SOF

1

Program Anal

OFTWARE LIC

A THING OF

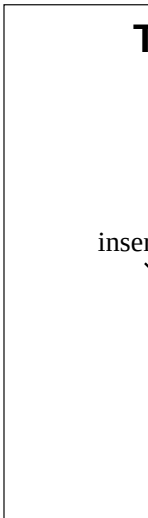
Bypassing Them Is

nalysis

CENSE CHEC

OF THE PAST!

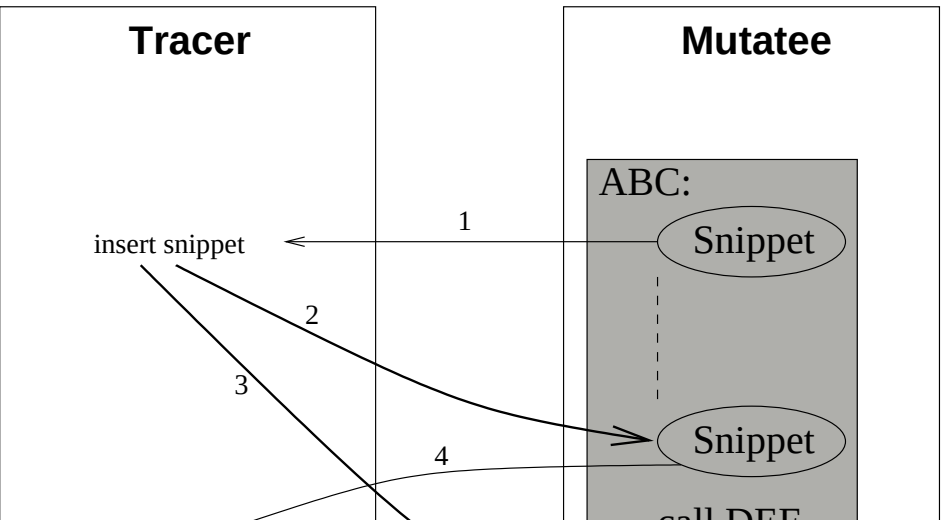
Is As Easy As 1-2-3...



CKS?

