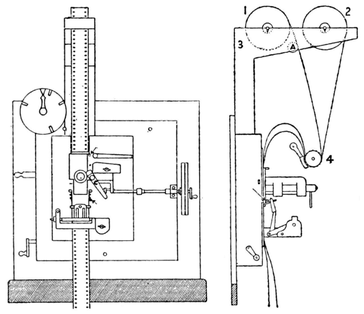
PolyTracker

Whole-Input Dynamic Information Flow Tracing

Evan Sultanik, Marek Surovič, Henrik Brodin, **Kelly Kaoudis**,
Facundo Tuesca, Carson Harmon, Lisa Overall,
Joseph Sweeney, Bradford Larsen

PolyTracker

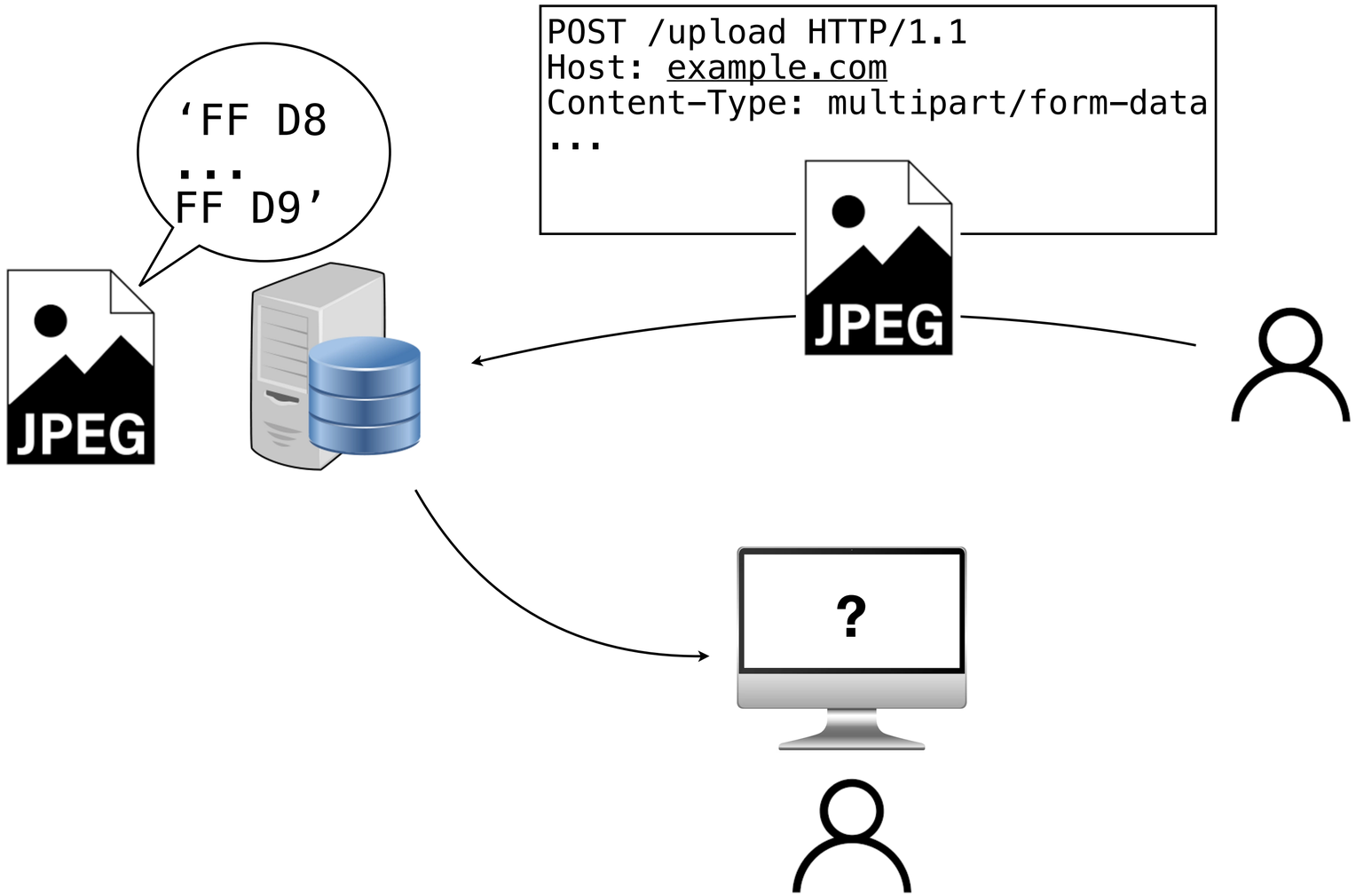
- Runtime (*dynamic* information flow tracing)
- Every input byte
- Record parts of CFG that data flow enters for later call stack reconstruction
- Intermediate labels' provenance relations to source *and* sink bytes
- Novel trace representation: the tainted directed acyclic graph



