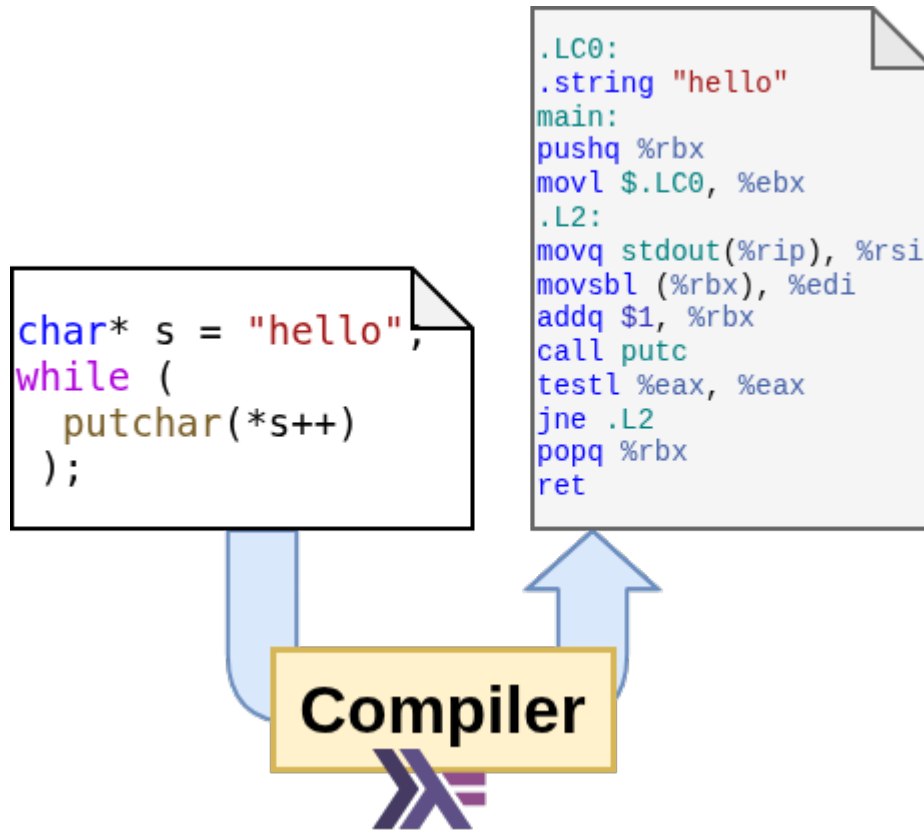
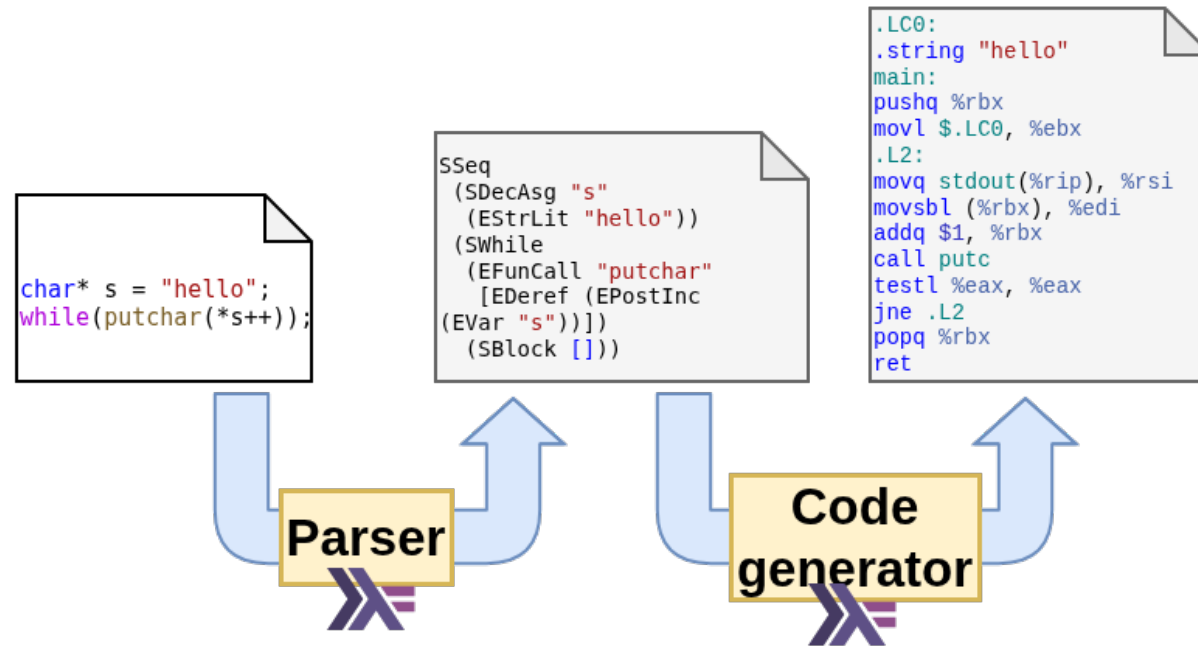