Tevfik Kosar
Mihai Christodorescu
Rob Iverson

• • •



- Trace function
  - Incrementa
  - Function F
- Compare outpu

failed runs

- Decide on a sub

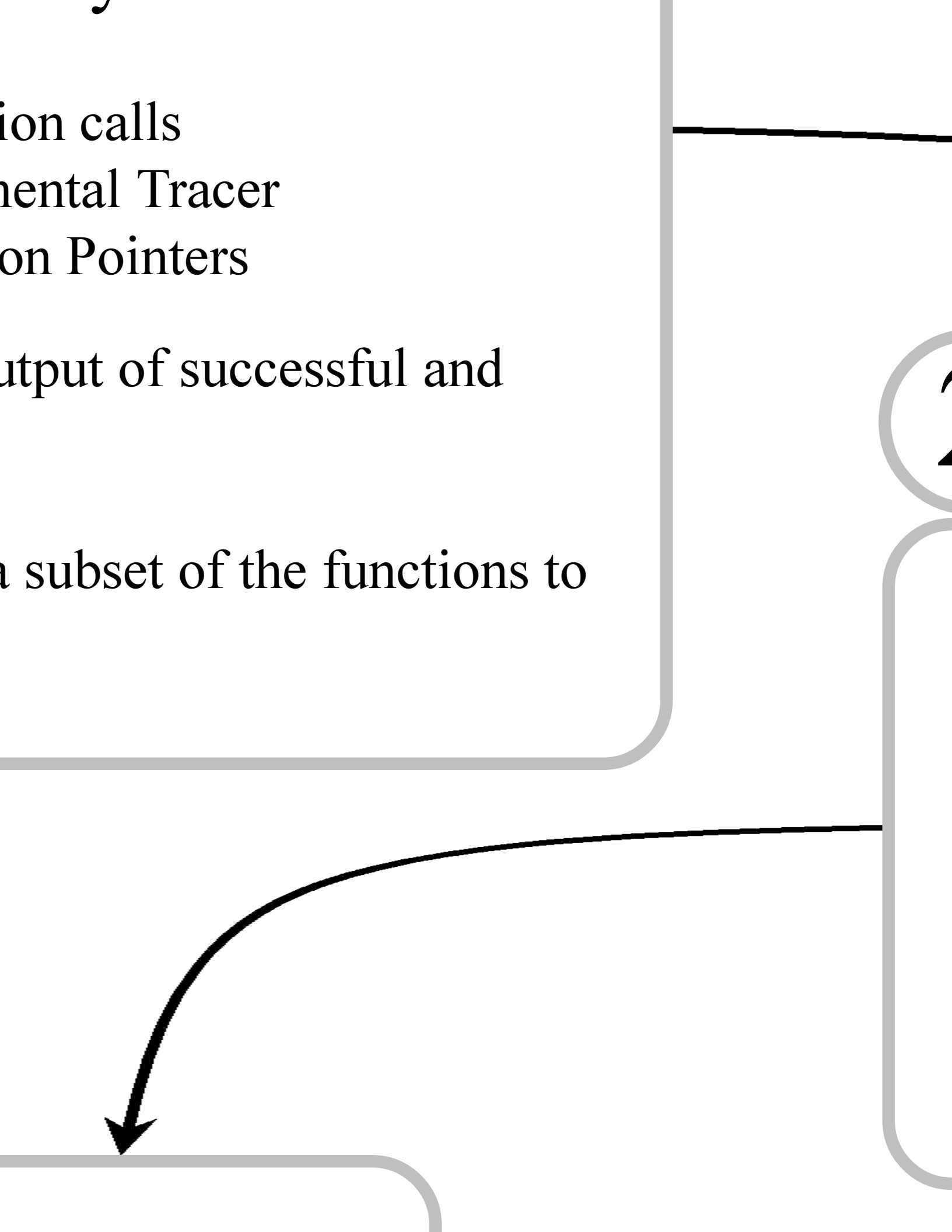
focus on

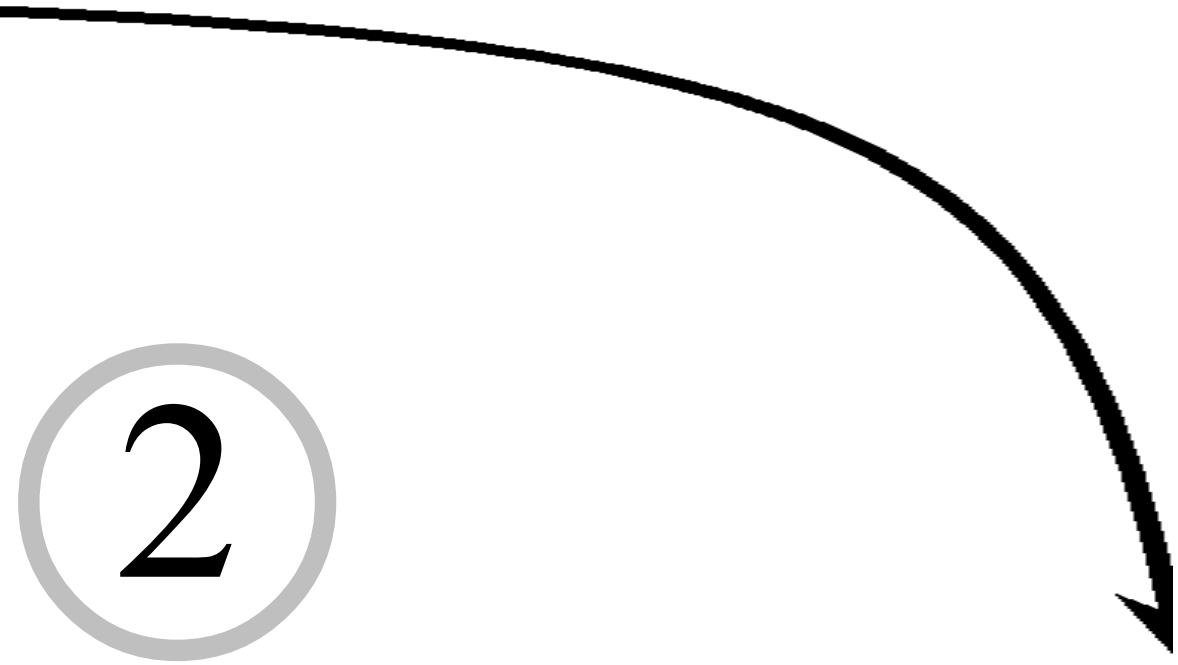
3

ion calls