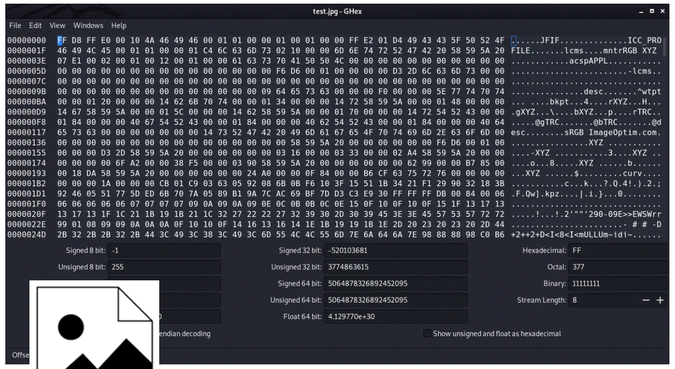

Spec

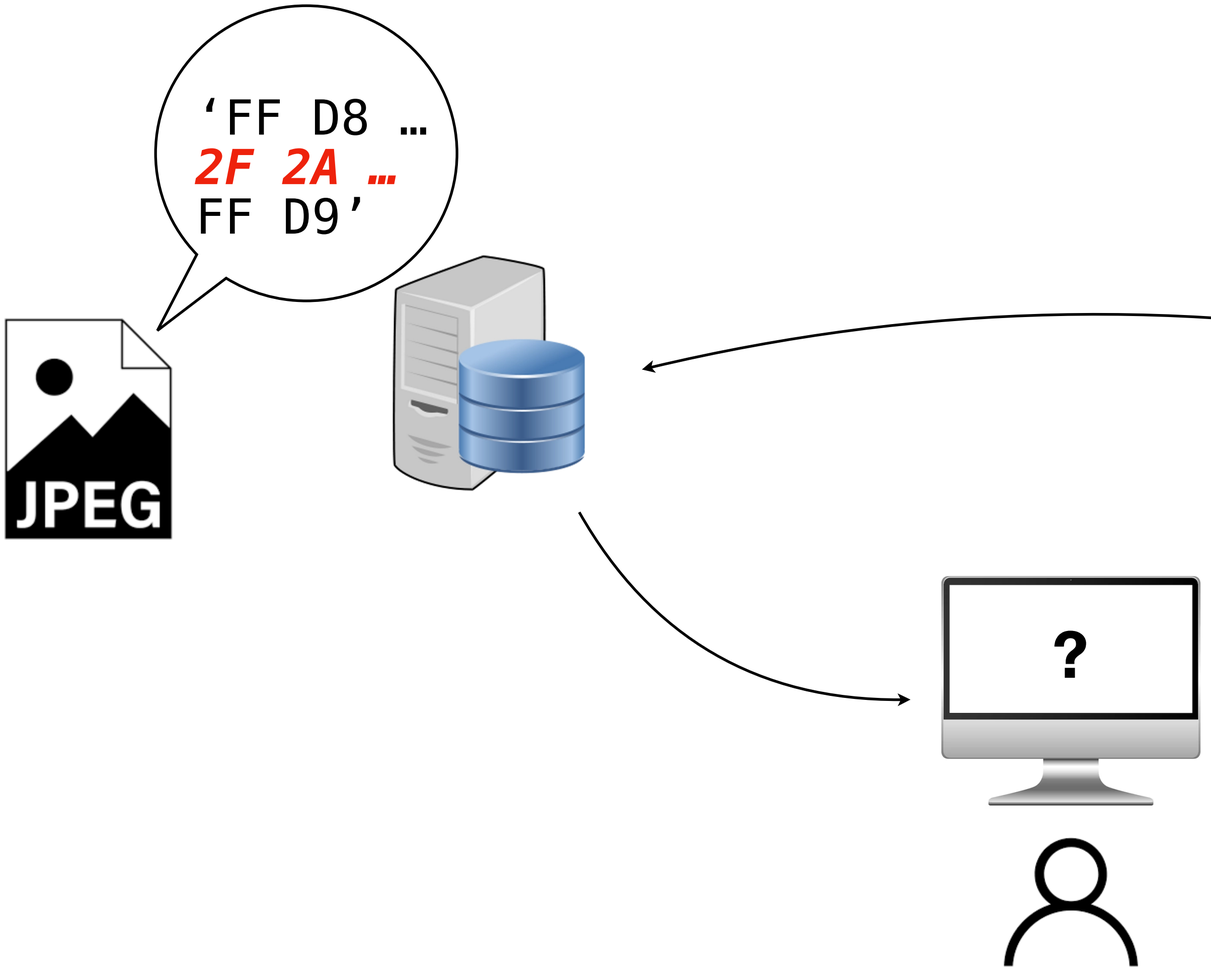

Spec
Spec

Malicious inputs?


‘FF D8
...
FF D9’
POST /upload HTTP/1.1
Host: example.com
Content-Type: multipart/form-data
...
JPEG
JPEG
?

https://infosecwriteups.com/exploiting-xss-with-javascript-jpeg-polyglot-4cff06f8201a
https://bugzilla.mozilla.org/show_bug.cgi?id=1288361





Research questions

Differences when handling benign and malicious input?

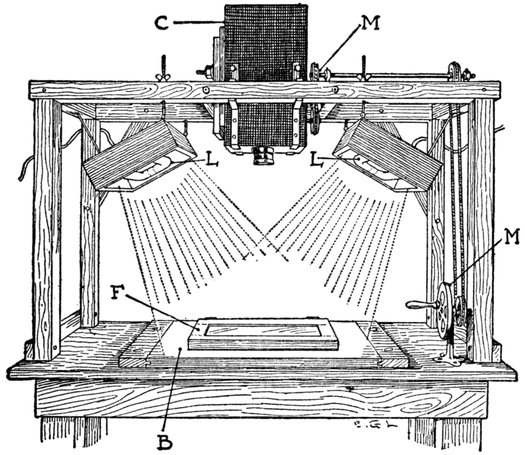
What program logic fails on unexpected input?

What differs between parsers that *should* implement the same input specification?