Analysis

Compilers



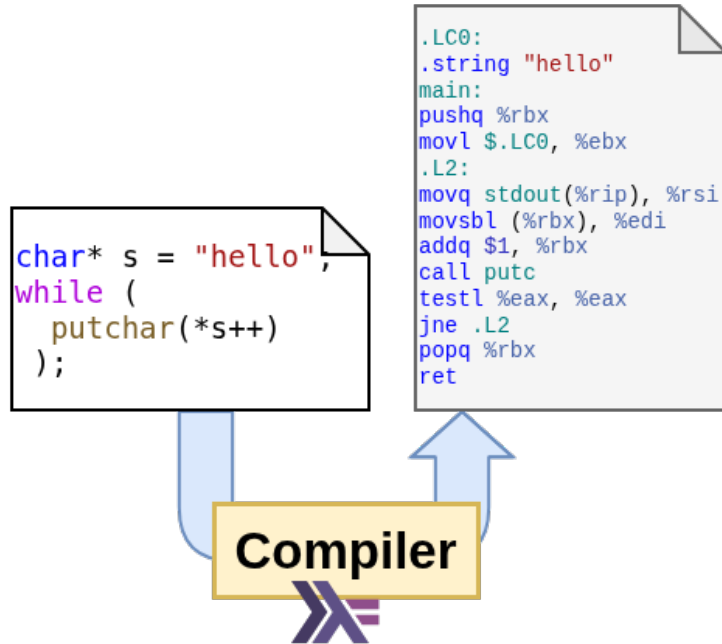
Compilers, so far



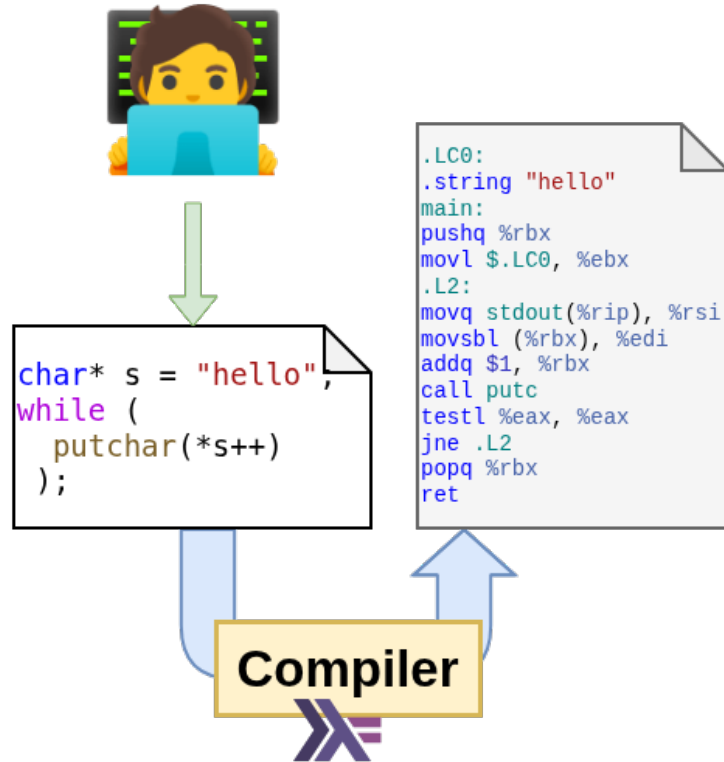
Human Error



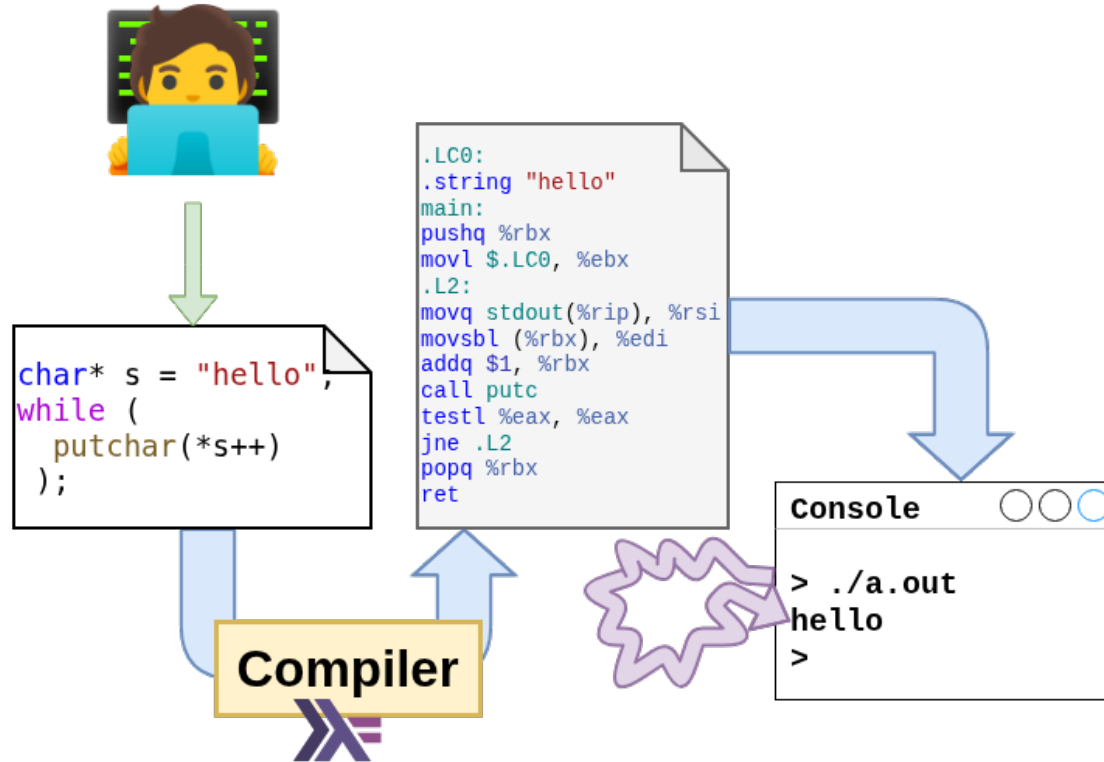
Programmer Error



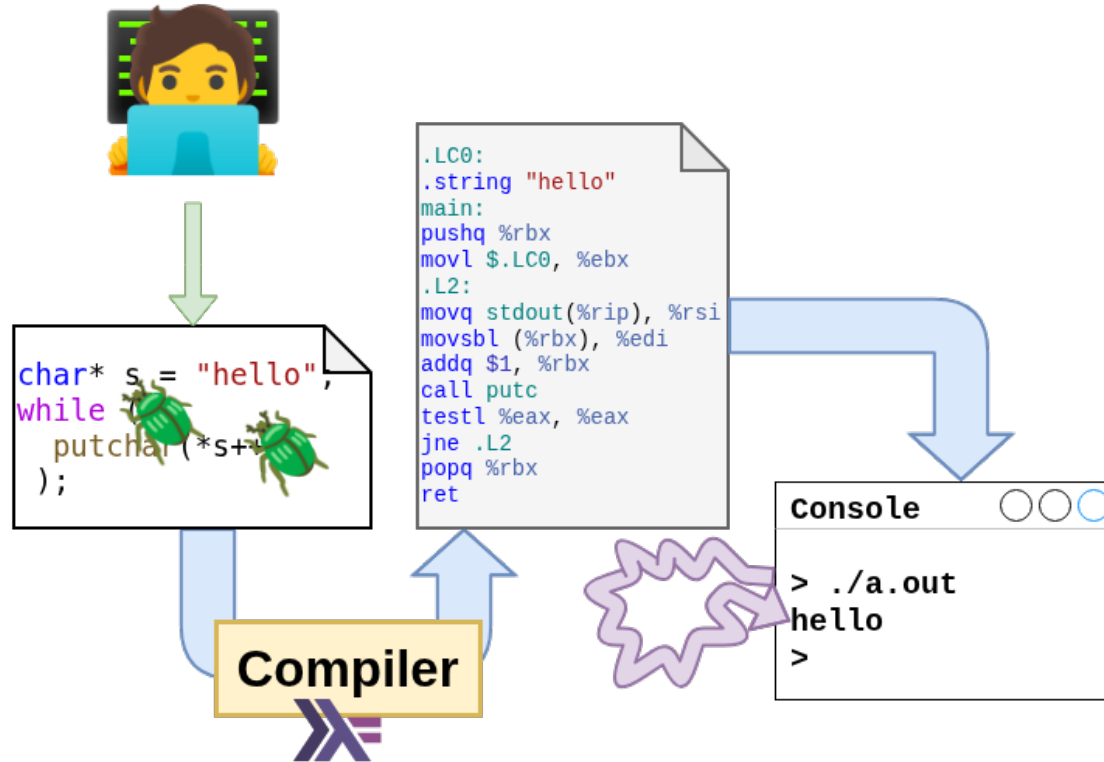
Programmer Error



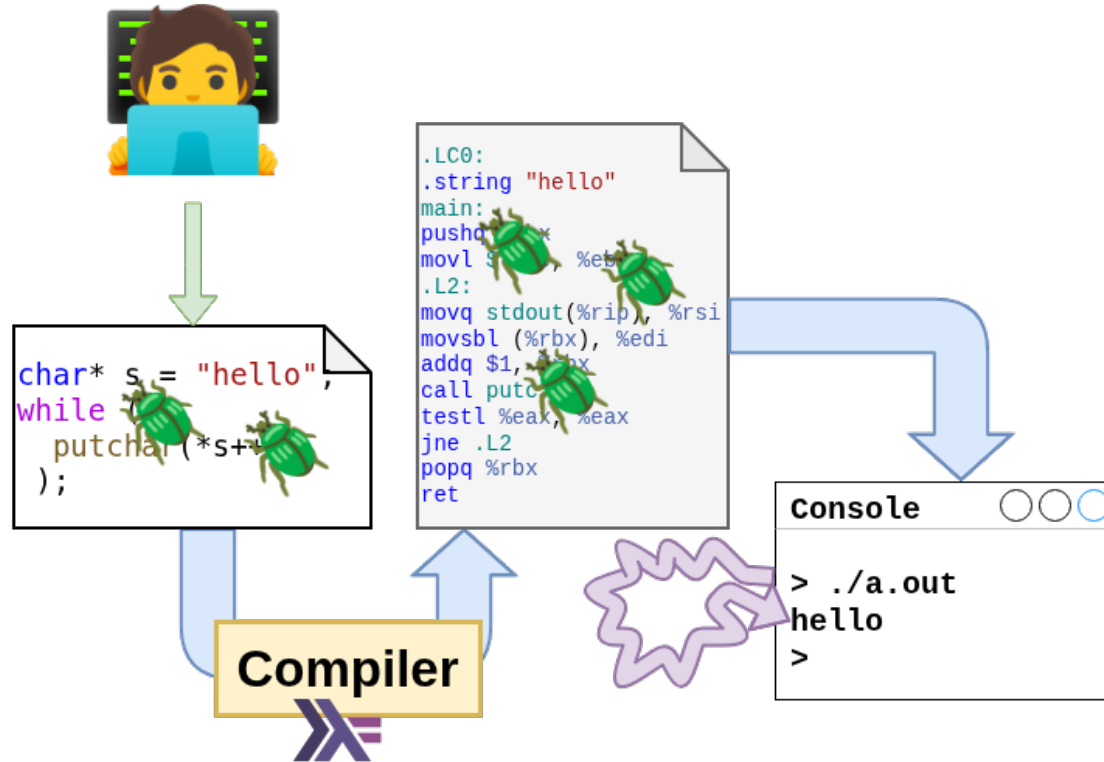
Programmer Error



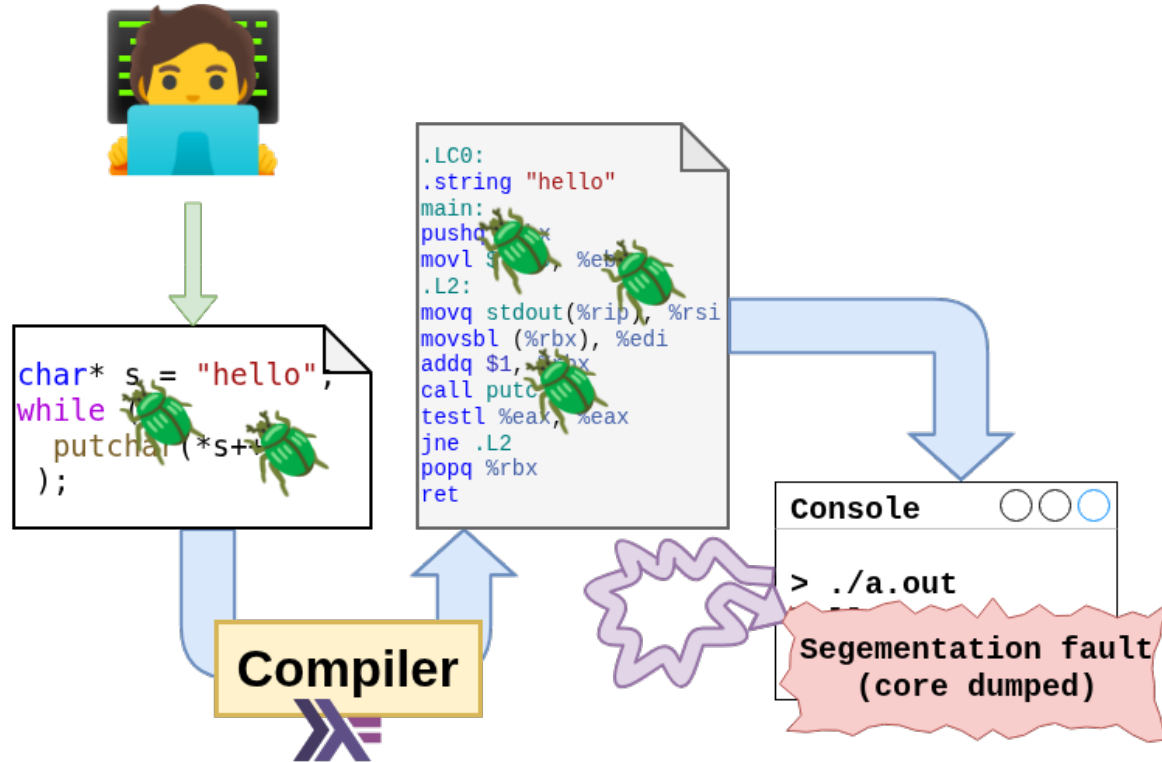
Programmer Error



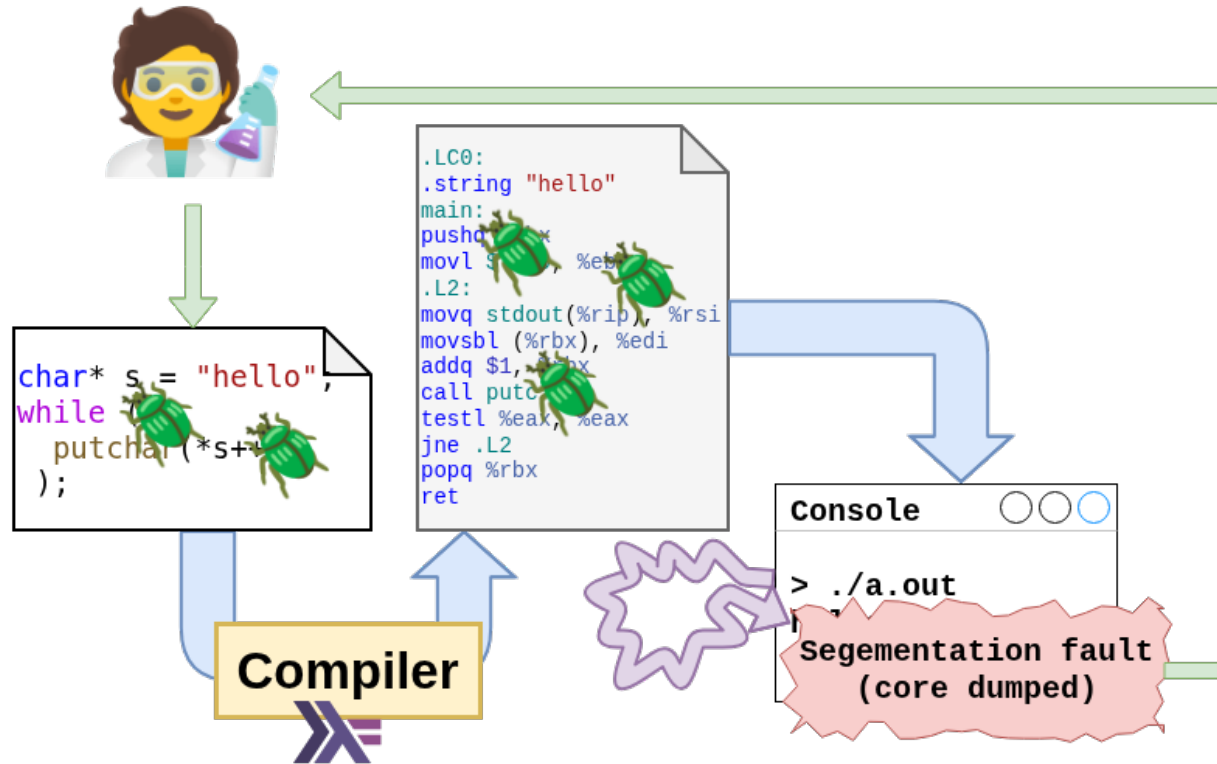
Programmer Error



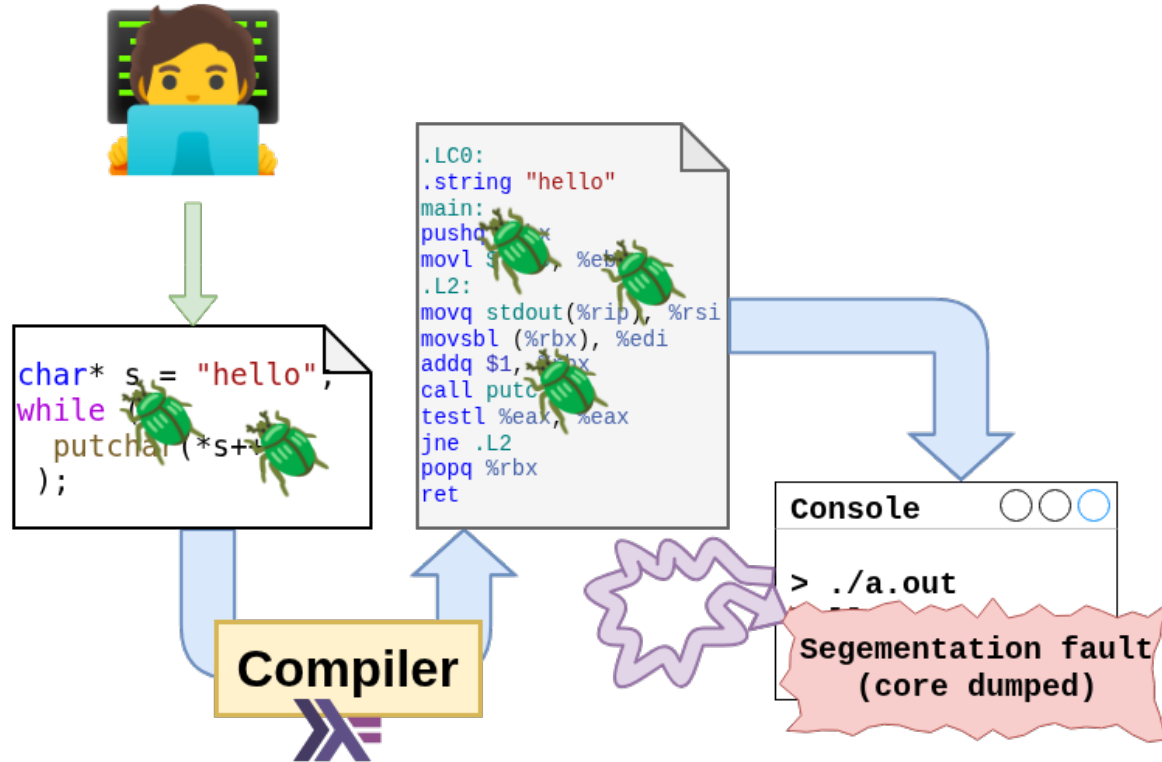
Programmer Error



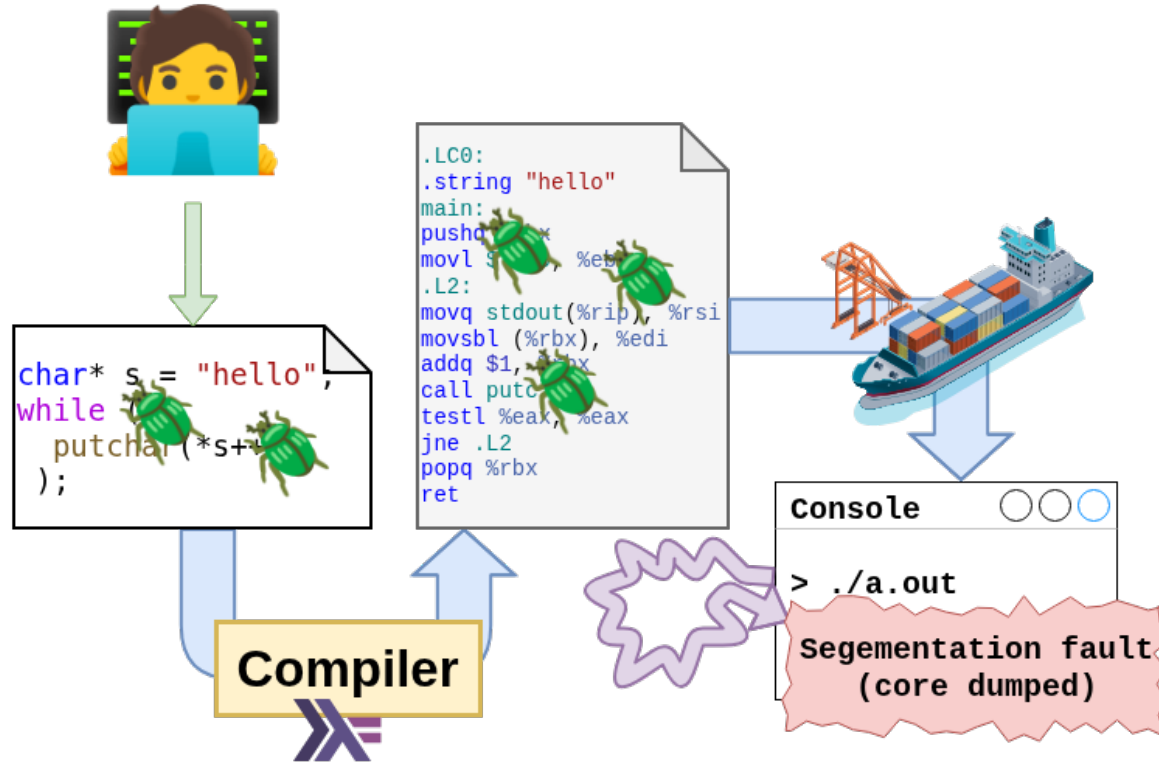
Programmer Error



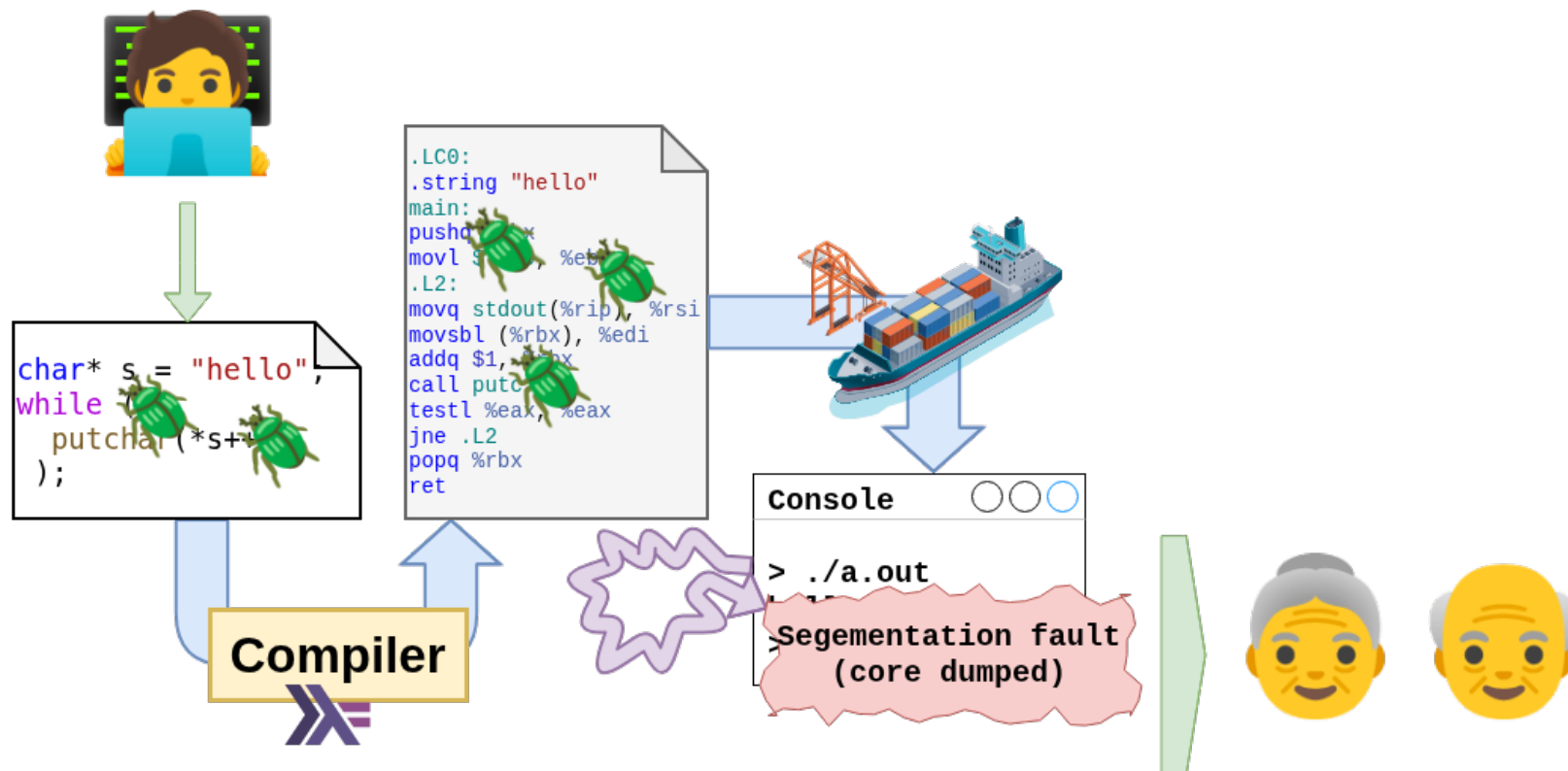
Programmer Error



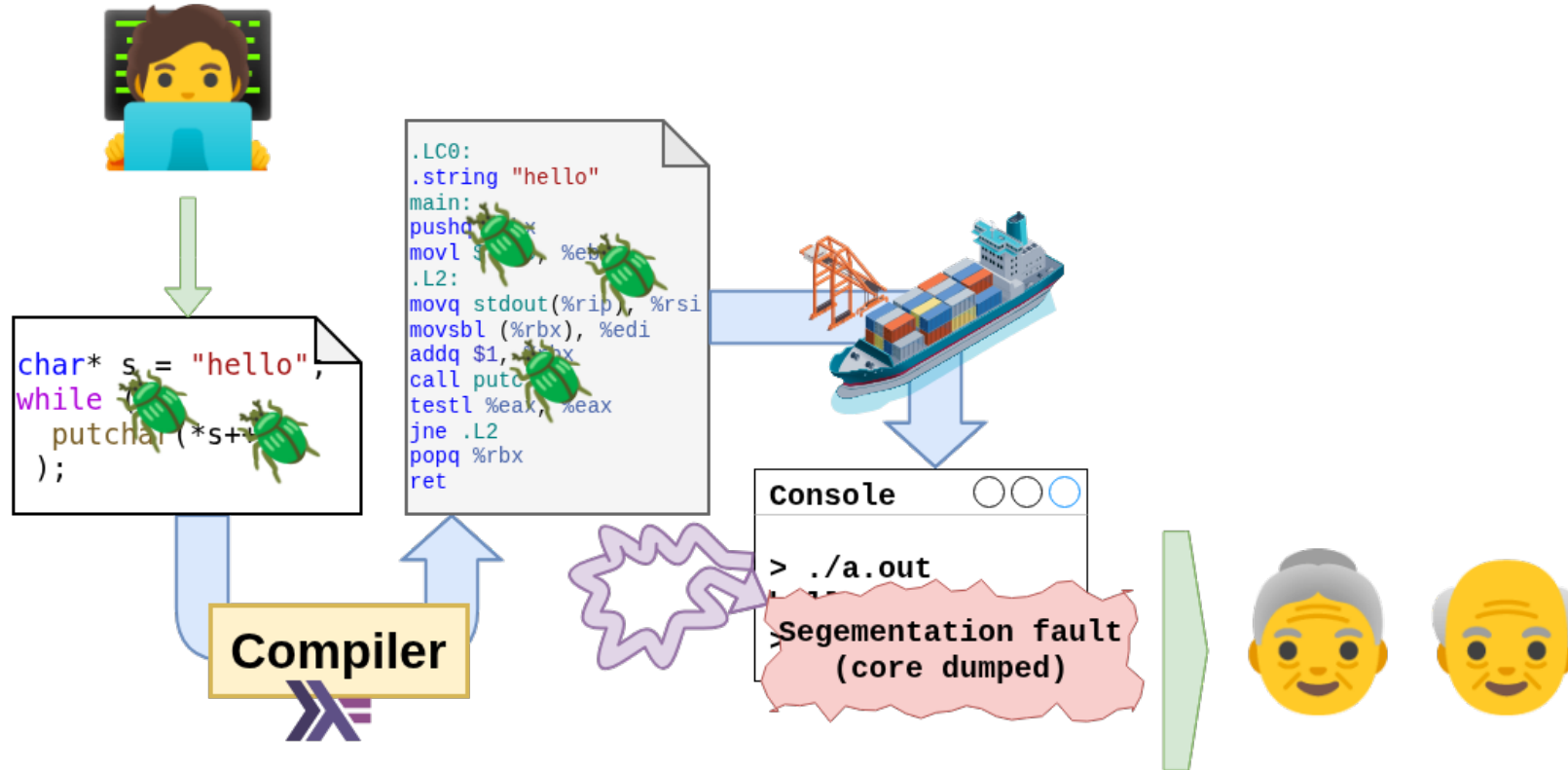