nental Tracer
on Pointers

utput of successful and

a subset of the functions to

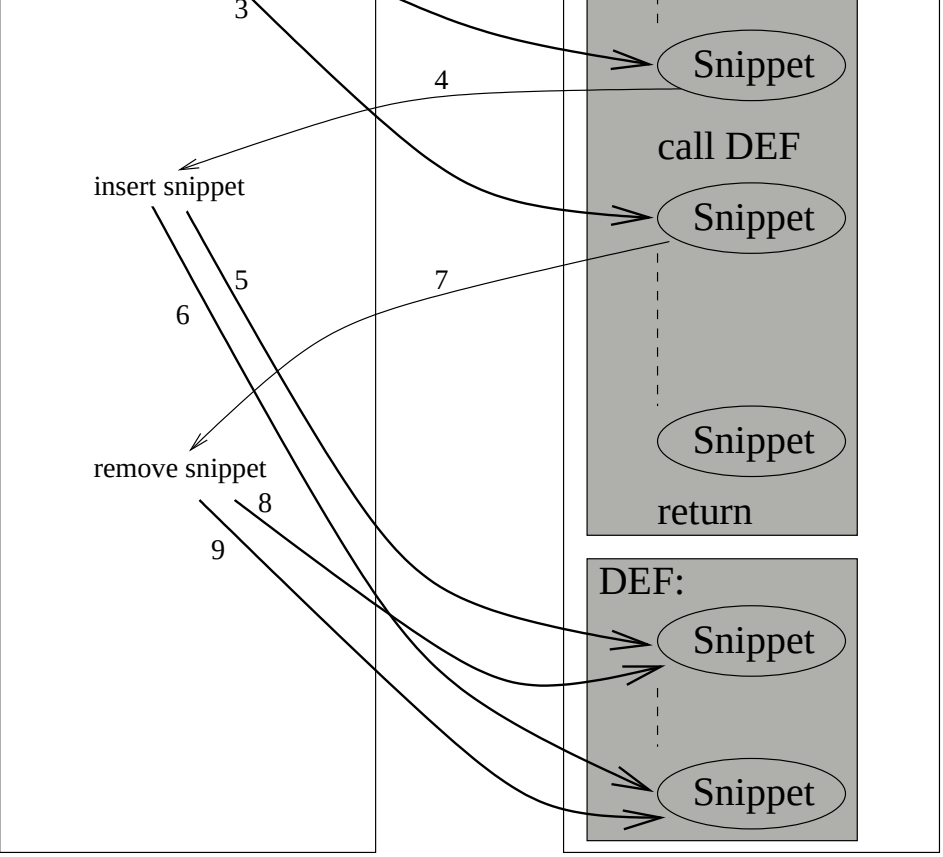




2

License-Checking Detailed

- I/O logging and analysis
- Function return value comparison
- Pointer tracking for structure analy