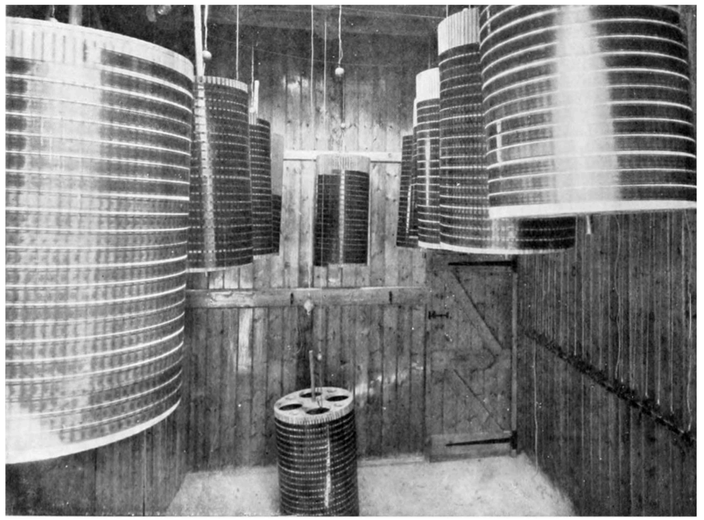
What parts of a specification enable creating polyglot files?

Format *ground truth*?

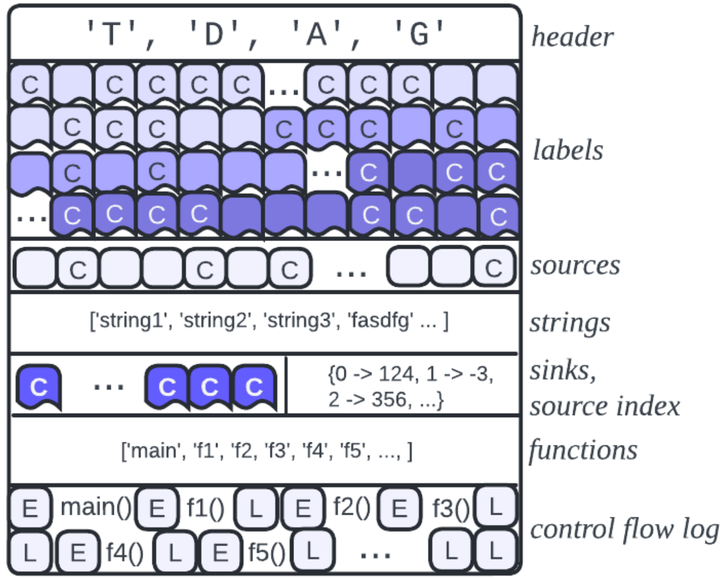
Challenge: manual instrumentation doesn’t scale



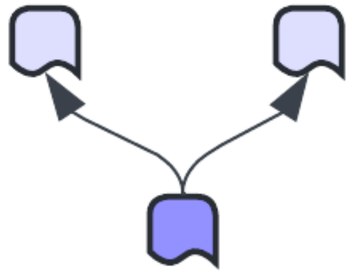
Challenge: *much* data



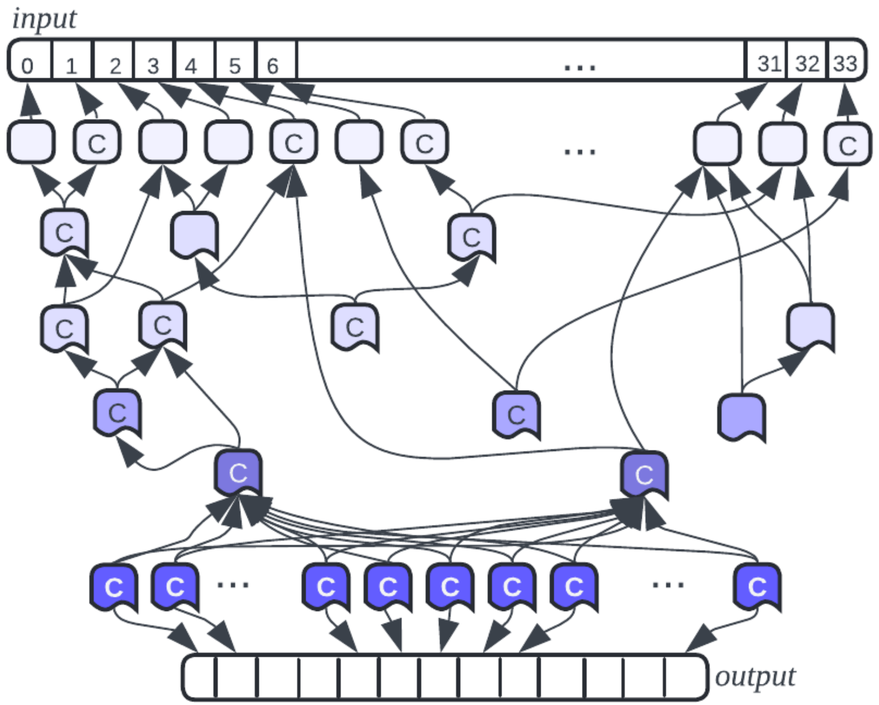
Tainted Directed Acyclic Graph (TDAG)