Programmer Error



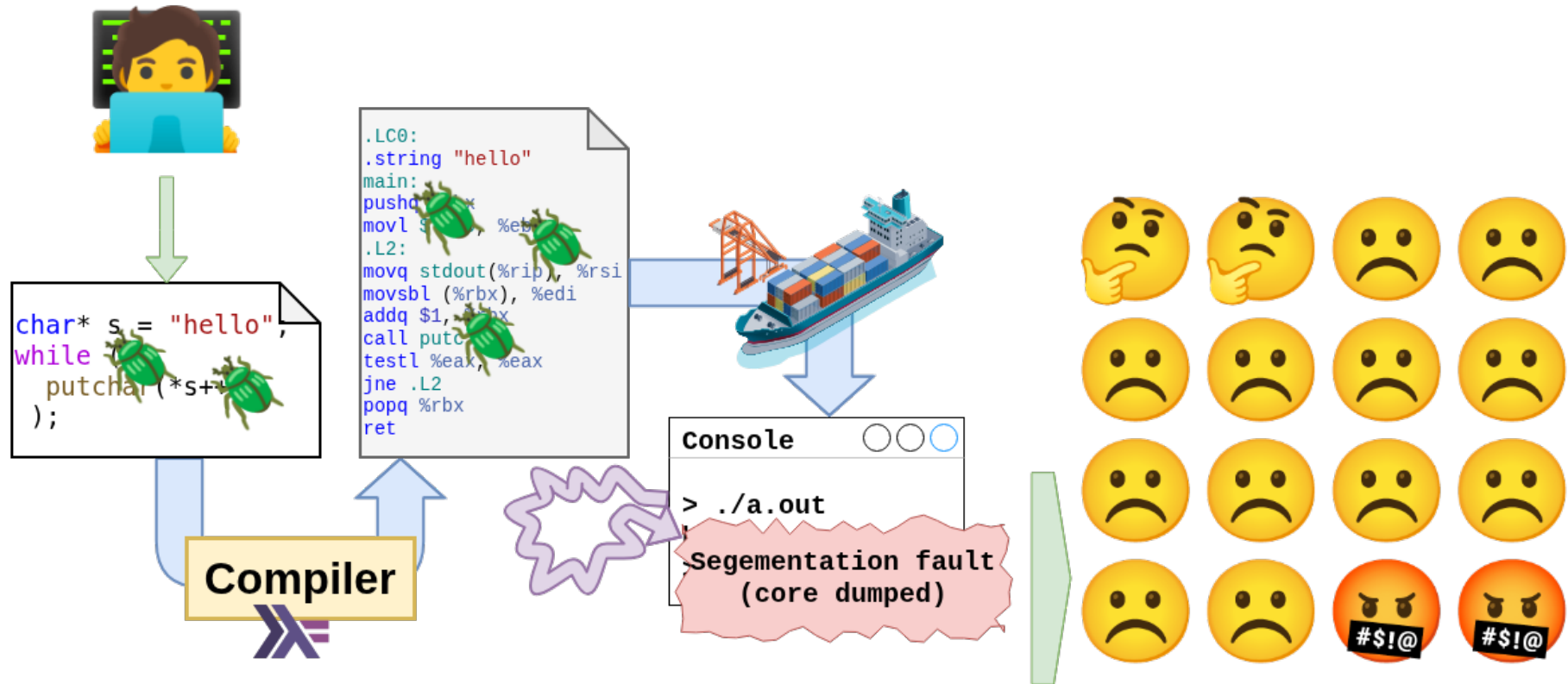
Programmer Error



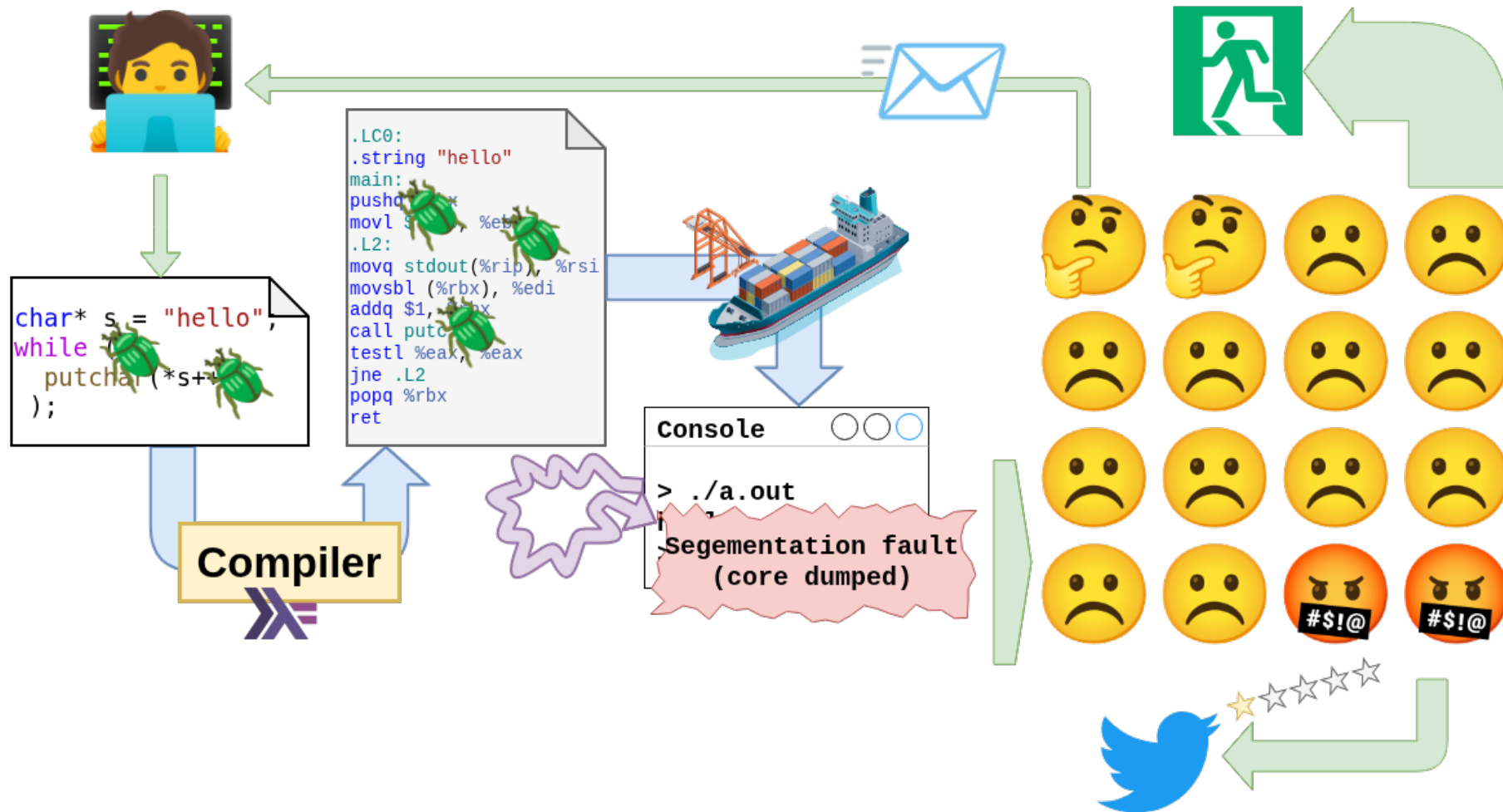
Consequences



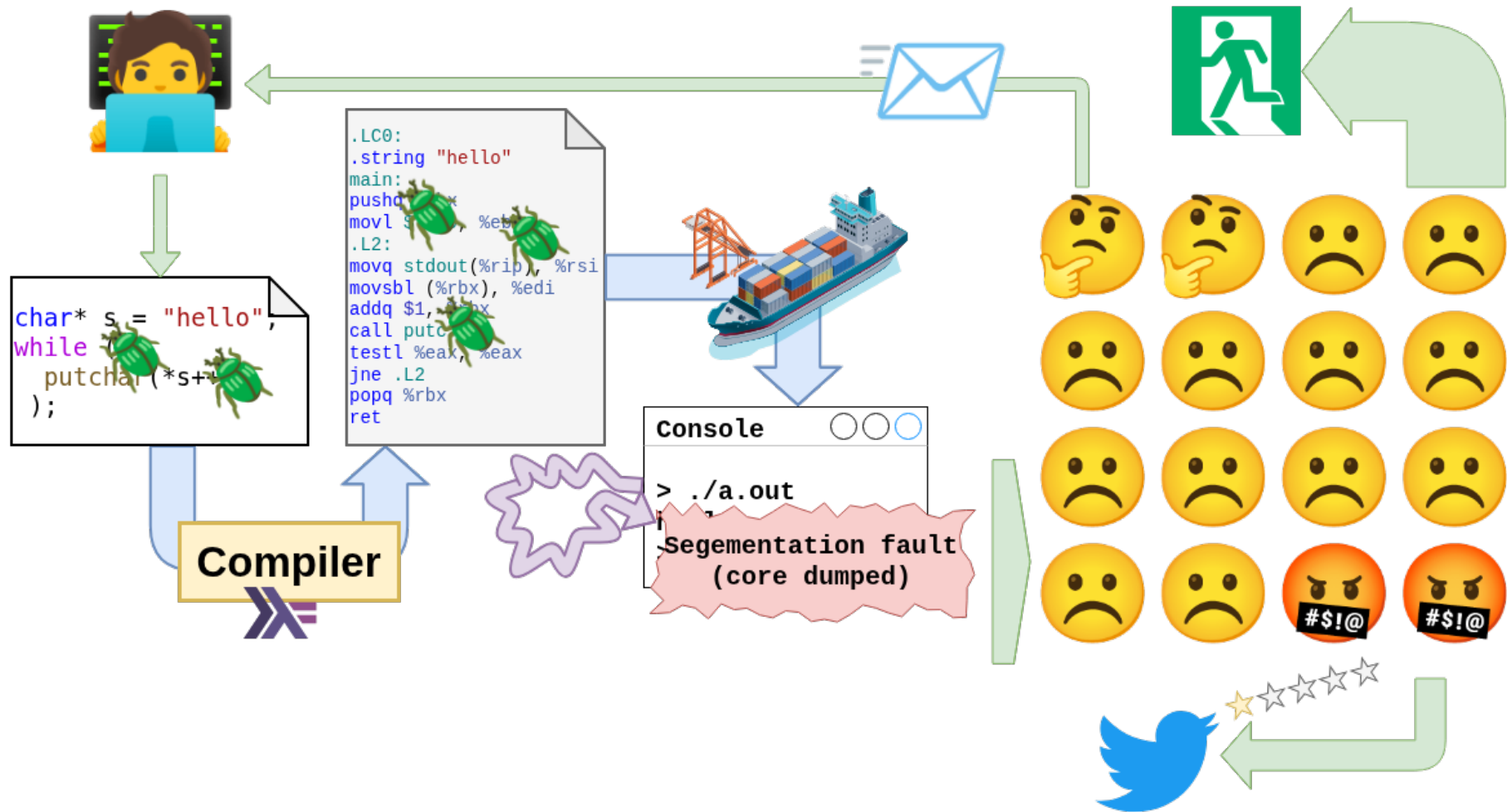
Consequences



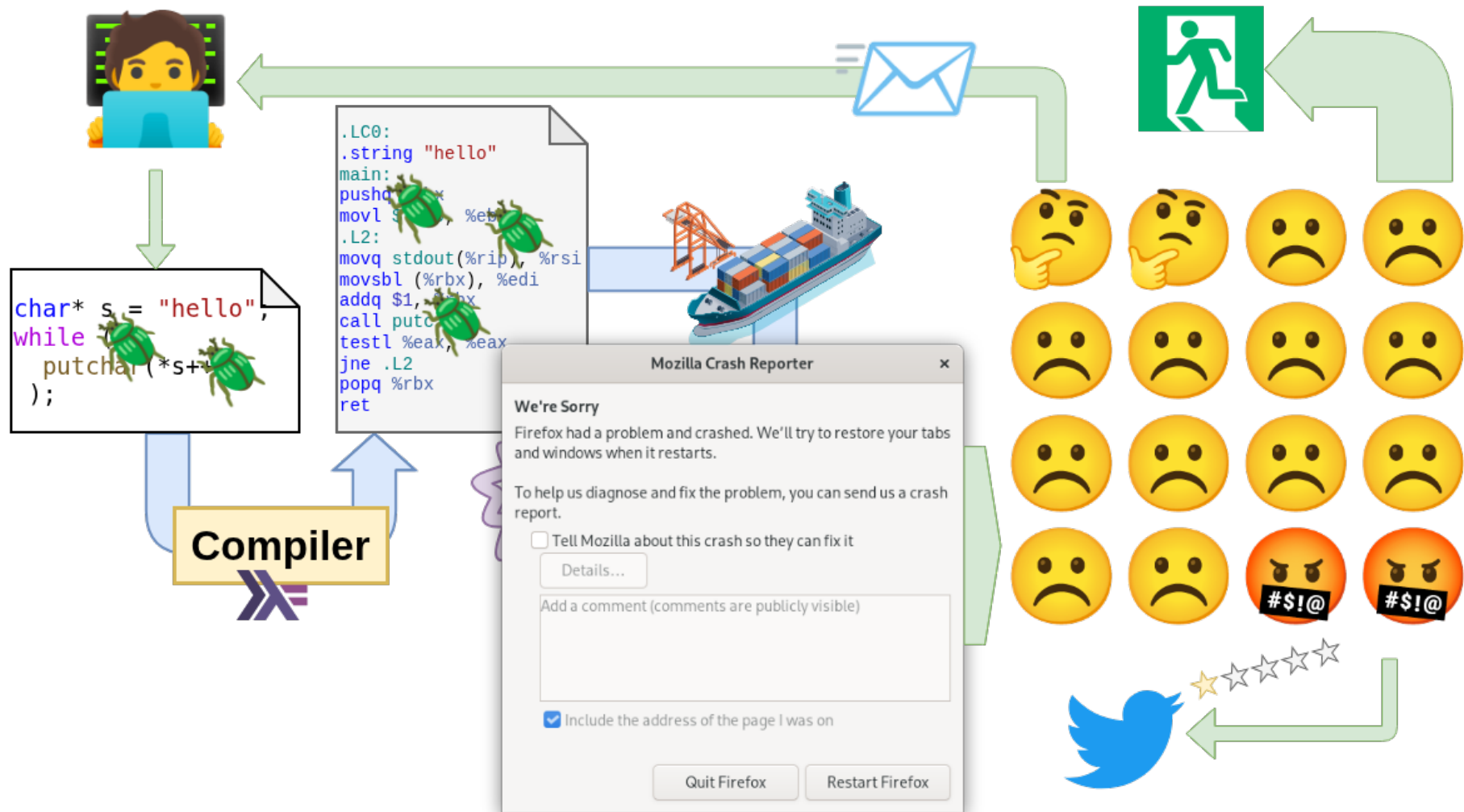
Consequences



Error Message Quality



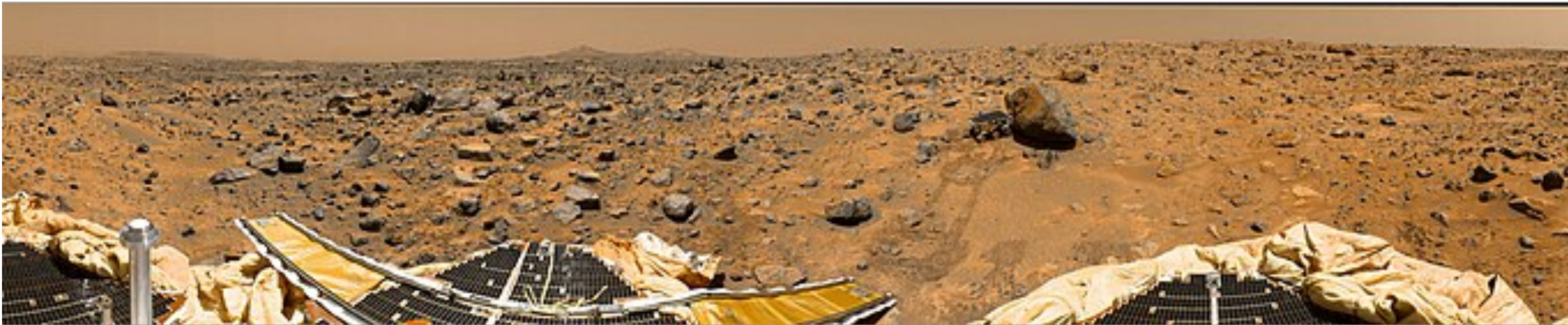
Error Message Quality



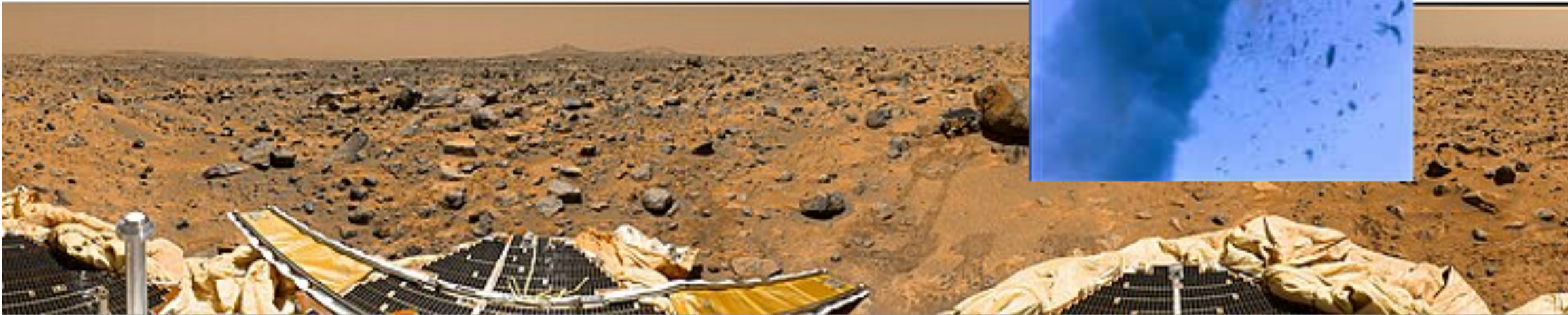
Error Messages aren't always enough



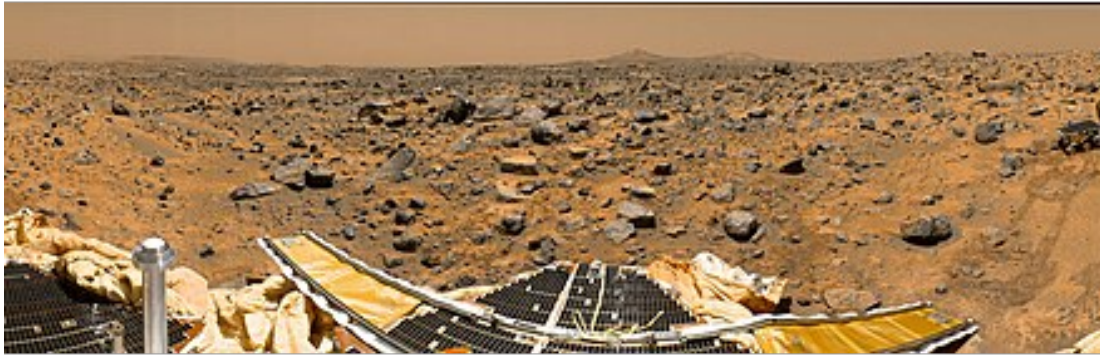
Error Messages aren't always enough



Error Messages aren't always enough



Error Messages aren't always enough



Error Messages aren't always enough



Ariane V88 self-destructs
after failed float64 -> int16