ed Analysis

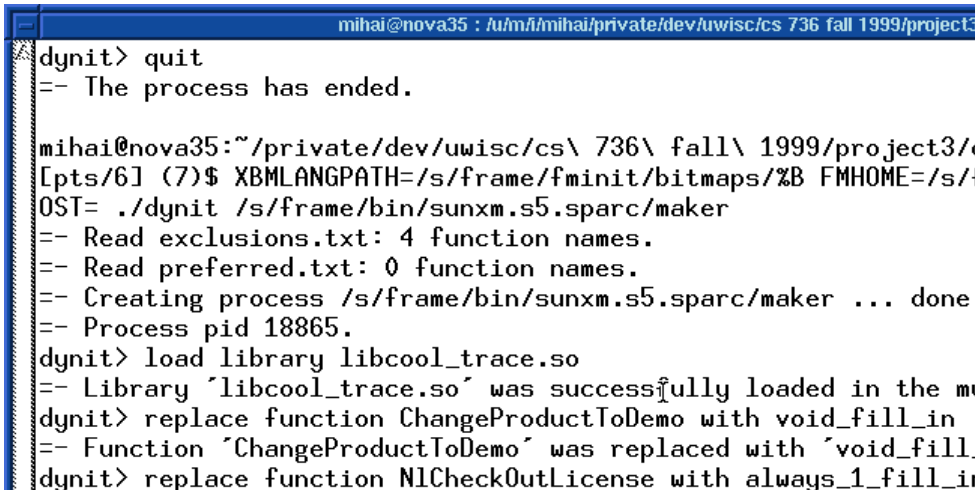
son

nalysis [planned]