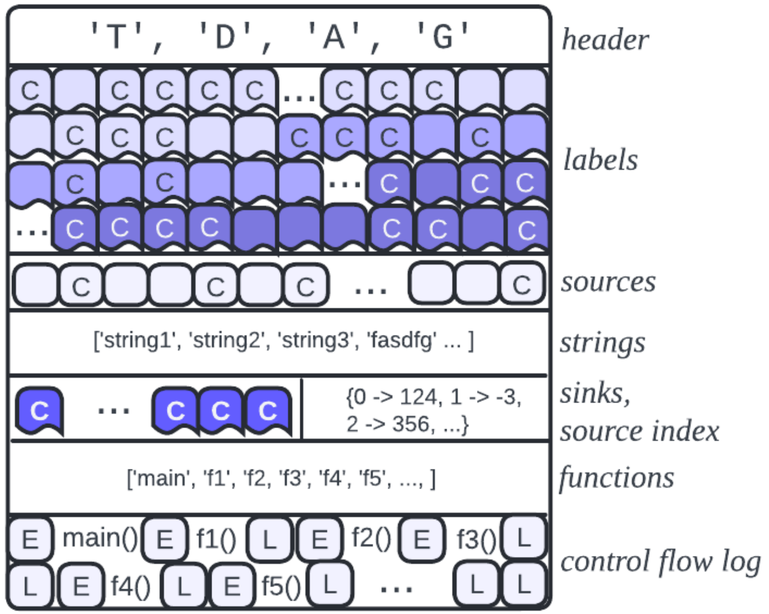


Tainted Directed Acyclic Graph (TDAG)