conversion (1996)

http://www.capcomespace.net/dossiers/espace_europeen/ariane/ariane5/AR501/V88_AR501.htm

Pathfinder Mars Lander
goes to sleep after
priority inversion (1997)

https://en.wikipedia.org/wiki/Mars_Pathfinder#On-board_computer

The New York Times

February 1, 2010

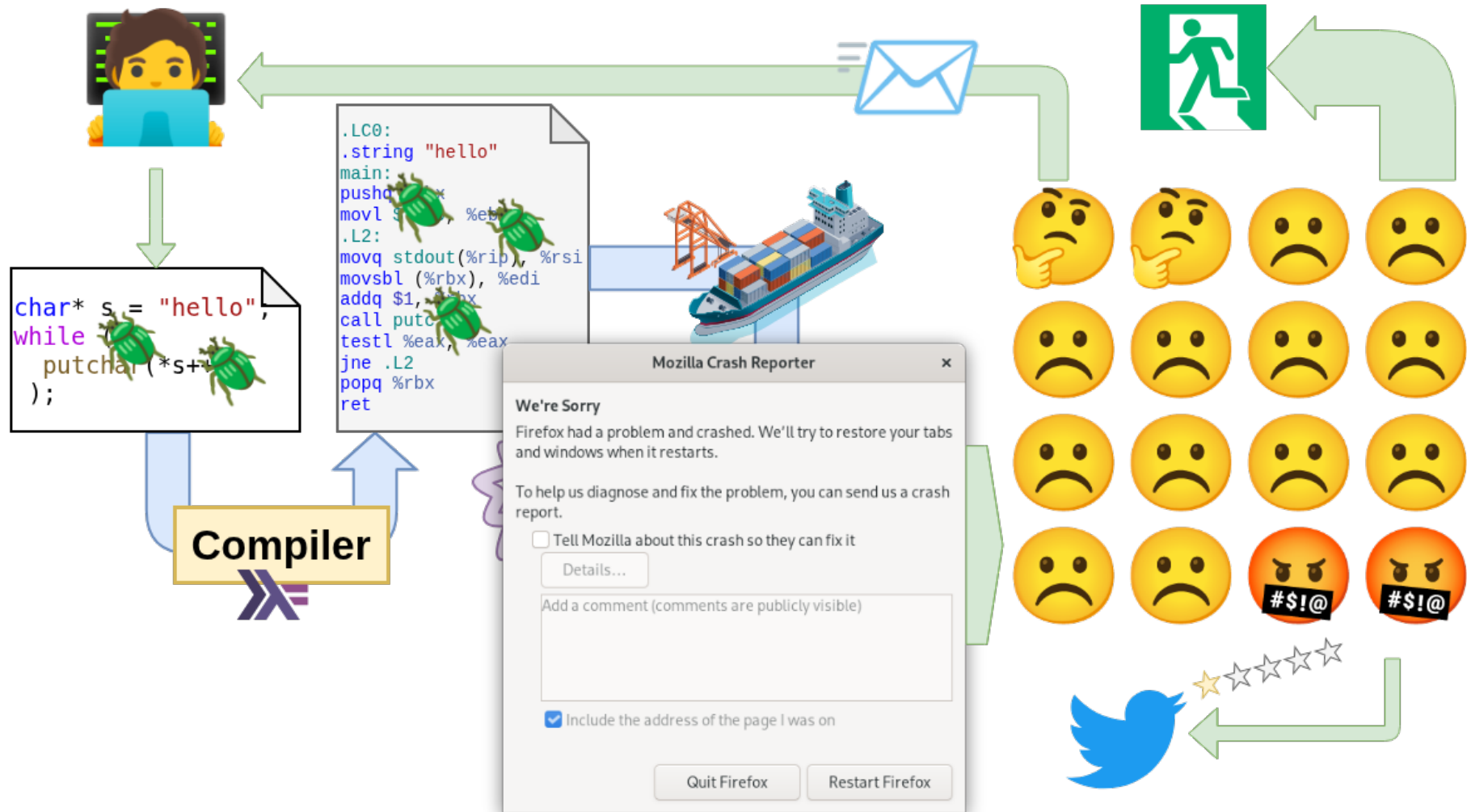
6200 "Sudden Unintended Acceleration"
complaints for Toyota cars (2010)
"Spaghetti code" suspected

https://ptolemy.berkeley.edu/projects/chess/pubs/1081/koopman14_toyota_ua_slides.pdf

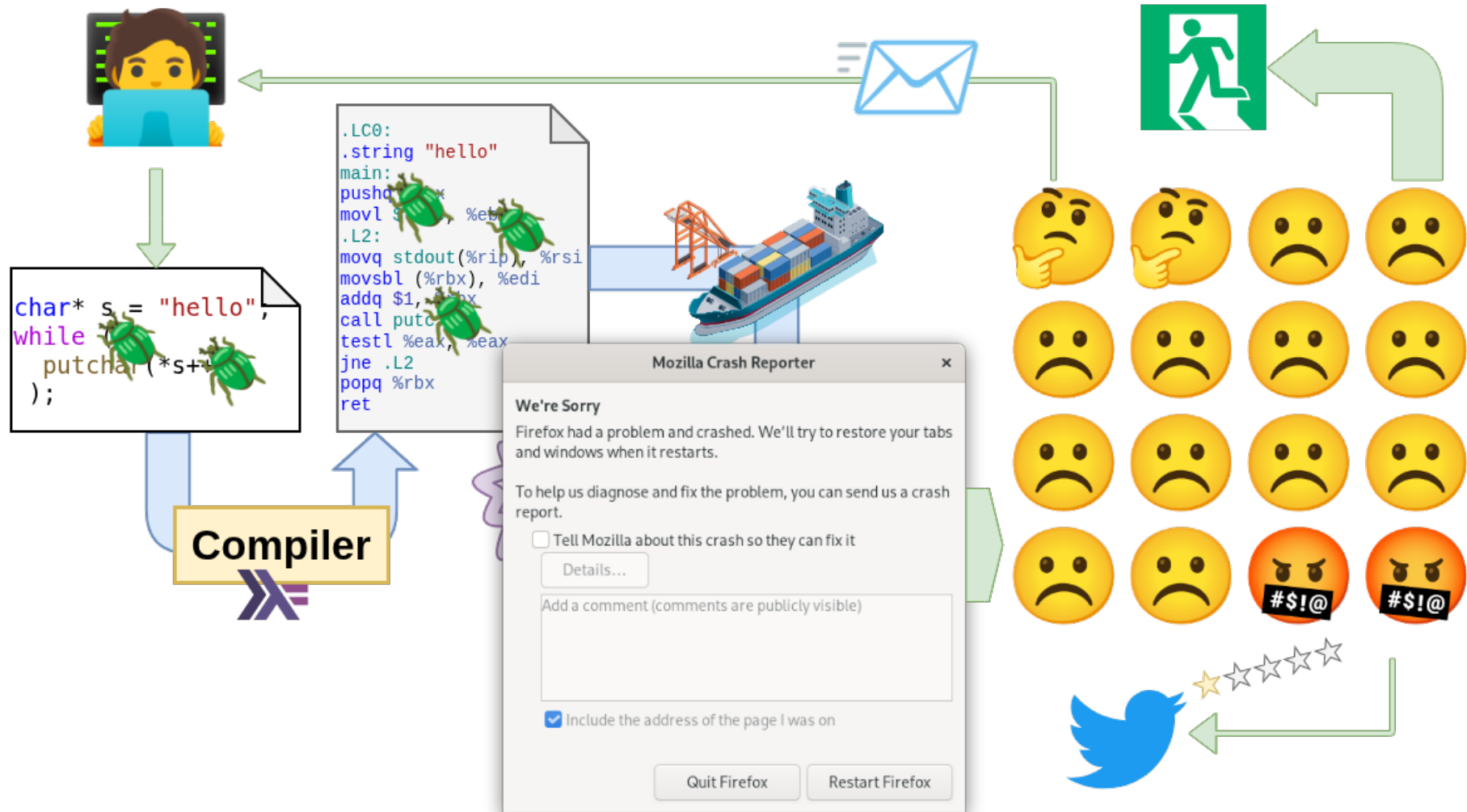
The wreckage of a Lexus ES 350 in which four people died in August after it accelerated out of control.