Binary Code

- Skip function c
- Replace functi
- Modify progra

dynit Shell



ode Rewriting

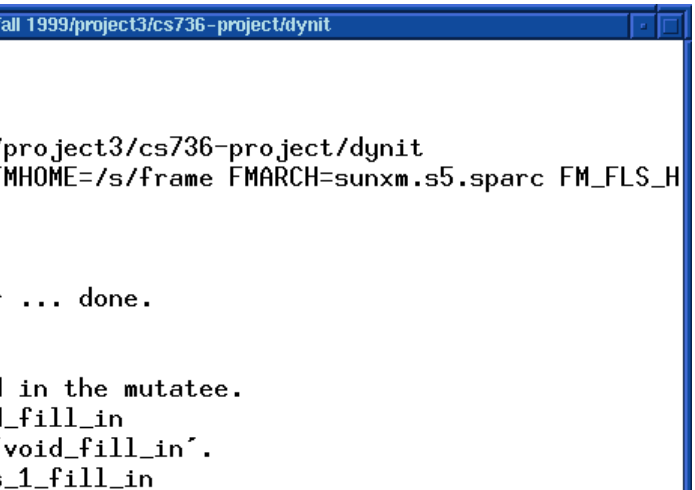
on calls

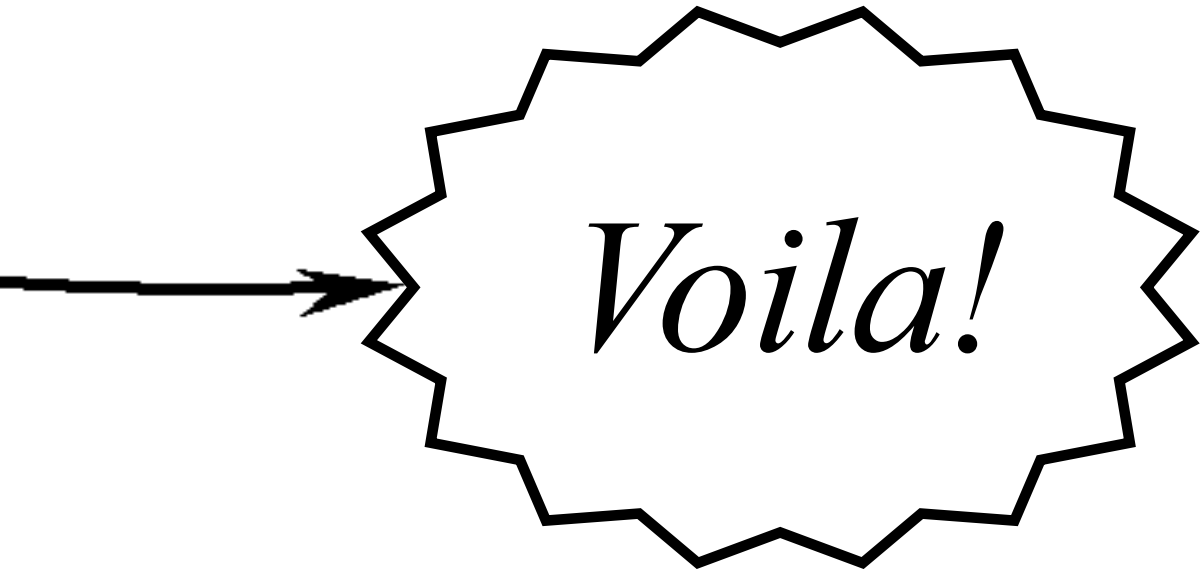
nctions

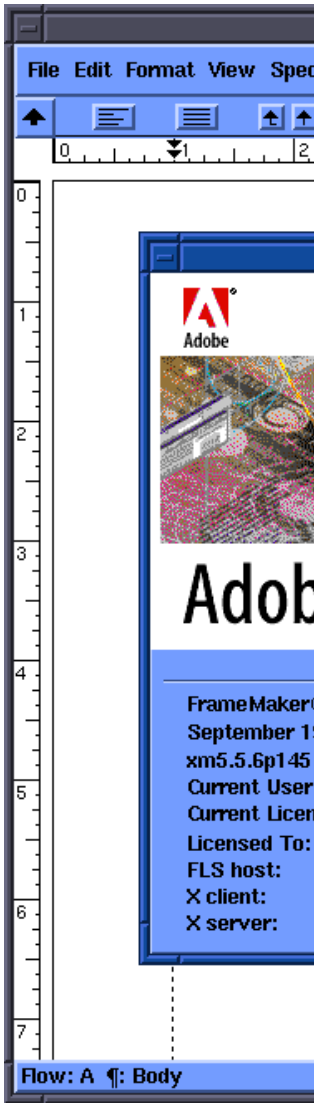
ogram variables

You too can do it, with

hell



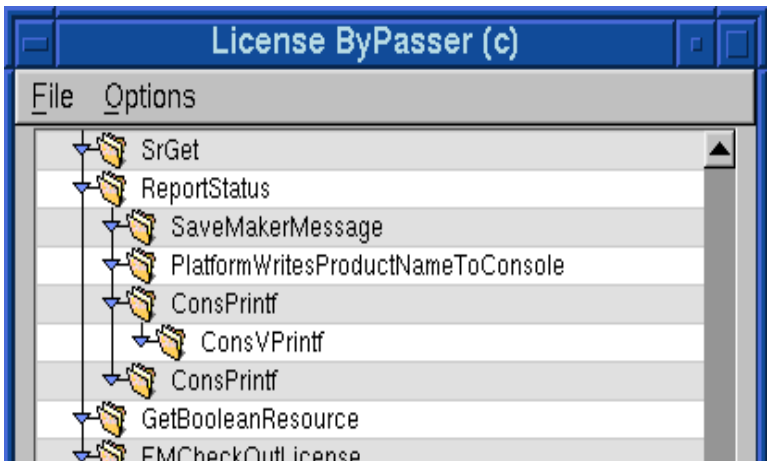


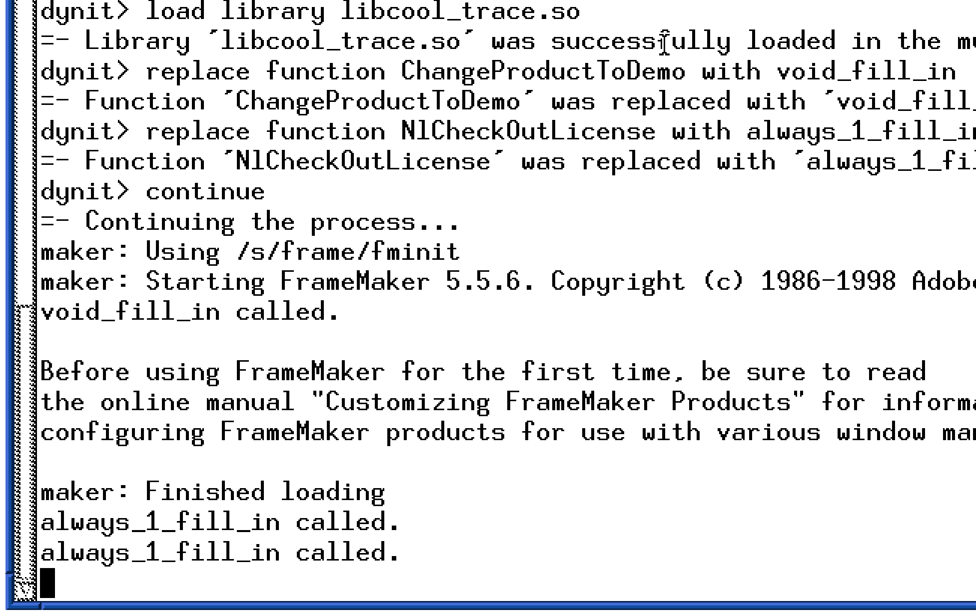


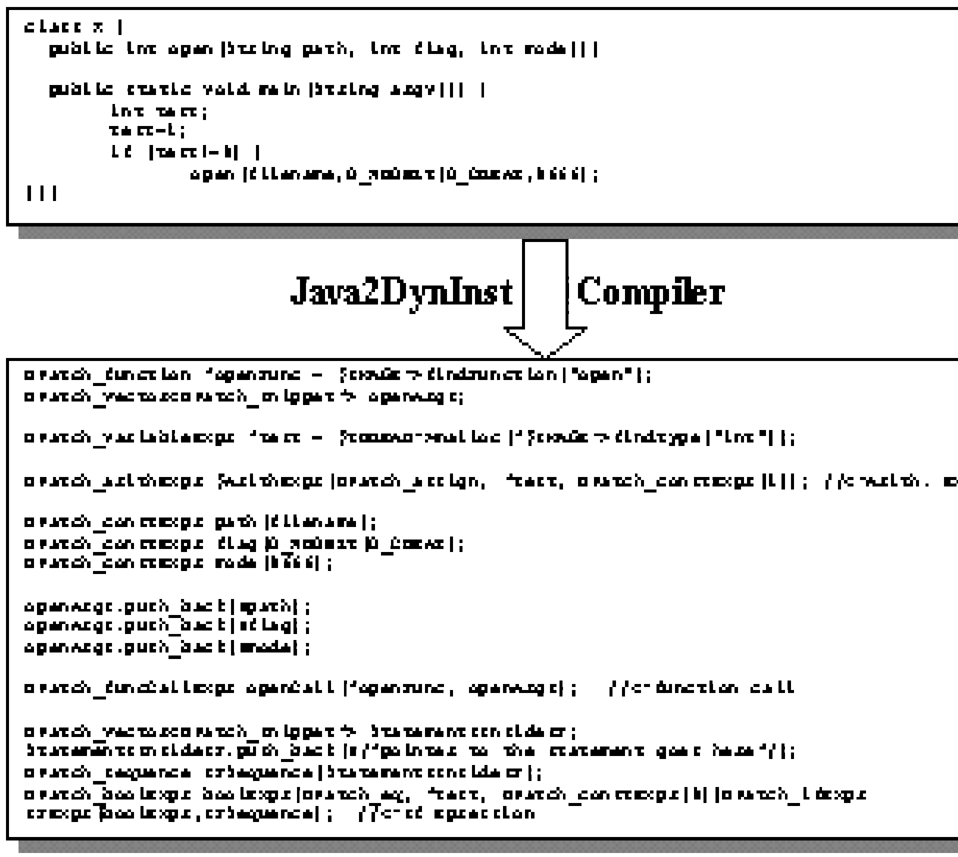
with these powerful tools:

USER

ByPasser GUI




dynit> load library libcool_trace.so
=- Library ´libcool_trace.so´ was successfully loaded in the mu
dynit> replace function ChangeProductToDemo with void_fill_in
=- Function ´ChangeProductToDemo´ was replaced with ´void_fill_
dynit> replace function NlCheckOutLicense with always_1_fill_in
=- Function ´NlCheckOutLicense´ was replaced with ´always_1_fil
dynit> continue
=- Continuing the process...
maker: Using /s/frame/fminit
maker: Starting FrameMaker 5.5.6. Copyright (c) 1986-1998 Adobe
void_fill_in called.
Before using FrameMaker for the first time, be sure to read
the online manual "Customizing FrameMaker Products" for informa
configuring FrameMaker products for use with various window man
maker: Finished loading
always_1_fill_in called.
always_1_fill_in called.


