivanje hipoteza, usmeravanje posmatranja prema uzroku problema i dr. Heuristike nisu optimalna rešenja niti egzaktna pravila koja vode rešenju problema, ali često su jako efikasne i daju "dovoljno dobra rešenja".[12]

2.3 Tehnike za prevenciju bagova

Tehnike za prevenciju bagova mogu biti unutrašnje i spoljašnje. Unutrašnje predstavljaju sve ono što se ugrađuje u programski kod samo radi pomoći u prevenciji i otklanjanju grešaka. Neke od njih su pravljenje pretpostavki(asserts), komentisanje značajnih odluka i mesta u kodu, testiranje jedinica koda... Spoljašnje tehnike i alati se koriste pri razvoju i ne ugrađuju se nužno u programski kod, ali se koriste u čitavom razvojnem ciklusu. Neki od spoljašnjih alata su debugger, alati za praćenje verzija programskog koda, alati za podršku i praćenje komunikacije, alati za automatizovanje pravljenja dokumentacije[12].

2.4 Debager

Debager je računarski program koji se koristi za uklanjanje grešaka, testiranje rada i proveru ispravnosti drugih programa. Debuggeri daju napredne funkcije kao što su pokretanje programa korak po korak (single-stepping), praćenje vrednosti promenljivih kao i stek okvira, praćenje na nivou instrukcija i stanja procesora, zaustavljanje ili pauziranje izvršavanja programa na takozvanim tačkama prekida (breakpoint), a neki čak i omogućavaju menjanje programa tokom izvršavanja.

Većina popularnih debuggera daje samo jednostavno komandno-linijsko okruženje (command-line interface - CLI), često iz razloga da maksimizuju portabilnost i minimizuju trošenje sistemskih resursa računara. Ipak, popravljjanje grešaka u programu preko grafičkog korisničkog okruženja (GUI) debuggera se često smatra jednostavnijim, produktivnijim i ugodnijim za rad. Neki debuggeri pružaju i mogućnosti obrnutog debugovanja (debugovanje unazad) koje omogućava da se vratimo na prethodno stanje programa (Step Backward). Jedan od debuggera koji pruža ovu mogućnost je IntelliTrace koji se koristi u Microsoft-ovom razvojnom okruženju VisualStudio. Debugovanje unazad je jako korisno i sve se više koriste debuggeri koji omogućavaju ovo svojstvo. Mana debugovanja unazad je usporavanje čitavog procesa debugovanja pa čak i do dva puta. Debuggeri mogu biti zavisni od programskog jezika, ako se mogu koristiti za debugovanje jednog konkretnog jezika ili mogu biti višezjezični i koristiti se za debugovanje više programskih jezika. Neki debuggeri uključuju i zaštitu memorije kako bi izbegli prekoračenje bafera, ili onemogućili korisnika da pristupa memoriji za koju nema dozvolu i slično.[16]

2.5 Lista debagera

Najčešće korišćeni debuggeri[8][4]:

1. GDB(gnu debugger)
2. Firefox javascript
3. Lldb
4. IntelliTrace
5. Windbg
6. Valgrind
7. Watcom

Mejnfrejm debuggeri[8][4]:

1. XPEDITER
2. z/XDC
3. IBM Oliver
4. CA/EZTEST

3 Upoznavanje sa LLDB-om

LLDB podržava standardne funkcije debugovanja preko komandne linije i može se koristiti kao debager u interaktivnom razvojnom okruženju. Konkretno, sa debagerom pokrenutim nad programom prevedenim sa debug opcijama omogućava se [9]:

- Aktiviranje procesa programa sa određenim argumentima komandne linije (eng. command line arguments).
- Korišćenje breakpoint-a (određenog reda ili funkcije u izvornom kodu pri kojima debager zaustavlja izvršavanje programa kada se stigne do odgovarajućeg dela izvršnog koda).

- Korišćenje watchpoint-a (određene promenljive, takve da debager zaustavlja proces ili nit kada se njeno stanje promeni).
- Korišćenje dodatnih uslova nad breakpoint-ovima i watchpoint-ovima.
 - Nastavljanje ili pokretanje programa.
- Pokretanje procesa red po red (sa „ulaženjem” u funkciju ili bez).
- Istraživanje promenljivih ili memorije procesa.
- Izvršavanje proizvoljnog izraza nad stanjem procesa (npr. menjanje neke promenljive na steku).
- Istraživanje steka okvira poziva.
- Izvršavanje drugih naprednih i raznih funkcija.