Gomez Len Film

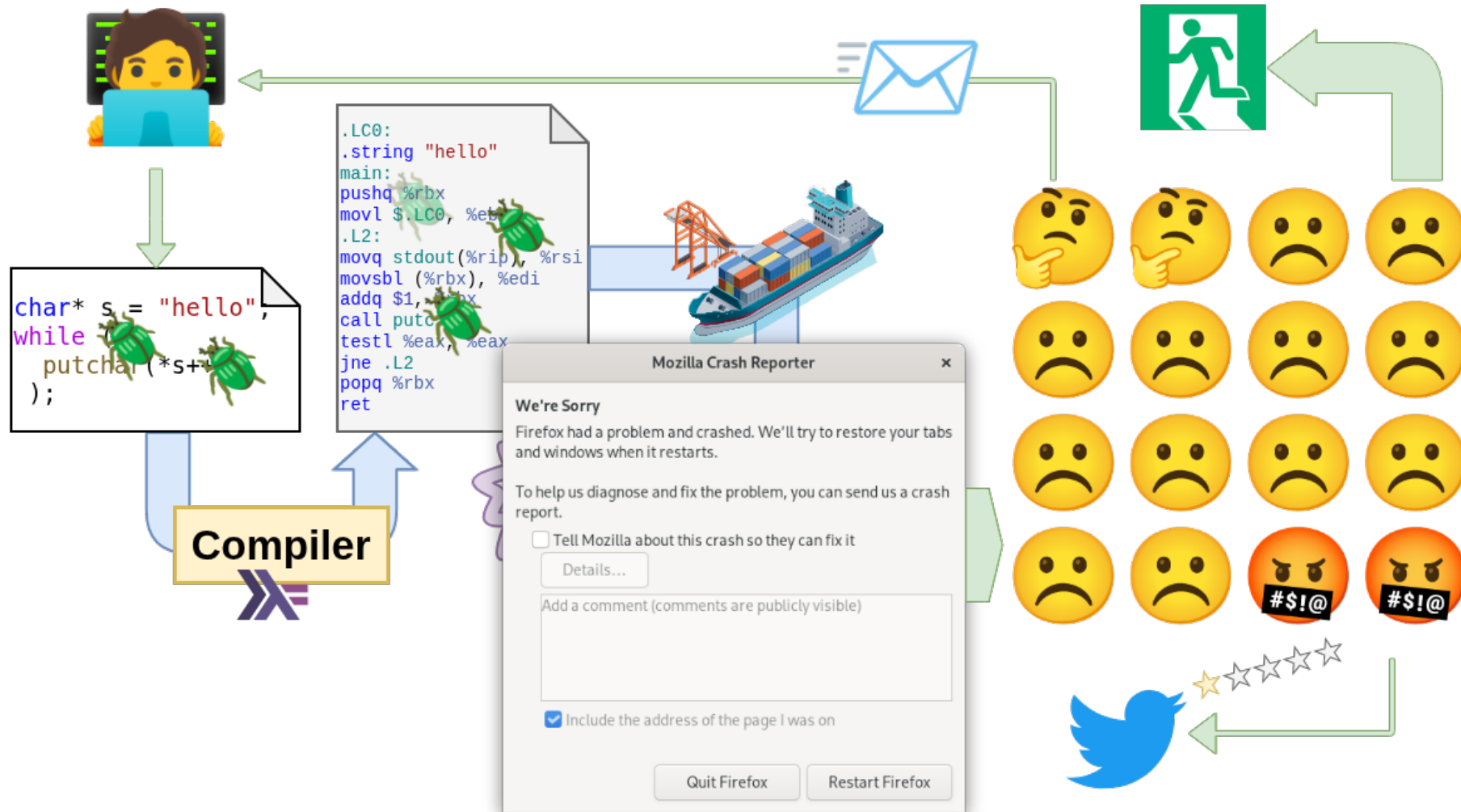
Fewer Errors



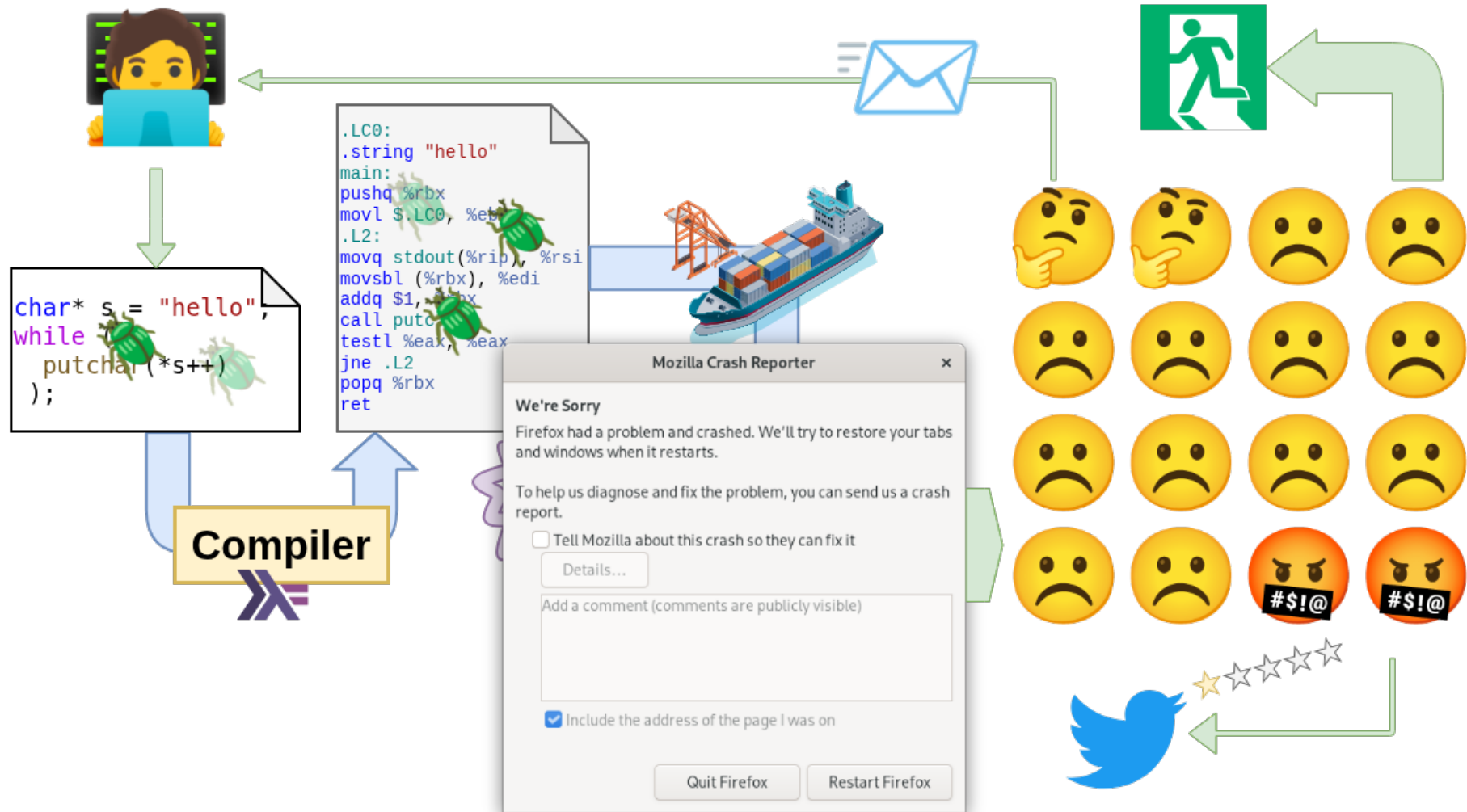
Fewer Errors



Fewer Errors



Fewer Errors



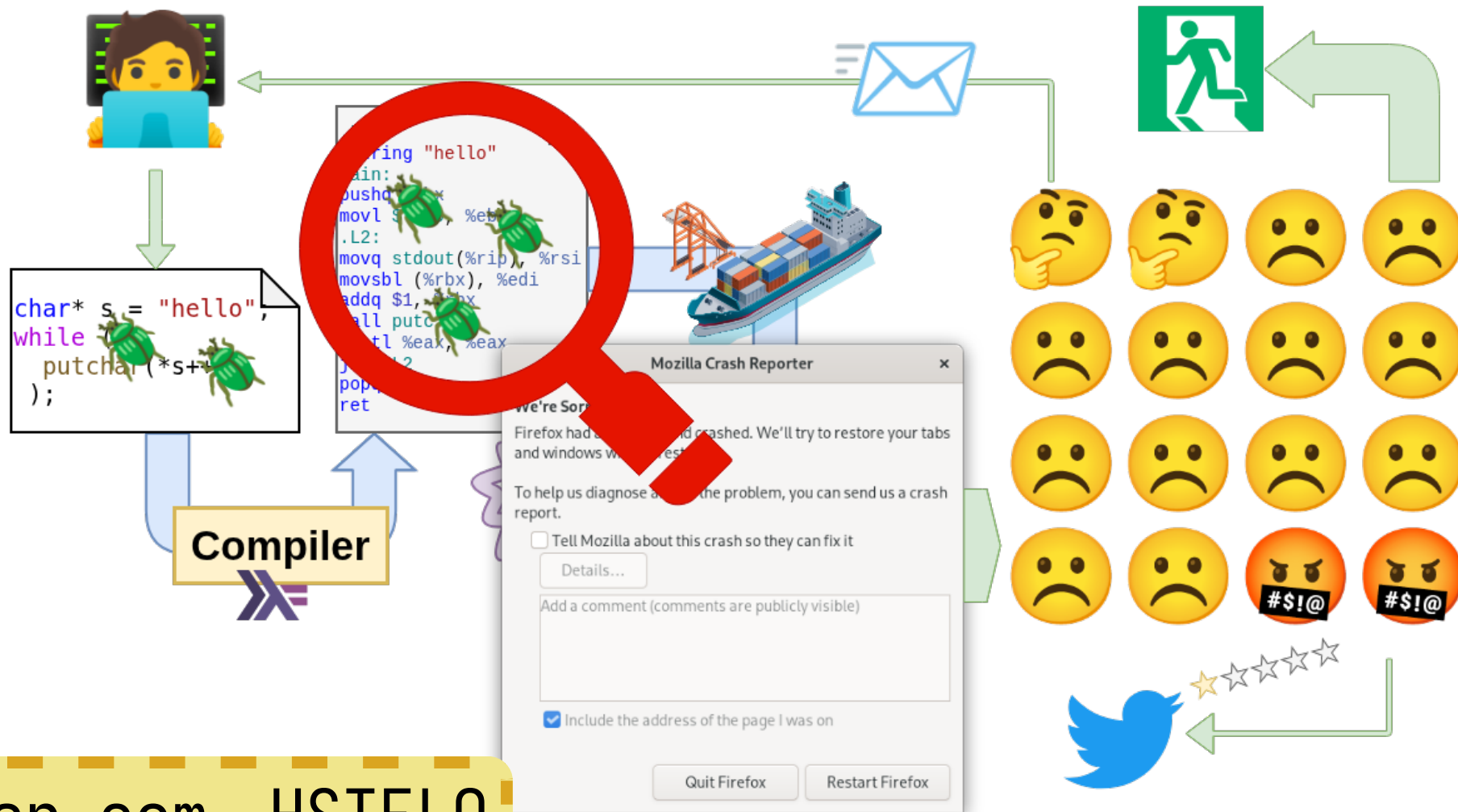
Where to hunt for



Where to hunt for



Where to hunt for



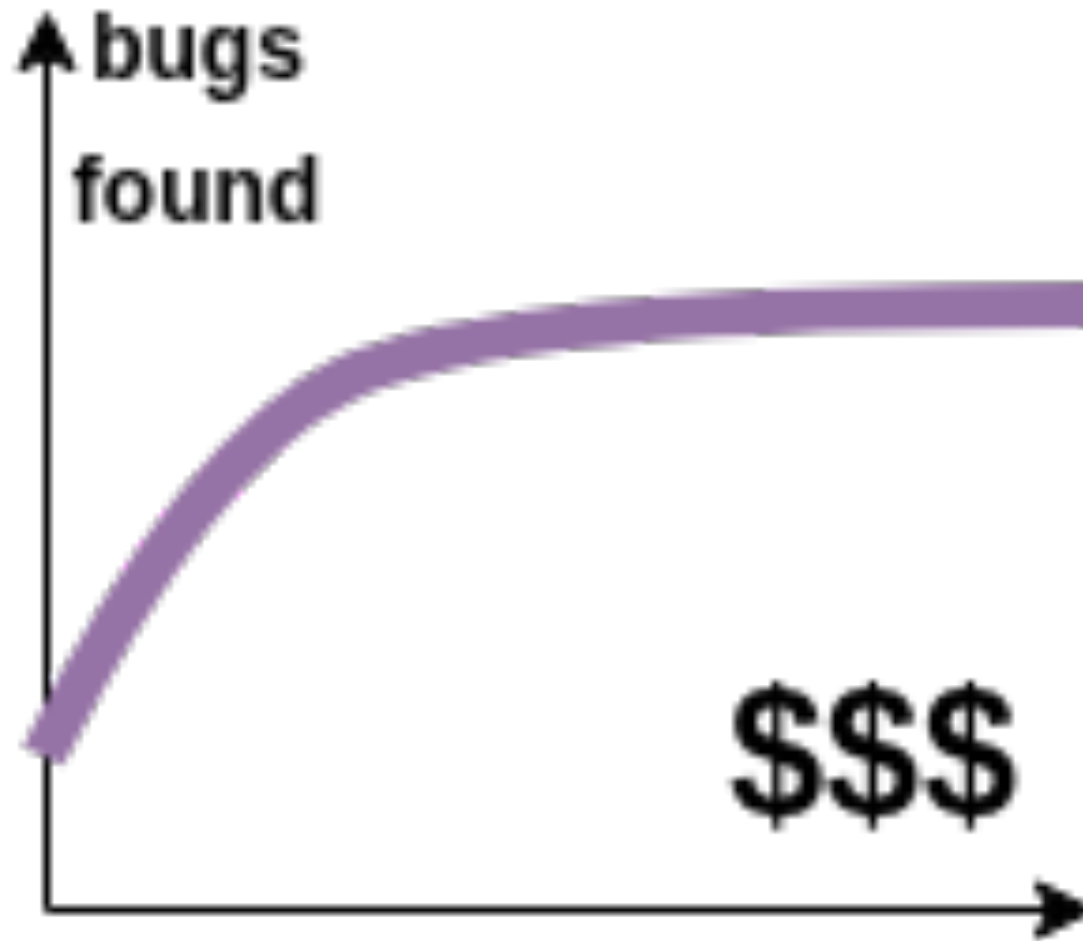
Where to hunt for



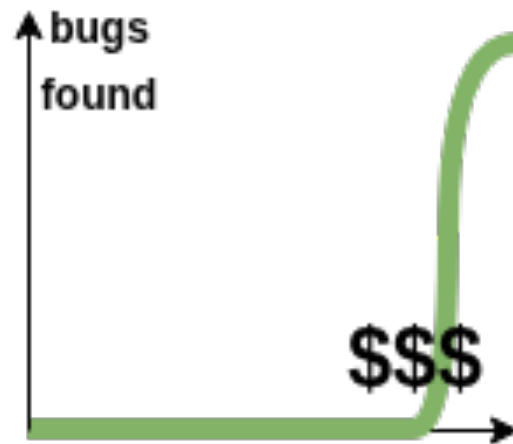
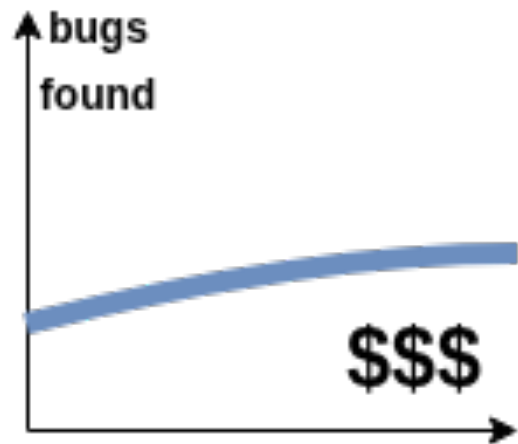
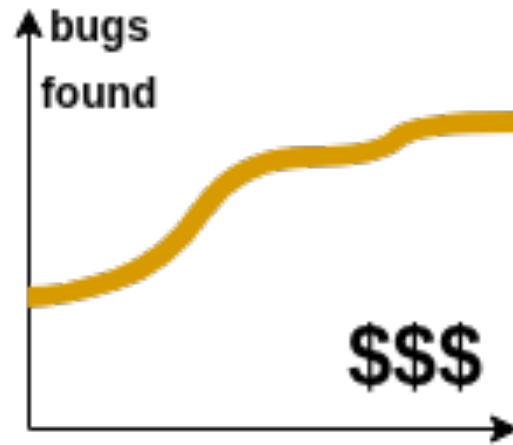
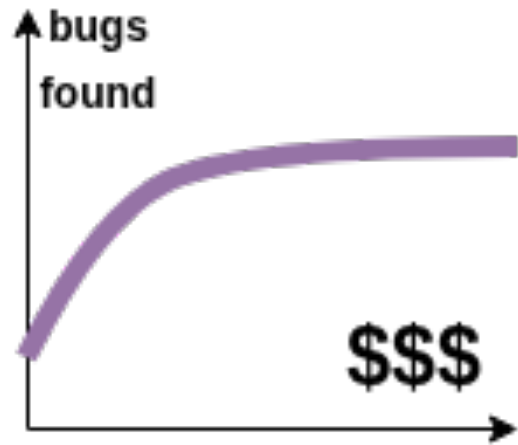
Where to hunt for