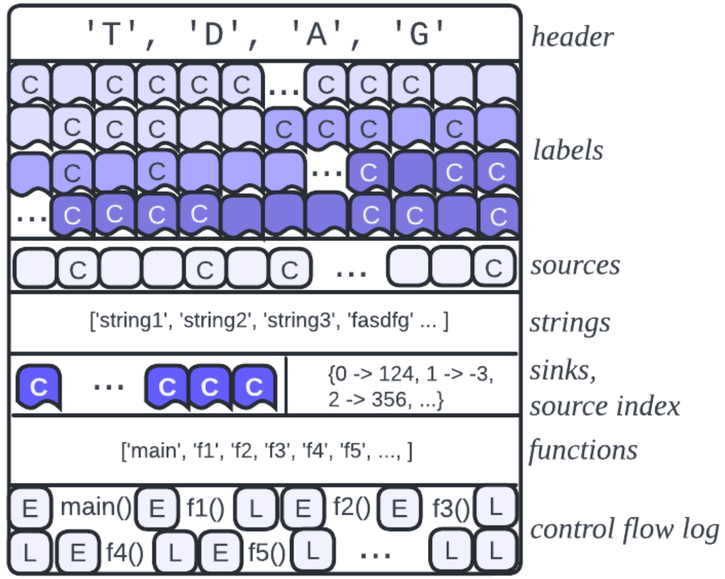


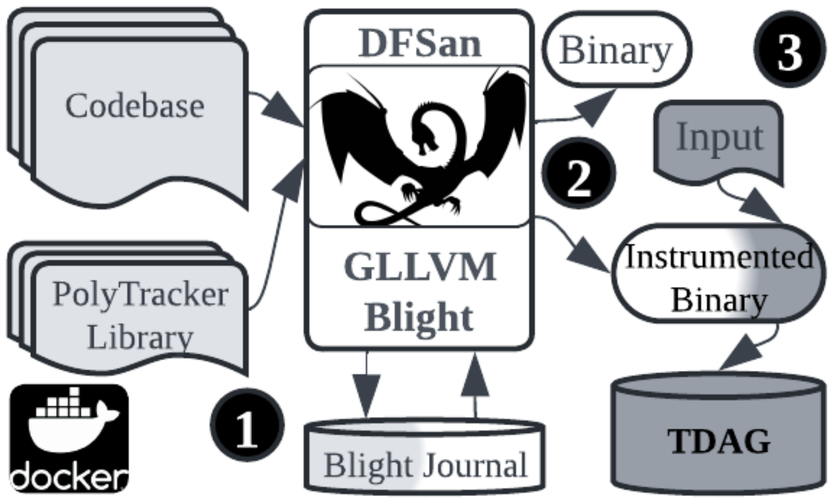
Tainted Directed Acyclic Graph (TDAG)





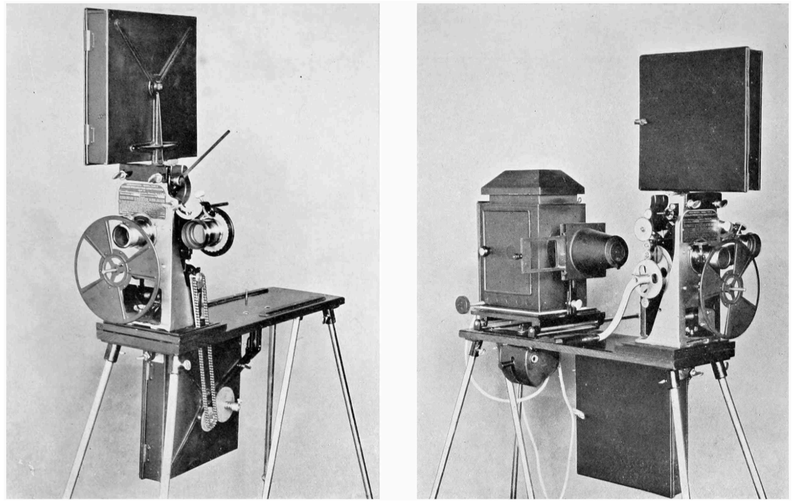
Tainted Directed Acyclic Graph (TDAG)





Write side implementation

```
root@a60fd5d03bf3:/polytracker/the_klondike/poppler# ls
AUTHORS                README-XPDF           config.h.cmake              hooks                      poppler                qt6
CMakeLists.txt         README.contributors   cpp                         make-glib-api-docs         poppler-cpp.pc.cmake   regtest
COPYING                README.md             do-the-gnupg-2.4-dance.sh   pdftops.instrumented       poppler-glib.pc.cmake  splash
COPYING3               _clang-format         fofi                        pdftops.instrumented.bc    poppler-qt5.pc.cmake   test
ConfigureChecks.cmake  blight_journal.jsonl  glib                        pdftotext.instrumented     poppler-qt6.pc.cmake   utils
INSTALL                build                 goo                         pdftotext.instrumented.bc  poppler.pc.cmake
NEWS                   cmake                 gtkdoc.py                   polytracker.tdag           qt5
root@a60fd5d03bf3:/polytracker/the_klondike/poppler#
```



ISSTA Tool Demonstrations | 18 September 2024 | kelly.kaoudis@trailofbits.com

https://github.com/trailofbits/polytracker

TRAIL OF BITS