Ono što ističe LLDB je omogućavanje korišćenja eksternih skripti za debugovanje preko javnog API-a za Python, izvršavanje proizvoljnog Python koda unutar debagera [17] (preko ugnježdenog interpretatora (eng. *embedded interpreter*) i omogućavanje REPL (Read-Evaluate-Print-Loop) funkcija za programske jezike zajedno sa mogućnostima debugovanja [5].

3.1 LLDB interfejs komandne linije

LLDB interfejs komandne linije (eng. *command line interface*) se aktivira pozivom `lldb` u ljusci (eng. *shell*) sa programom koji želimo debugovati kao argumentom. Program komandne linije `lldb` se odlikuje strukturisanom sintaksom osnovnih komandi koja je sledećeg oblika [18]:

Primer 3.1

```
<imenica> <glagol> [-opcije [vrednost-opcije]] [argument [argument...]]
```

U ovakvom obliku, imenica se zove i komanda, a glagol potkomanda. Postoje i skraćenice (eng. *alias*) za komande koje mogu odstupati od ovog oblika. Upravo zato što je ovaj format komandi jako strukturisan mogu nam biti pogodni skraćeni oblici komandi koji mogu biti sličniji onome što je poznato korisnicima drugih debagera [6]. U tabeli 1 su date neke od osnovnih komandi kao primer korišćenja interfejsa i reprezentativni prikaz širokog skupa mogućnosti LLDB-a koji nije naveden u potpunosti u ovom radu. Posebno se ističu komande `help` i `apropos`, koje mogu biti korisne početnicima u korišćenju ovog alata.

4 Gde se on koristi i za koje jezike?

LLDB se koristi za debugovanje programa pisanih u programskim jezicima C, Objective-C, i C++. Postoji i verzija za debugovanje programa napisanih u Swift programskom jeziku, tu verziju održava Swift zajednica. Dostupan je na FreeBSD, Linux, macOS, NetBSD, i od 2015 na Windows platformi. Kompletnost skupa funkcionalnosti varira od platforme do platforme.

- FreeBSD - zaostaje za Linux-om, ali brzo napreduje.
- Linux - Približava se kompletnosti funkcionalnosti za debugovanje x86-64, i386, ARM, AArch64, IBM POWER (ppc64), IBM Z (s390x=, i MIPS64 programa.
- macOS - LLDB je sistemski debager na macOS, iOS, tvOS, i watchOS za x86, i386, ARM, i AArch64 debugovanje. Na ovoj platformi ima najbogatiji skup funkcionalnosti koje implementira.
- Windows - I dalje u razvojnoj fazi, ali već koristan za i386 programe.

Skup funkcionalnosti se iz godine u godinu unapređuje i teži se da bude kompletan na svim platformama. Najbolja i najpotpunija podrška je trenutno na Linux i macOS platformama što se može videti iz tabele 2.

Tabela 1: Upotreba interfejsa komandne linije LLDB-a [9][18].

<code>process launch -- <argumenti></code>	Pokreće izabrani program sa datim argumentima.
<code>thread step-in</code>	U trenutnoj niti nastavlja izvršavanje programa sledeće instrukcije izvornog koda, ulazeći u pozive funkcija.
<code>thread step-inst-over</code>	U trenutnoj niti nastavlja izvršavanje programa sledeće instrukcije izvršnog koda, ne ulazeći u pozive funkcija.
<code>breakpoint set --file 1.c --line 42</code>	Postavlja breakpoint na red 42 u izvornom kodu programa 1.c.
<code>breakpoint list</code>	Ispisuje postojeće breakpoint-ove debagera.
<code>breakpoint disable 1</code>	Deaktivira breakpoint 1.
<code>apropos <ključna_reč></code>	Traži u pomoći za upotrebu komandi (eng. command help) datu ključnu reč.
<code>help</code>	Štampa pomoć za komande. (help se može koristiti i za nalaženje pomoći za upotrebu potkomandi određene komande [6]).

Tabela 2: Funkcionalosti LLDB na najpopularnijim platformama

Feature	Linux	macOS	Windows
Backtracking	Yes	Yes	Yes
Breakpoints	Yes	Yes	Yes
C++11	Yes	Yes	Unkown
Commandline tool	Yes	Yes	Yes
Core file debugging	Yes	Yes	Yes
Remote debugging	Yes	Yes	No
Disassembly	Yes	Yes	Yes
Expression evaluation	Yes (Known problems)	Yes	Yes (known issues)
JIT debugging	Symbolic debugging only	Untested	No
Objective C	N/A	Yes	N/A

Korisnici Windows platformi obično preferiraju alate napravljene od strane Microsoft-a jer su najbolje integrisani sa Windows-om i imaju najbolju podršku na tom operativnom sistemu.