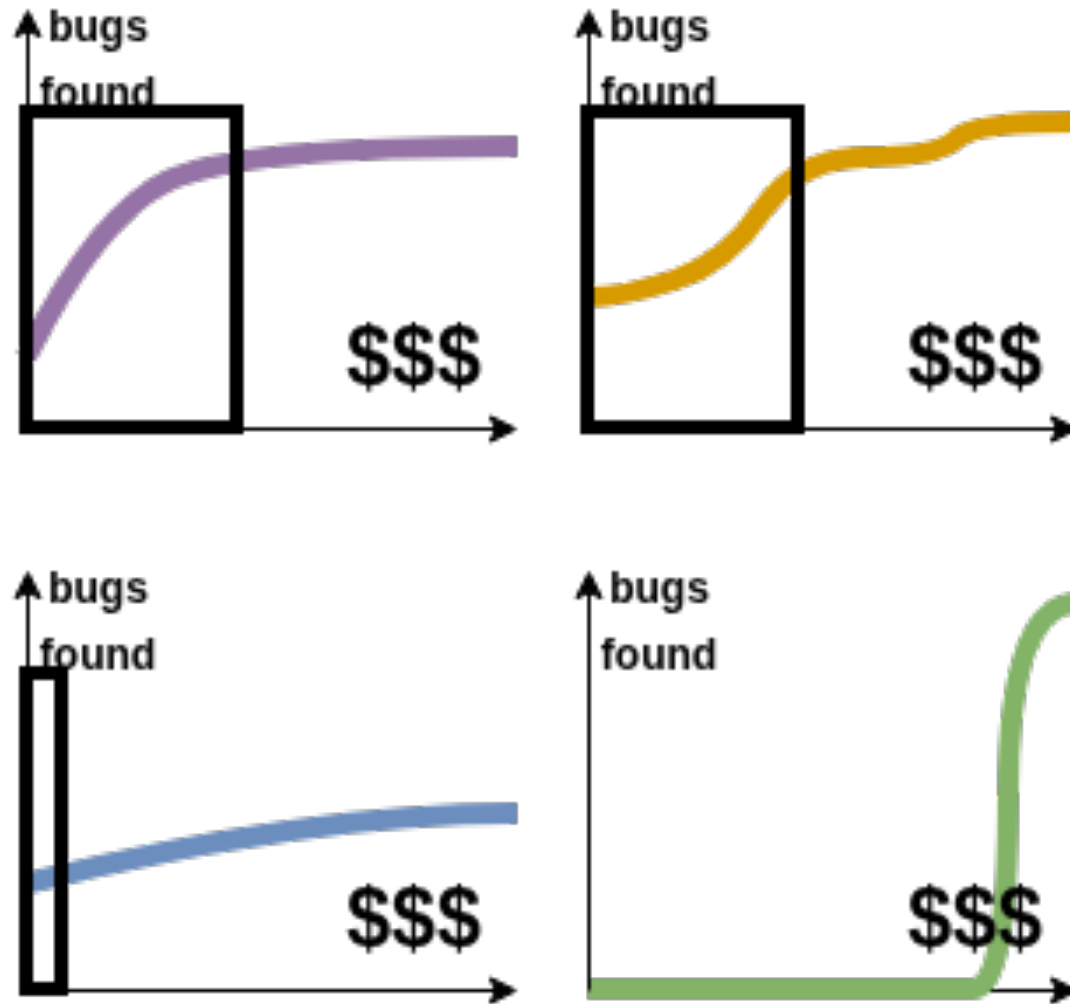
Diminishing returns



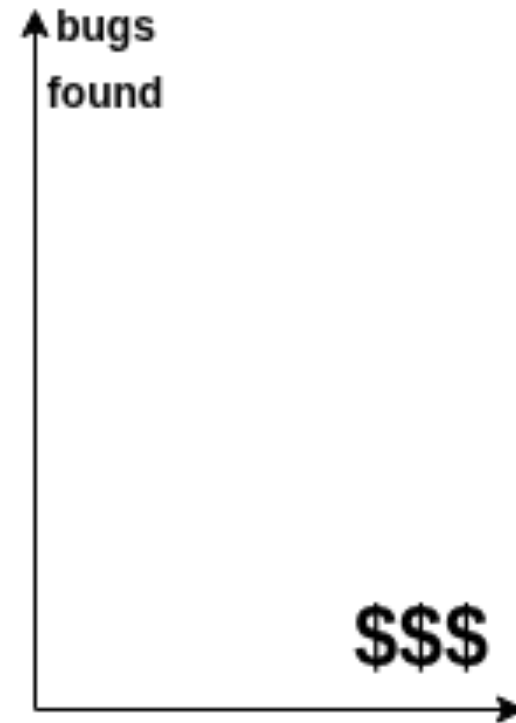
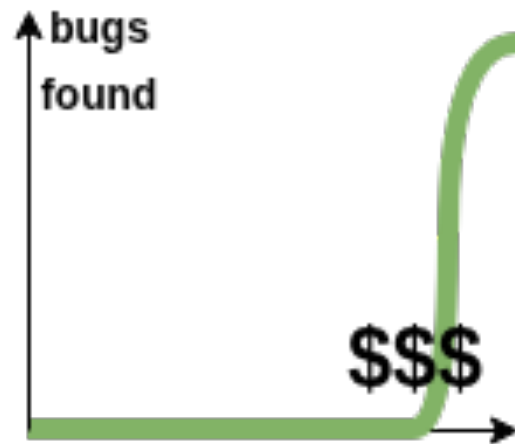
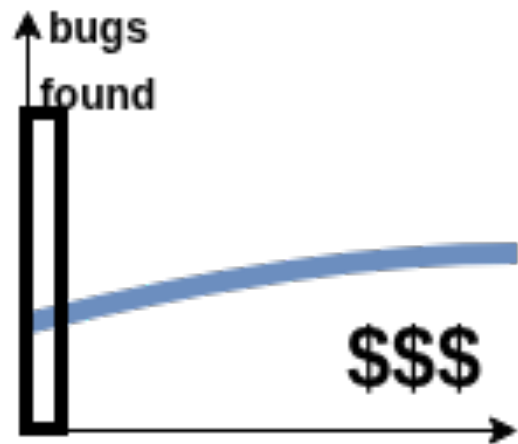
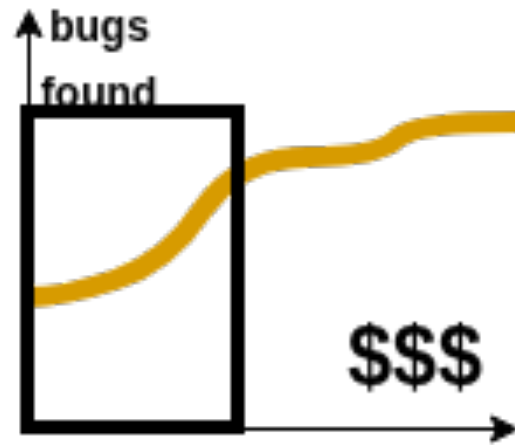
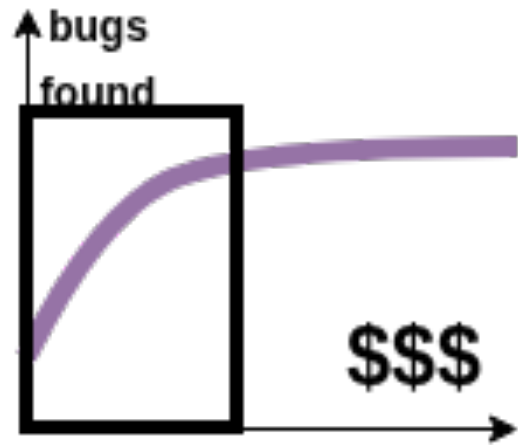
Diminishing returns



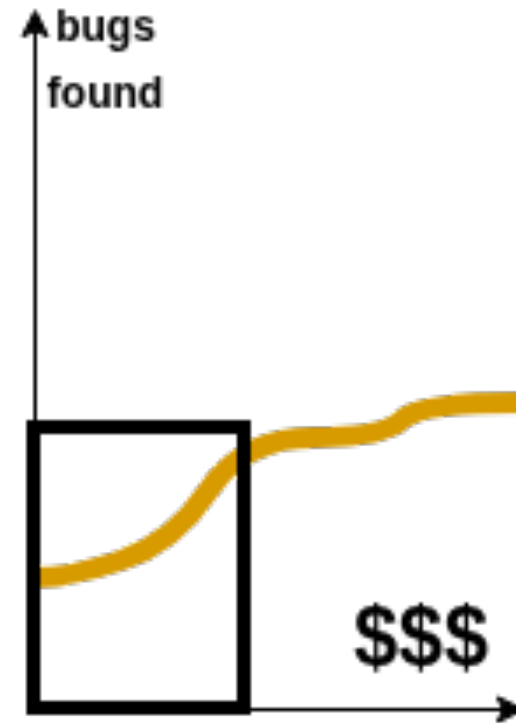
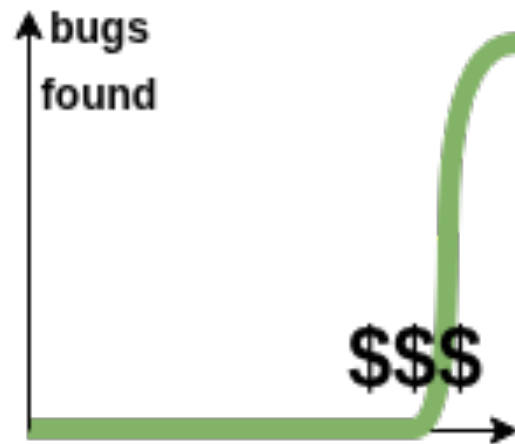
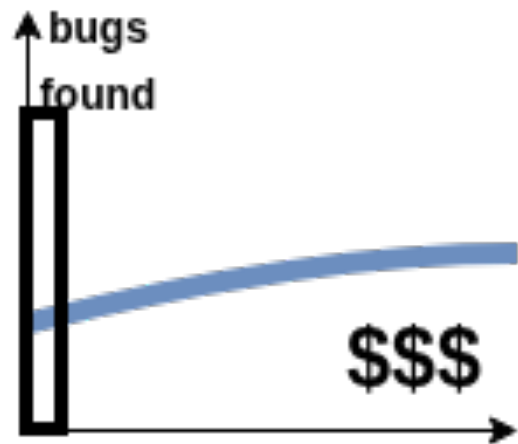
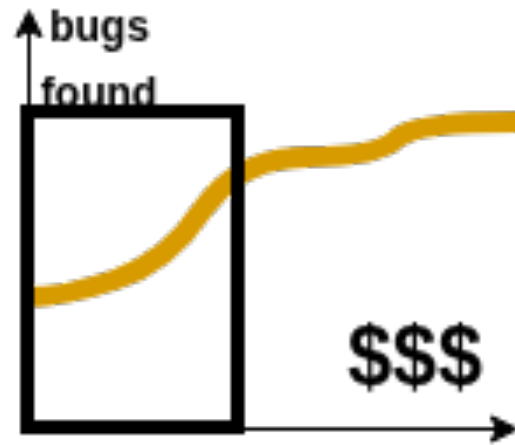
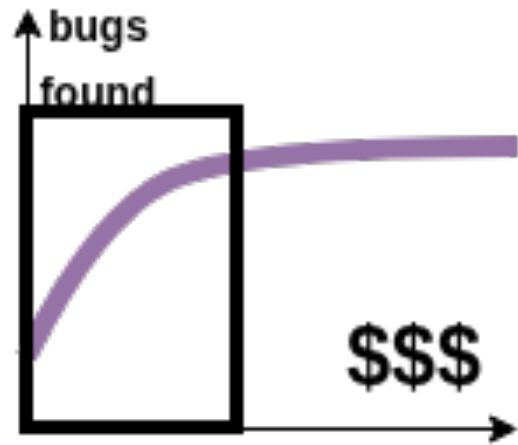
Diminishing returns



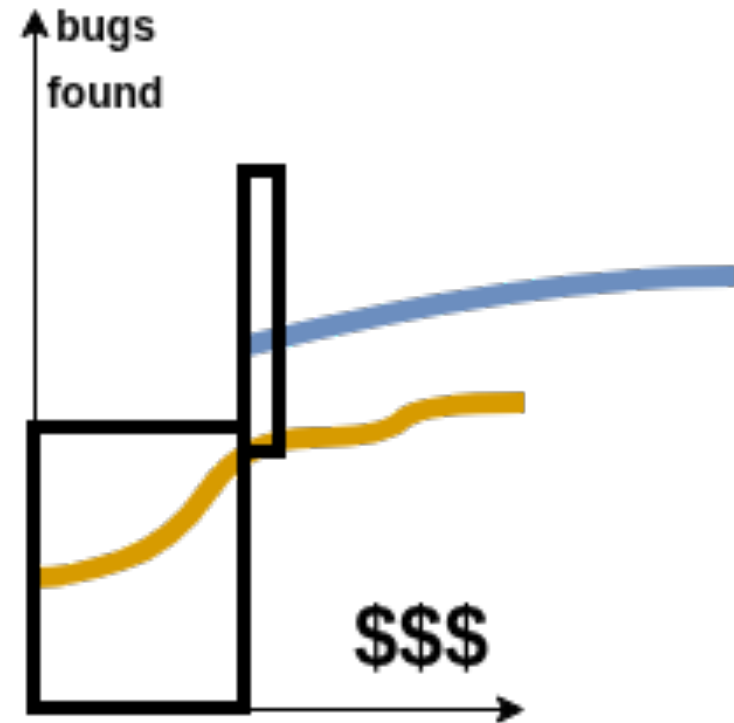
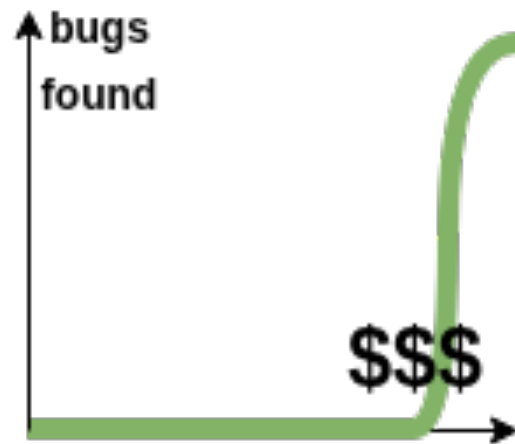
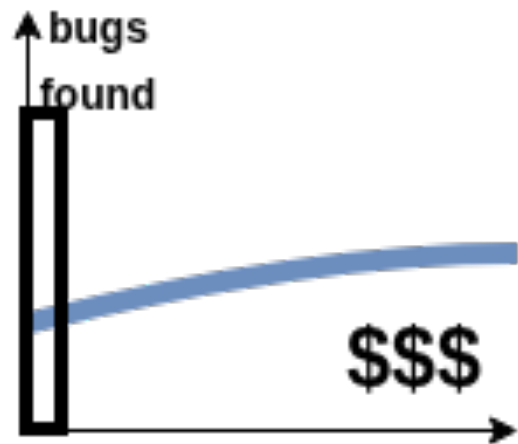
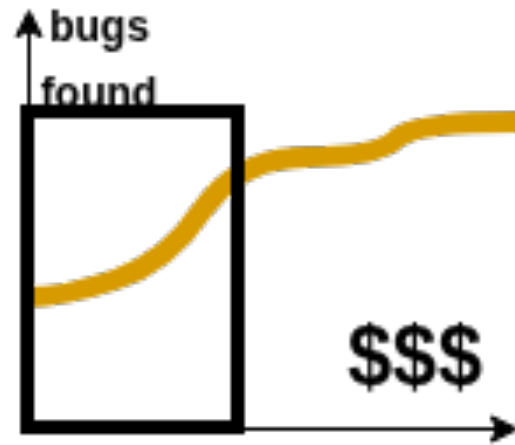
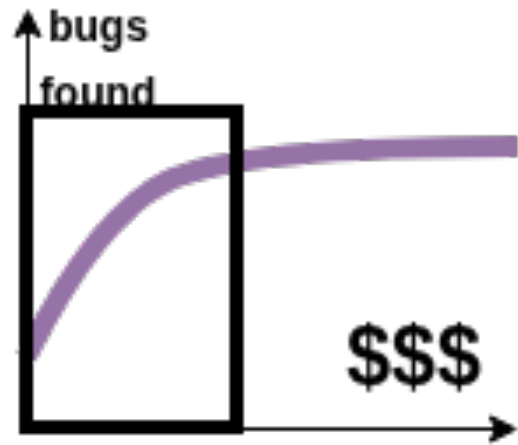
Diminishing returns



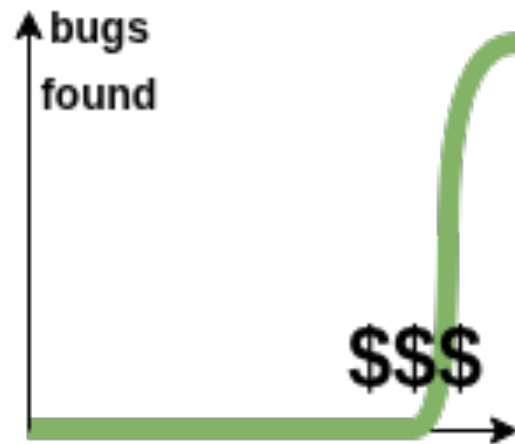
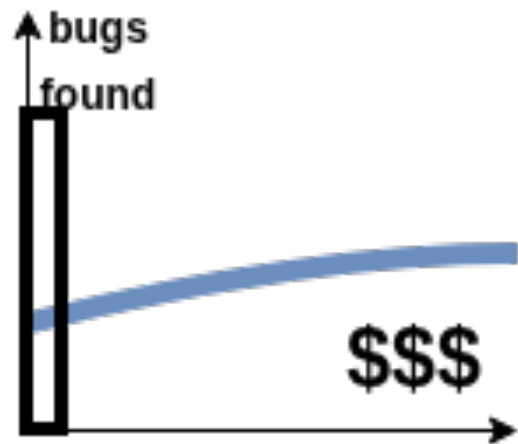
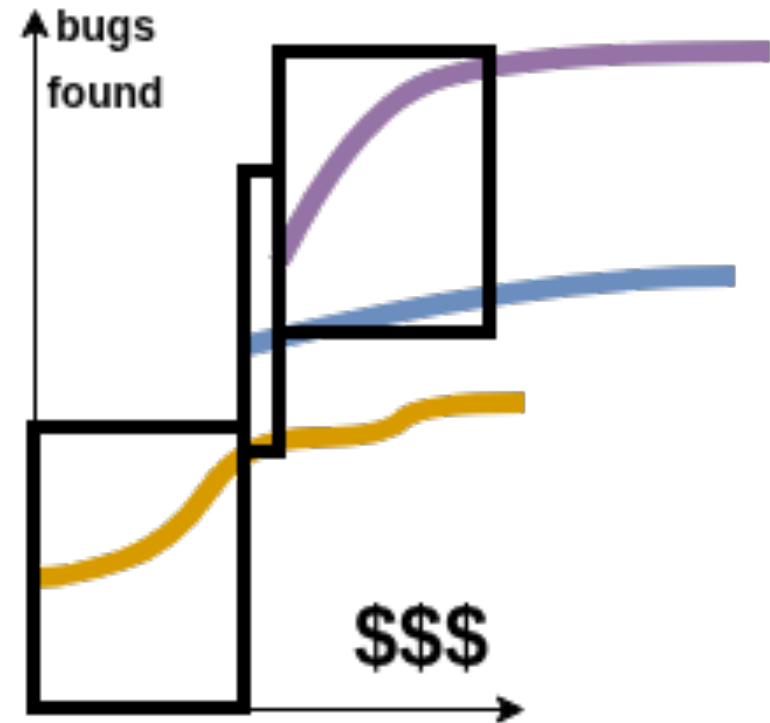
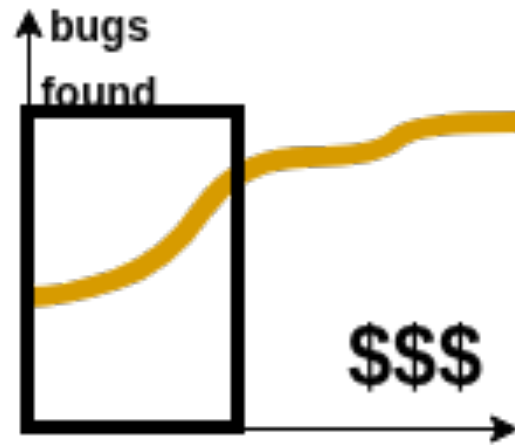
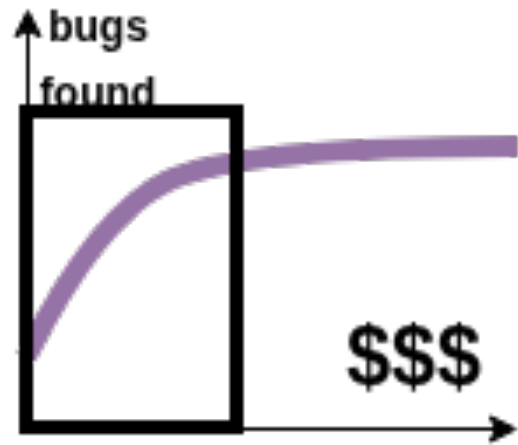
Diminishing returns