Java2DynInst
Compiler

] in the mutatee.
]_fill_in
`void_fill_in´.
s_1_fill_in
`ways_1_fill_in´.

-1998 Adobe Systems Incorporated.

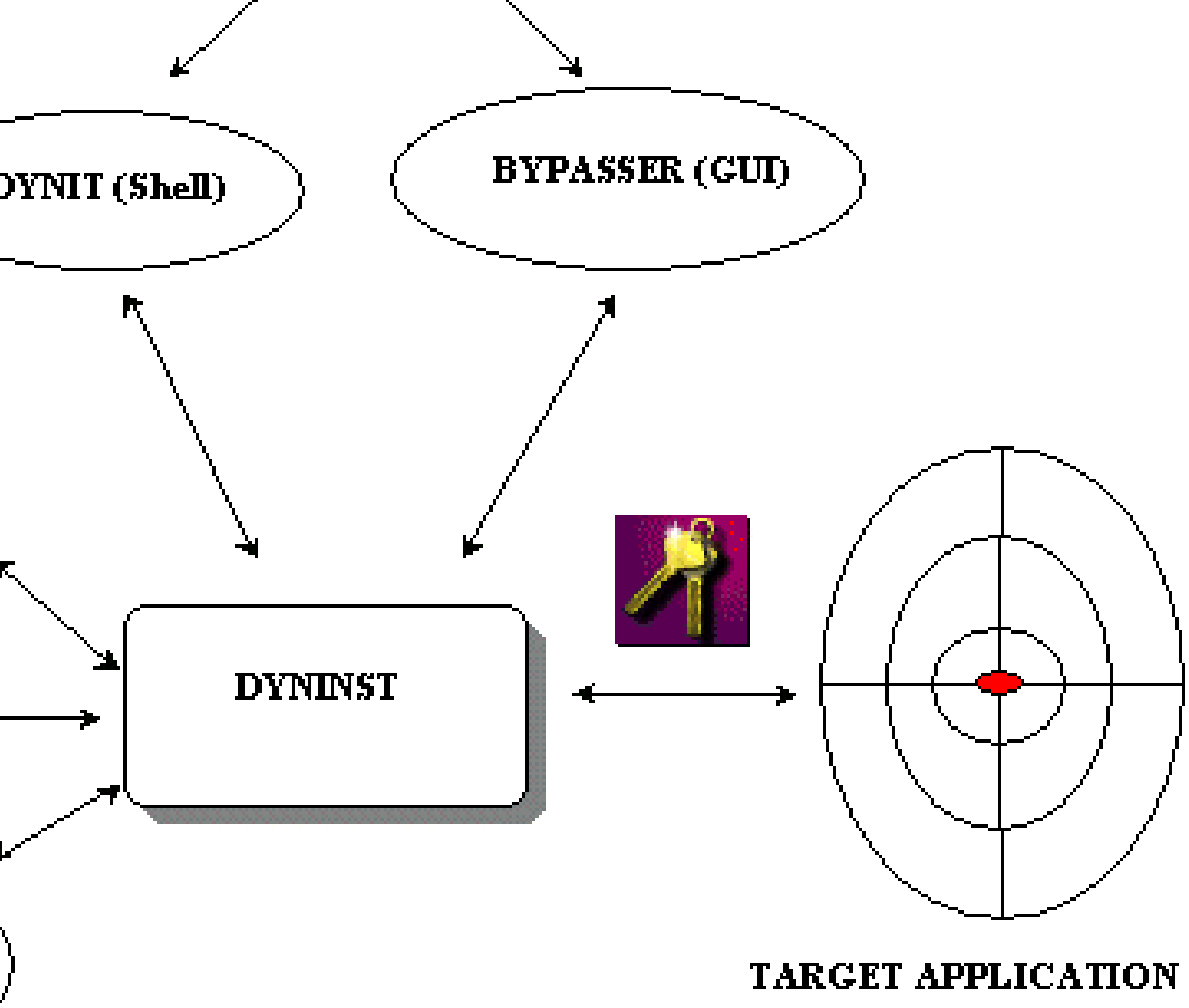
to read
for information on
window managers.