Na Linux i macOS najčešće korišćene funkcionalnosti debagera su implementirane u LLDB. Na macOS platformi je LLDB najbolji izbor zato što ima najpotpuniji skup funkcionalnosti u odnosu na druge platforme i održavan je od strane Apple-a. Na Linux-u je izbor između LLDB i nekog drugog popularnog debagera, kao što je na primer GDB, stvar preferenci programera jer oba debagera implementiraju sve najčešće korišćene funkcionalnosti i imaju sličan interfejs za korišćenje.

5 Koja razvojna okruženja podržavaju upotrebu ovog debagera i kako?

LLDB se može koristiti kao alat komandne linije ili uz neko razvojno okruženje. Neka od najpopularnijih razvojnih okruženja koja imaju mogućnost integracije LLDB su Visual Studio Code, Eclipse, CLion, i Xcode 5. Pošto Apple održava LLDB verziju za svoje operativne sisteme LLDB je podrazumevani debager u XCode 5 razvojnom okruženju. U daljem tekstu je dat opis načina instalacije na svakom od gore navedenih okruženja i kratak opis koje funkcionalnosti LLDB debagera podržavaju. Za detalje i detaljna uputstva pogledati zvanične veb stranice ovih razvojnih okruženja.

5.1 Visual Studio Code

Instalacija u Visual Studio Code (VSC) se svodi na instaliranje dodataka sa VSC repozitorijuma[15]. Komande LLDB se zadaju preko VCS grafičkog korisničkog interfejsa. Podržava:

- Debugovanje na Linux (x64 or ARM), macOS i Windows,
- Uslovni breakpoint-i, breakpoint-i na funkcijama, breakpoint'i na podacima
- Pokretanje iz internog ili eksternog terminala,
- Dissassembly pogled i kretanje instrukciju po instrukciju,
- Python skripte,
- HTML renerovanje za naprednu vizuelizaciju,
- Podrška za Rust programski jezik sa vizuelizacijama za vektor, string i liste

5.2 Eclipse

U Eclipse razvojnom okruženju se korišćenje omogućava instaliranjem Eclipse dodataka[1] koji integrše postojeći lldb na sistemu sa eclipse razvojnim okruženjem. Radi na svim platformama koje podržava lldb i eclipse. Za razliku od VCS ima nekoliko ograničenja:

- Debugovanje sa drugog računara nije moguće
- Core dump debugovanje nije moguće
- Watch points ne radi
- Ne može se izmeniti vrednost promenljivih tokom debugovanja
- Ne može se menjati sadržaj memorije
- Skoči na liniju, pomeri se na liniju nije implementirano Modules view se ne popuni

5.3 CLion

LLDB dolazi u paketu zajedno sa CLion razvojnim okruženjem na Linux i macOS platformama[7]. Postoji i eksperemintalna verzija LLDB baziranog debagera sa MSVC razvojne alate na Windows platformi.

Da bi omogućili korišćenje lldb potrebno je u podešavanjima za dati projekat odabrati postojeći lldb debager. Ne postavlja nikakva ograničenja na LLDB debager kao što je to slučaj kod Eclipse razvojnog okruženja. Dostupne funkcionalnosti variraju od platforme kao što se može videti u tabeli 2.

5.4 Xcode 5

Sa verzijom 5 Xcode razvojnog okruženja LLDB debager je podrazumevani debager u Xcode razvojnem okruženju. LLDB je Eplova zamena za GDB koja je razvijana u koordinaciji sa LLVM kompajlerima. Počevši od Xcode 5 svi novi i postojeći projekti se automatski rekonfigurišu tako da koriste LLDB. Dizajniran je tako da korišćenje bude što sličnije GDB debageru kako bi omogućio programerima da se lako prebace sa GDB na LLDB debager. LLDB debager u Xcode 5 ima najbogatiji skup implementiranih funkcionalnosti u odnosu na druge platforme.

6 Poredjenje sa drugim popularnim debagerima

Potrebno je naglasiti da pri poređenju različitih debagera ne možemo objektivno odrediti koji je debager bolji, jer to dosta zavisi od toga koji se operativni sistem koristi, a i samih preferenci korisnika. Visual Studio Code, jedan od popularnijih editora, koristi LLDB, GDB i VSD za C++ u zavisnosti od od operativnog sistema na kojem je instaliran [13]:

- **Linux:** GDB
- **macOS:** LLDB or GDB
- **Windows:** the Visual Studio Windows Debugger or GDB (using Cygwin or MinGW)

	LLDB	GDB	Visual Studio Debugger
Podrška za programske jezike	C, C++, Objective C	C, C++, Objective C, Java, Fortran etc.	C#, C++, Visual Basic, JavaScript etc.
Implementacija	C++	C	C++/C#
Podrška za operativne sisteme	Unix, Windows, MacOS	Unix, Windows, MacOS	Windows
Razvijen od strane	GNU Project	LLVM developer group	Microsoft
UI	TUI	TUI	GUI