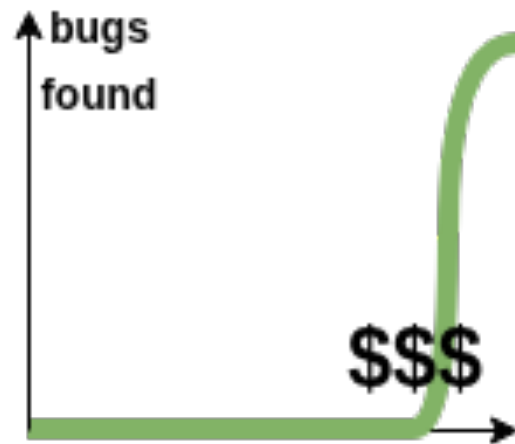
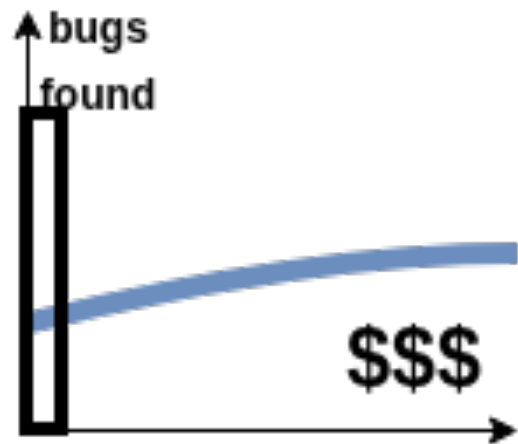
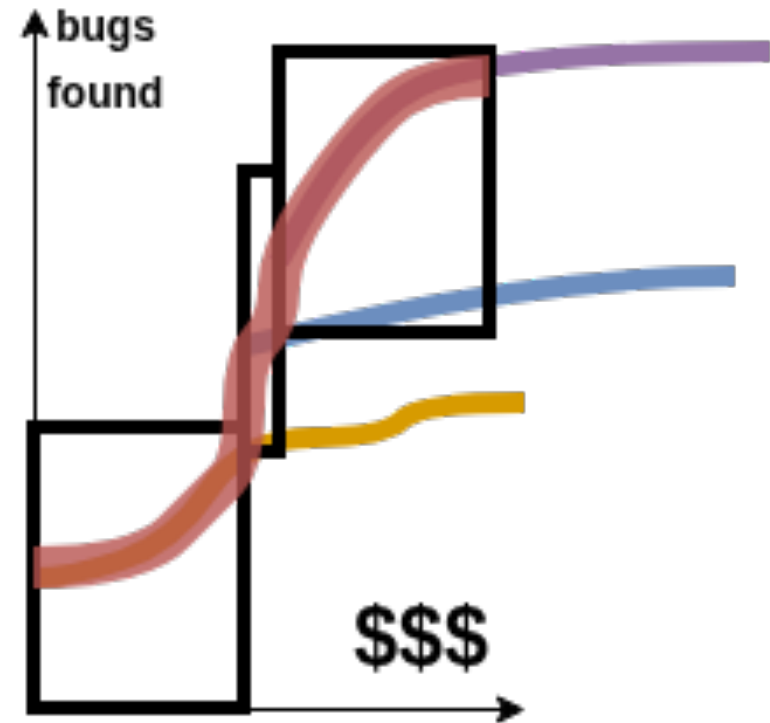
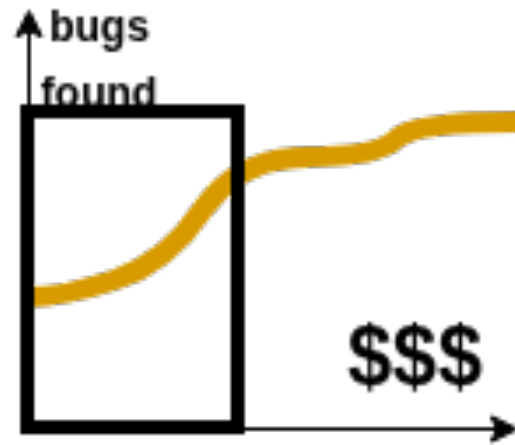
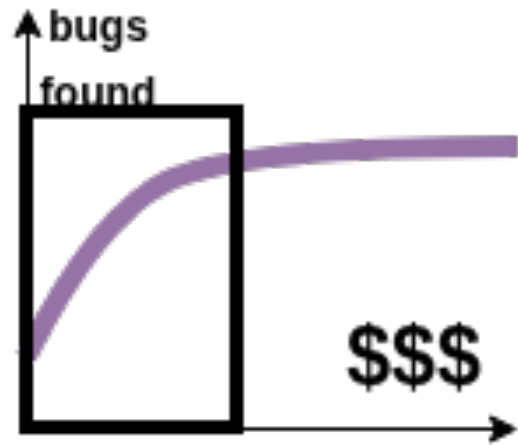
Diminishing returns



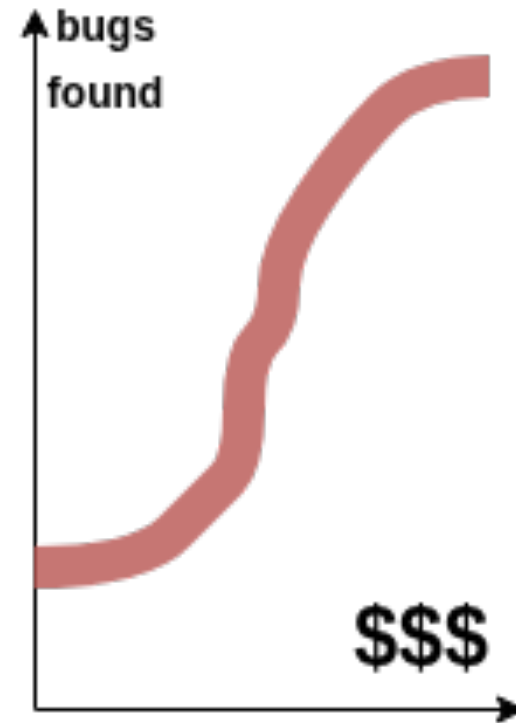
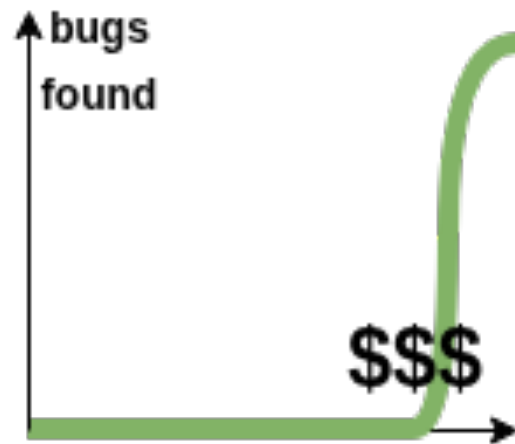
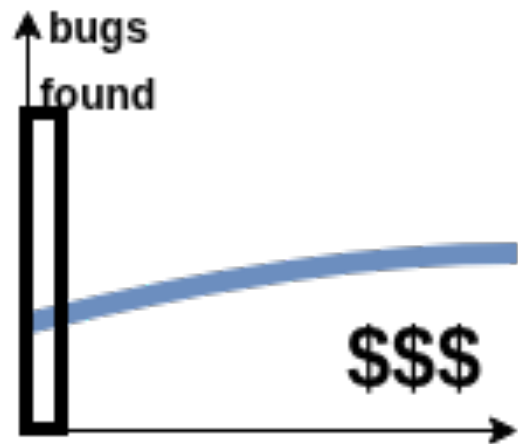
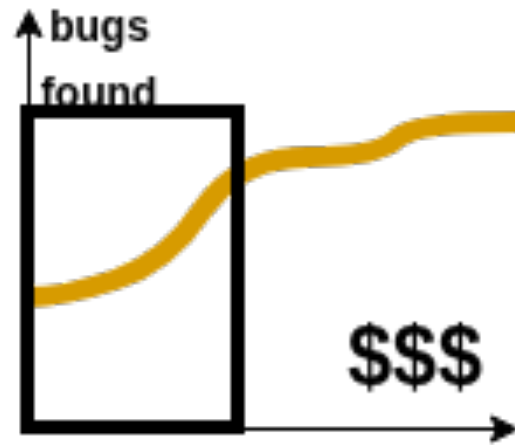
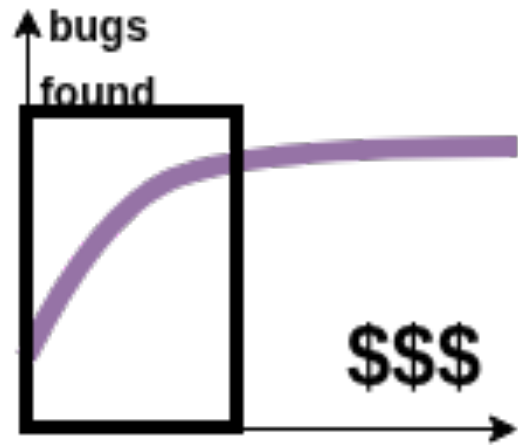
Diminishing returns



Diminishing returns



Diminishing returns



Who hunts for 🐛?



Who hunts for ?



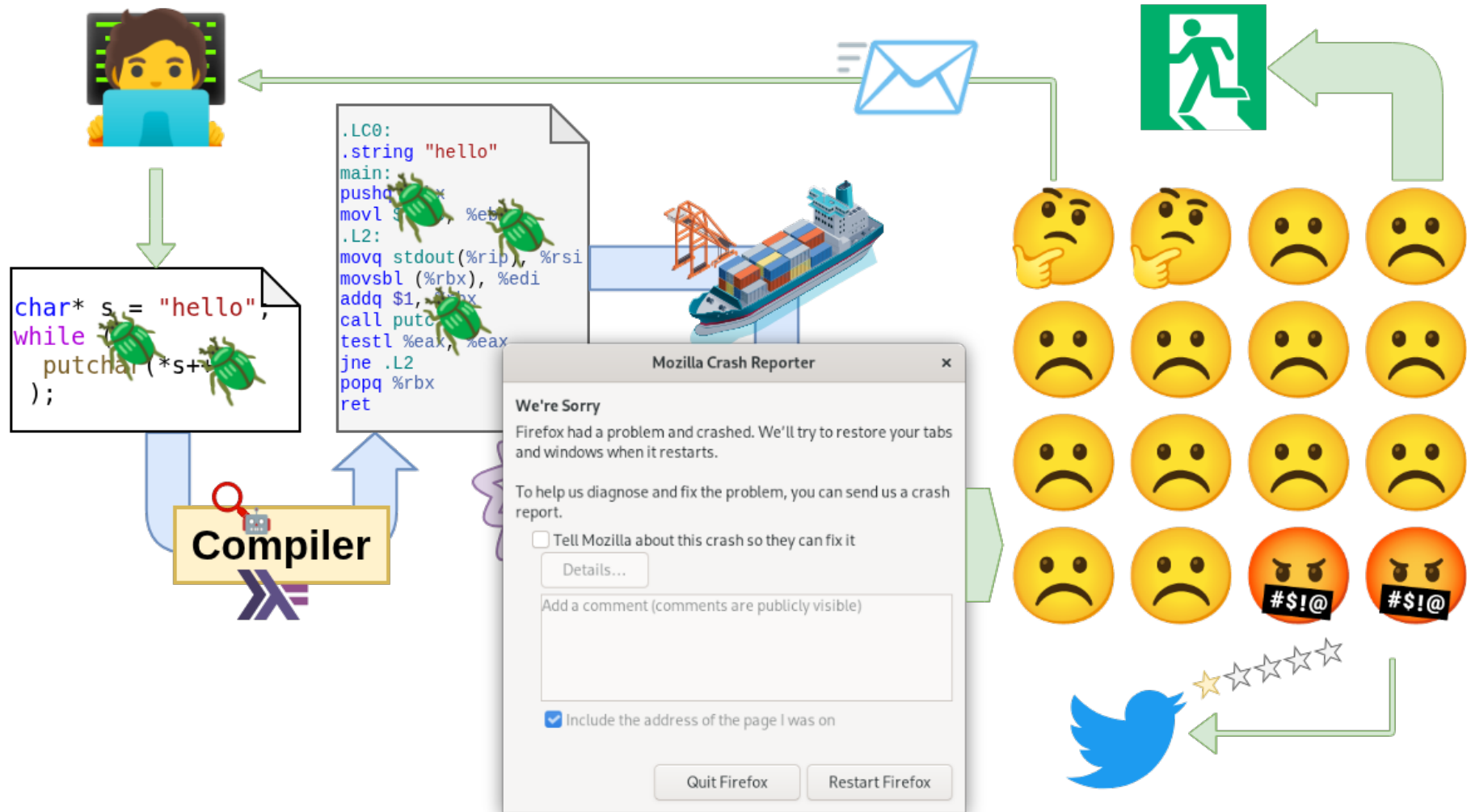
Who hunts for ?



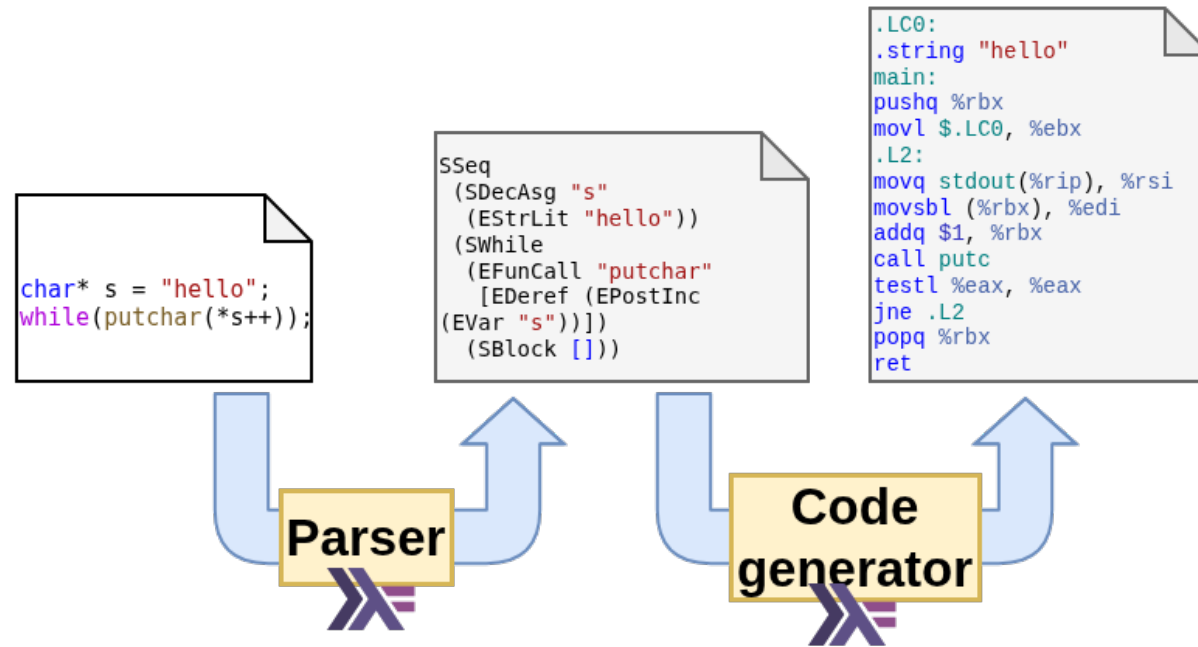
Who hunts for ?