DYNIT

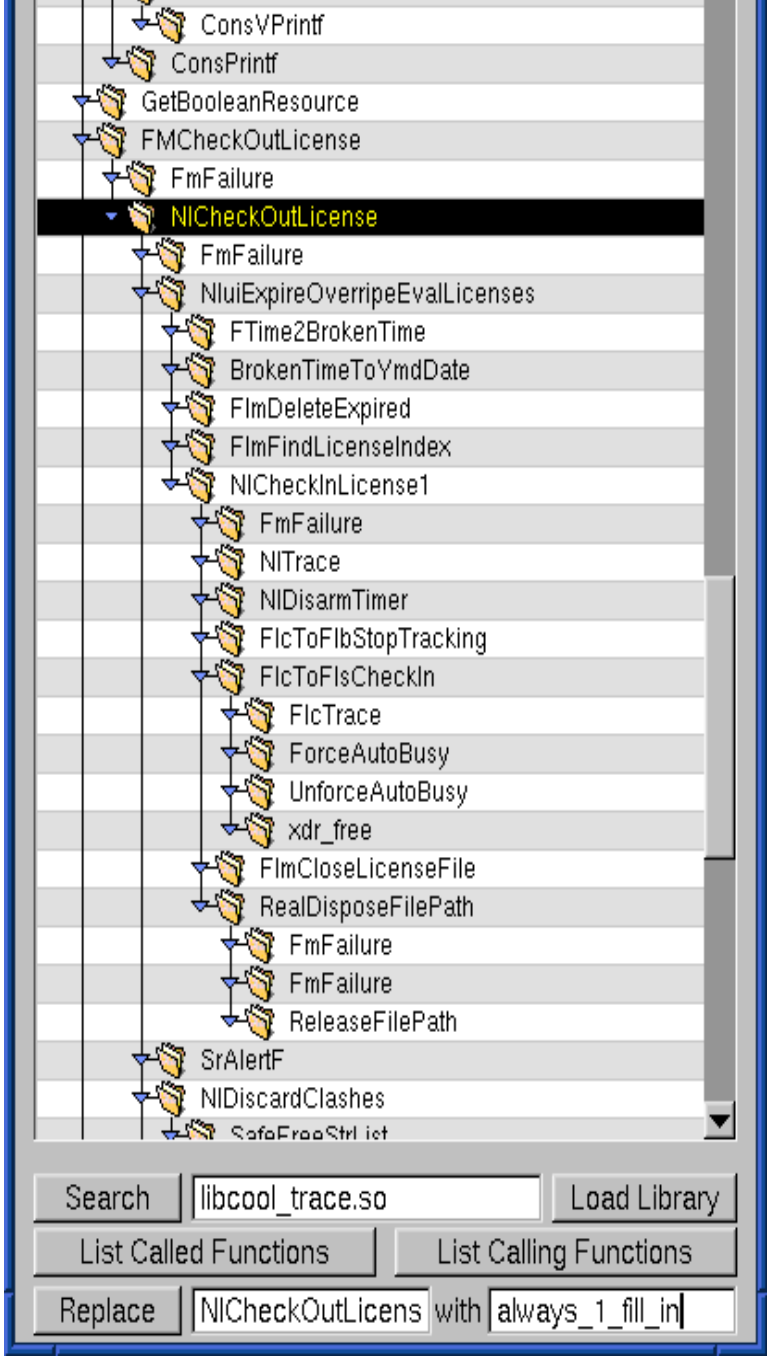
JAVA_2_DYNINST
COMPILER

PROGRAMMER

PARAMETER
PARSER



Note: portions of this poster were designed using H



sing FrameMaker without a valid license.