Slika 2: LLDB, GDB, Visual Studio Debugger [3][10][14]

6.1 Poređenje: GDB i LLDB

Debugger GDB predstavlja standard za GNU sisteme (ne striktno samo za GNU) [3]. Ako se proverava kvalitet debagera LLDB, onda u potpunosti ima smisla upoređivati ga prvo sa GDB debagerom kao jednim od najpopularnijih debagera. Debager LLDB u debagovanju velikih programa pokazuje bolje performanse od GDB debagera i ima dobar korisnički interfejs [11]. Novije verzije GDB podržavaju MacOS, ali u proteklih par godina se pretežno koristio LLDB kao glavni debager za MacOS. Postoji zvaničan rečnik koji prevodi komande iz GDB u LLDB. [9] Primer:

	GDB	LLDB
Pokretanje procesa:	run	run
Postavljanje argumenata:	set args <args>	settings set target.run-args <args>
sljedeći korak:	step	step
izlazak iz grejma	finish	finish

Ova tabela predstavlja uzorak iz mape preslikavanja. Vidi se je način korišćenje ova dva debagera je veoma sličan i skup komandi se većinom poklapa.

6.2 Visual Studio Debugger i LLDB

Visual studio debugger je takođe jedan od poznatijih debagera koji se može uporediti sa LLDB-om. Prednost VSD u odnosu na LLDB je u tome što VSD nudi grafički „point-and-click“ korisnički interfejs, a prednost LLDB je u broju operativnih sistema koji za koju ima podršku [14].

7 Zaključak

Literatura

- [1] Eclipse. Eclipse Plugin, 2020. https://wiki.eclipse.org/CDT/User/FAQ#How_do_I_get_the_LLDB_debugger.3F.
- [2] Vladimir Filipovic. Debagovanje, 2016. <http://poincare.matf.bg.ac.rs/~vladaf/Courses/Matf%20RS2/Prezentacije/CC%2023%20-%20Debagiranje%20-%20Goran%20Vinterhalter.pdf>.
- [3] Free Software Foundation. GDB: The GNU Project Debugger, 2020. on-line at: <https://www.gnu.org/software/gdb/>.
- [4] Rubaiat Hossain. Best Linux Debuggers for Modern Software Engineers, 2020. <https://www.ubuntupit.com/best-linux-debuggers-for-modern-software-engineers/>.
- [5] Apple Inc. REPL and Debugger, 2020. on-line at: <https://swift.org/lldb/#why-combine-the-repl-and-debugger>.
- [6] Apple Inc. Understanding LLDB Command Syntax, 2020. on-line at: <https://developer.apple.com/library/archive/documentation/General/Conceptual/lldb-guide/chapters/C2-Understanding-LLDB-Command-Syntax.html>.
- [7] JetBrains. Clion LLDB, 2020. <https://www.jetbrains.com/help/clion/configuring-debugger-options.html>.
- [8] Linux Links. Best Free Linux Debuggers, 2020. <https://www.linuxlinks.com/debuggers/>.
- [9] LLVM. GDB to LLDB command map, 2020. on-line at: <https://lldb.llvm.org/use/map.html>.
- [10] LLVM. The LLDB Debugger, 2020. on-line at: <https://lldb.llvm.org>.
- [11] LLVM. The LLDB Debugger, 2020. on-line at: <http://blog.llvm.org/2010/06/new-lldb-debugger.html>.
- [12] Sasa Malkov. Debagovanje, 2019. <http://poincare.matf.bg.ac.rs/~smalkov/files/rs.r290.2019/public/Predavanja/Razvoj%20softvera.08.2019%20-%20Debagovanje.p4.pdf>.
- [13] Microsoft. Visual Studio Code Suport, 2019. <https://code.visualstudio.com/docs/cpp/cpp-debug>.
- [14] Microsoft. Visual Studio Debugger Suport, 2019. <https://docs.microsoft.com/en-us/visualstudio/debugger/debugger-feature-tour?view=vs-2019>.
- [15] Microsoft. Visual Studio Code LLDB plugin, 2020. <https://marketplace.visualstudio.com/items?itemName=vadimcn.vscode-lldb>.
- [16] Margaret Rouse. Debagovanje, 2020. <https://searchsoftwarequality.techtarget.com/definition/debugging>.

- [17] The LLDB Team. Python Scripting, 2020. on-line at: <https://lldb.llvm.org/use/python.html>.
- [18] The LLDB Team. Tutorial, 2020. on-line at: <https://lldb.llvm.org/use/tutorial.html>.