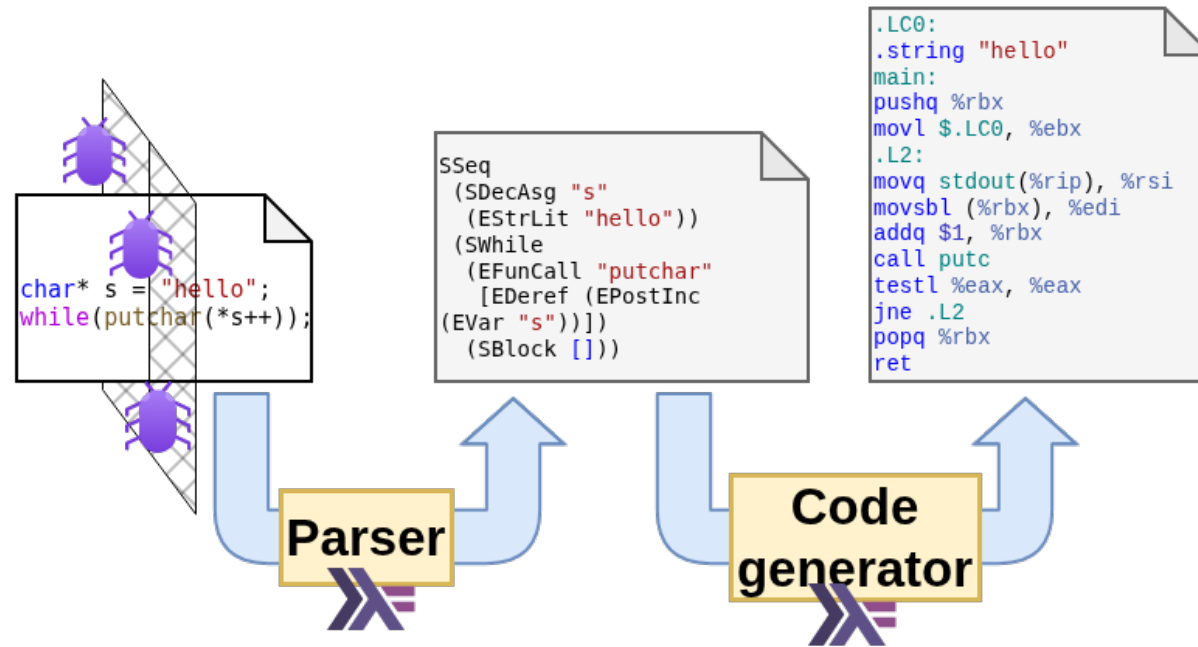
Compiler checks



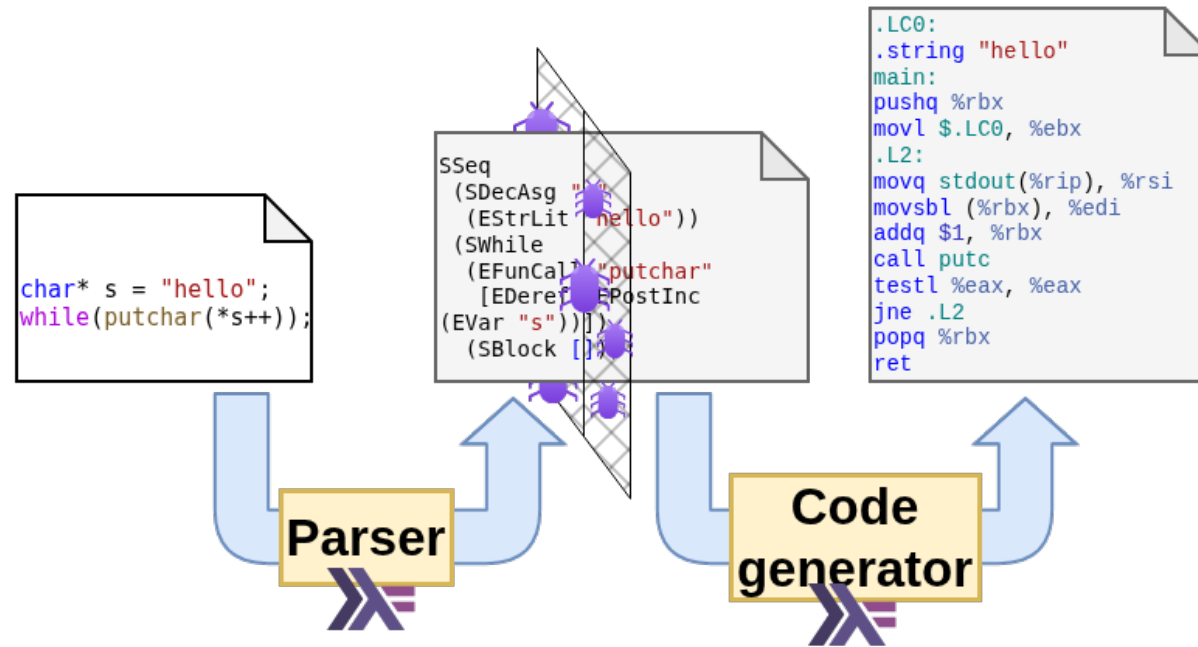
Compiler checks, but where?



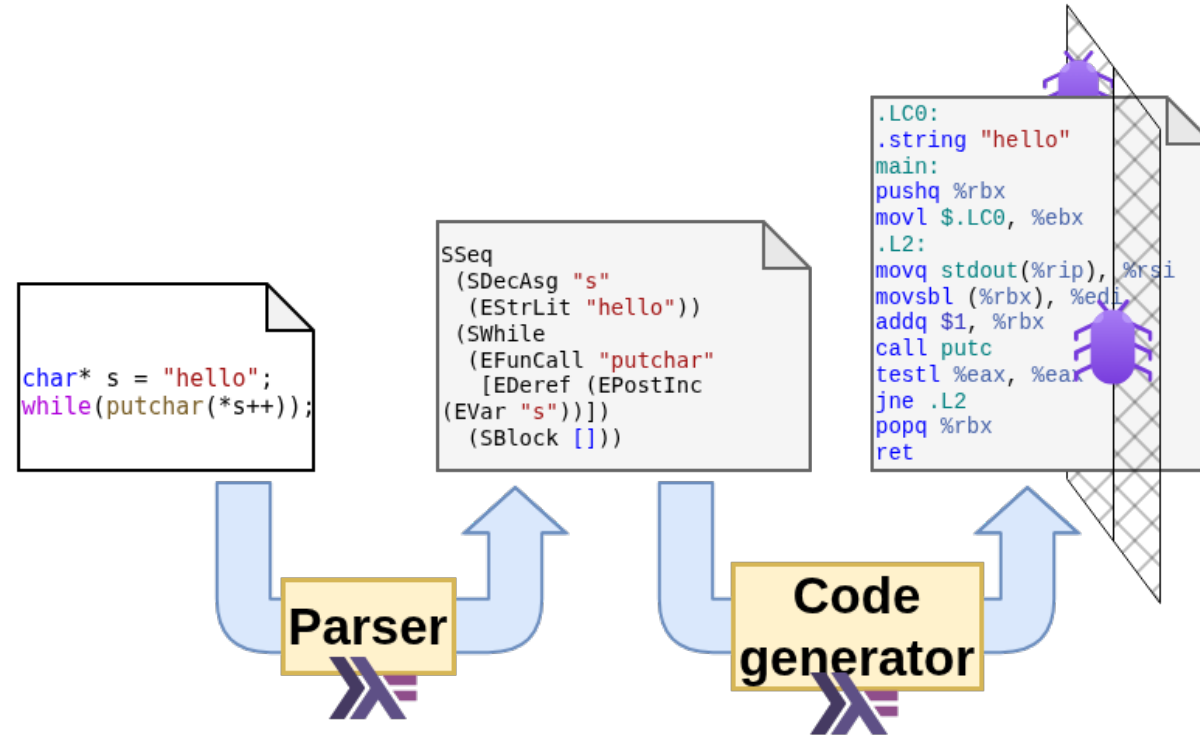
Compiler checks, but where?



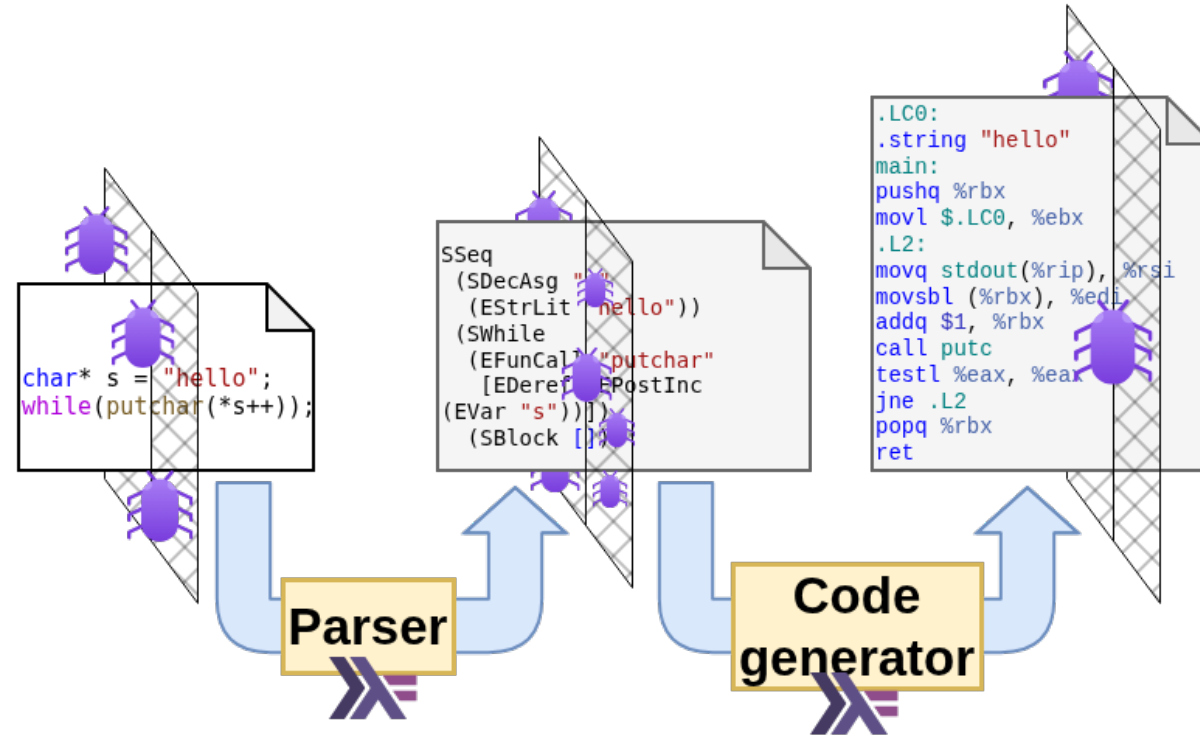
Compiler checks, but where?



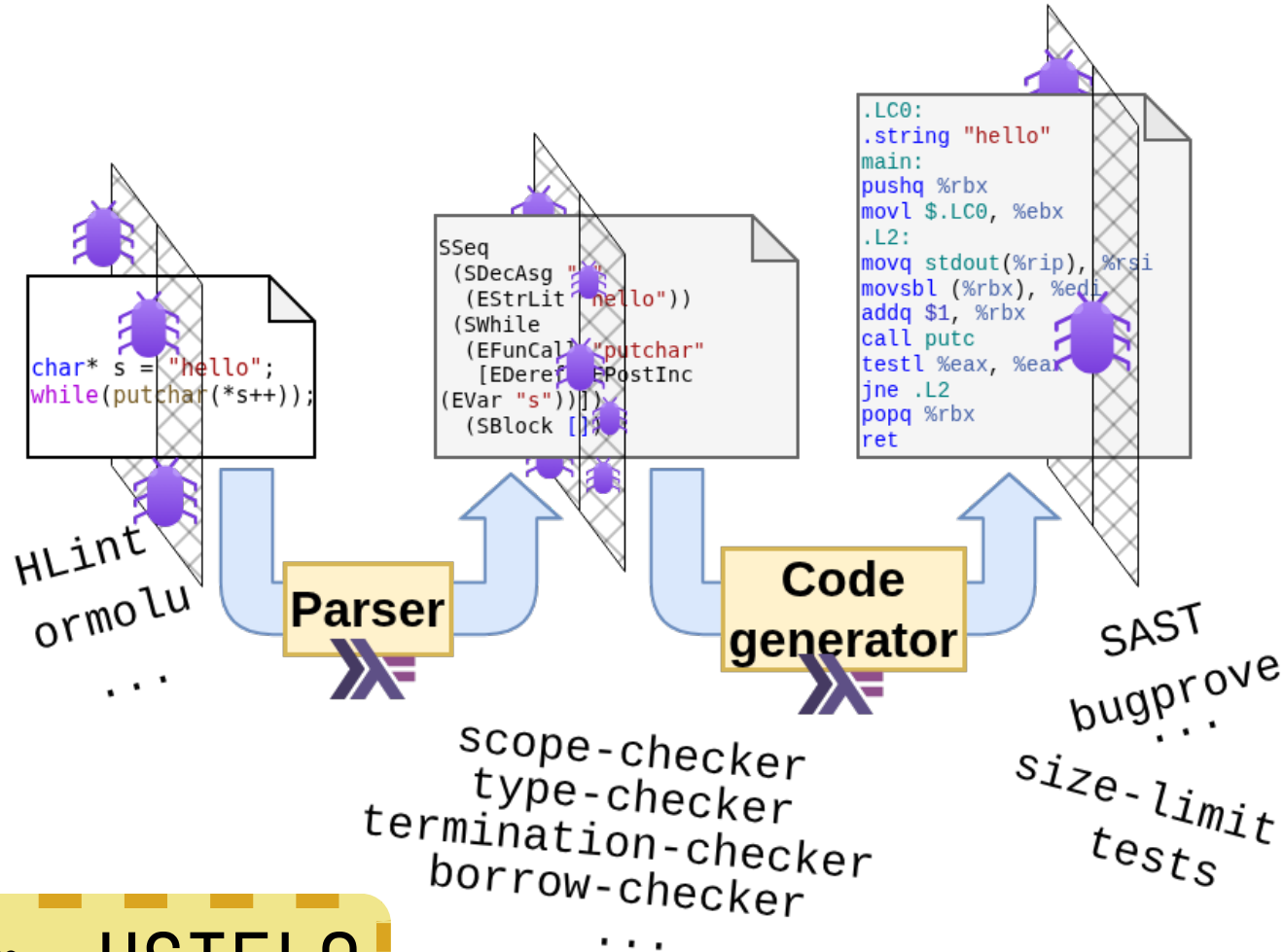
Compiler checks, but where?



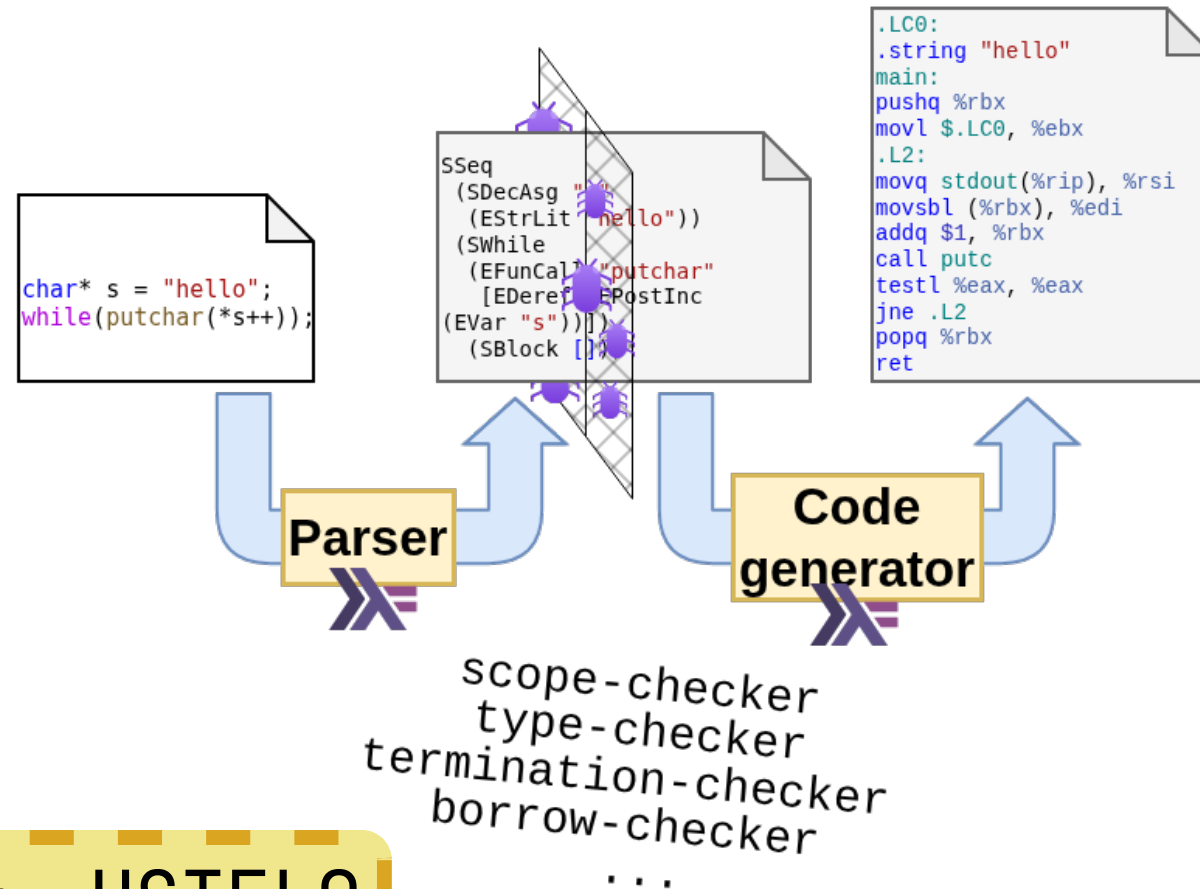
Compiler checks, but where?



Compiler checks, but where?



Compiler checks, but where?



Example

(live coding)

Summary (1/3)

check :: Annotation → Exp → Bool

infer :: Exp → Maybe Annotation

unsafeXXX :: Exp → ...

safeXXX :: Exp → Maybe ...

safeXXX e = infer e \$> unsafeXXX e

Summary (2/3)

`validate` $:: \text{Exp} \rightarrow \text{Valid} [\text{ErrorMsg}] \text{AnnotatedExp}$

$\text{Valid } a \ b \cong \text{Either } a \ b$

`safeXXX'` $:: \text{AnnotatedExp} \rightarrow \dots$

`safeXXX` $:: \text{Exp} \rightarrow \text{Valid} [\text{ErrorMsg}] \dots$

`safeXXX e = safeXXX' <$> validate e`

Summary (3/3)

