



SoF

1

Program Anal



SOFTWARE LICENSING A THING OF

Bypassing Them Is

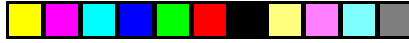
analysis



CENSE CHECK OF THE PAST!

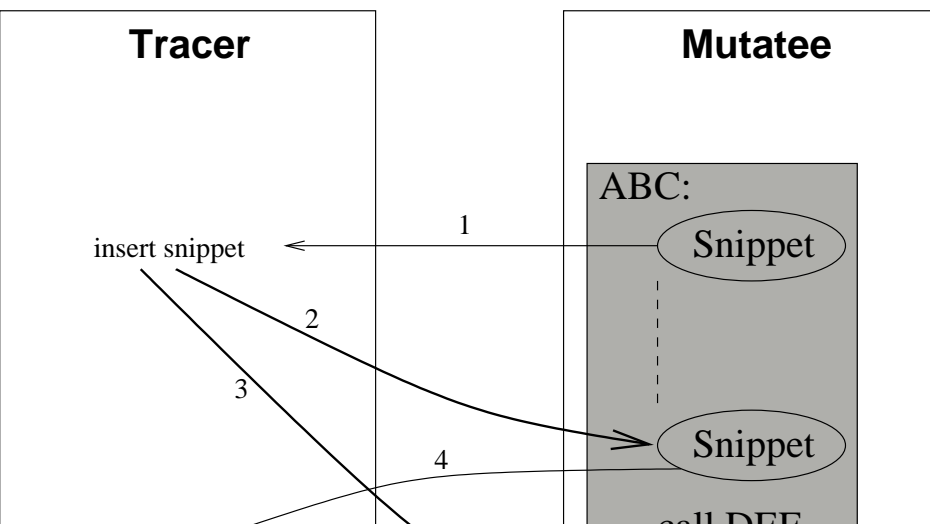
Is As Easy As 1-2-3...

CKS?



Tevfik Kosar
Mihai Christodorescu
Rob Iversen

• • •



- Trace function c
 - Increment
 - Function P
- Compare output
failed runs
- Decide on a sub
focus on

3



ion calls
mental Tracer
on Pointers

output of successful and

a subset of the functions to

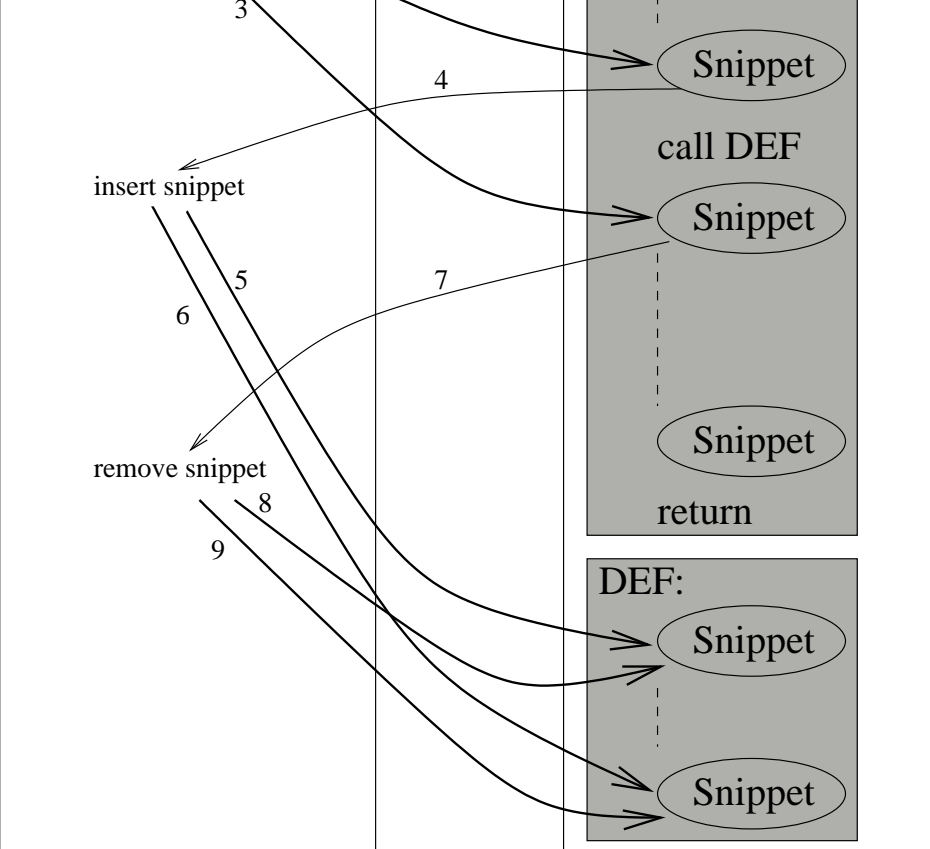




2

License-Checking Detailed

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



ed Analysis

son

analysis [planned]





Binary Code

- Skip function c
- Replace functi
- Modify progra

dynit Shell

```
mihai@nova35 : /u/m/mihai/private/dev/uwisc/cs 736 fall 1999/project3
dynit> quit
=- The process has ended.

mihai@nova35:~/private/dev/uwisc/cs\ 736\ fall\ 1999/project3/
[pts/6] (7)$ XBMLANGPATH=/s/frame/fminit/bitmaps/%B FMHOME=/s/
OST= ./dynit /s/frame/bin/sunxm.s5.sparc/maker
=- Read exclusions.txt: 4 function names.
=- Read preferred.txt: 0 function names.
=- Creating process /s/frame/bin/sunxm.s5.sparc/maker ... done
=- Process pid 18865.
dynit> load library libcool_trace.so
=- Library "libcool_trace.so" was successfully loaded in the m
dynit> replace function ChangeProductToDemo with void_fill_in
=- Function "ChangeProductToDemo" was replaced with "void_fill
dynit> replace function NlCheckOutLicense with always_1_fill_i
```

Code Rewriting

on calls

nctions

rogram variables

You too can do it, with

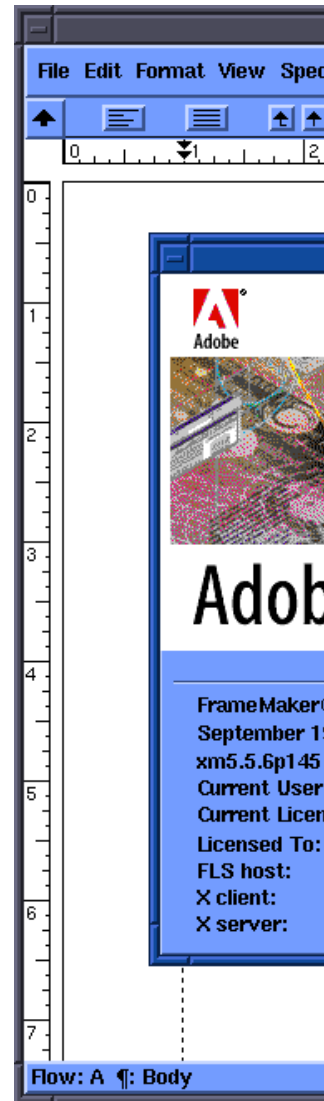
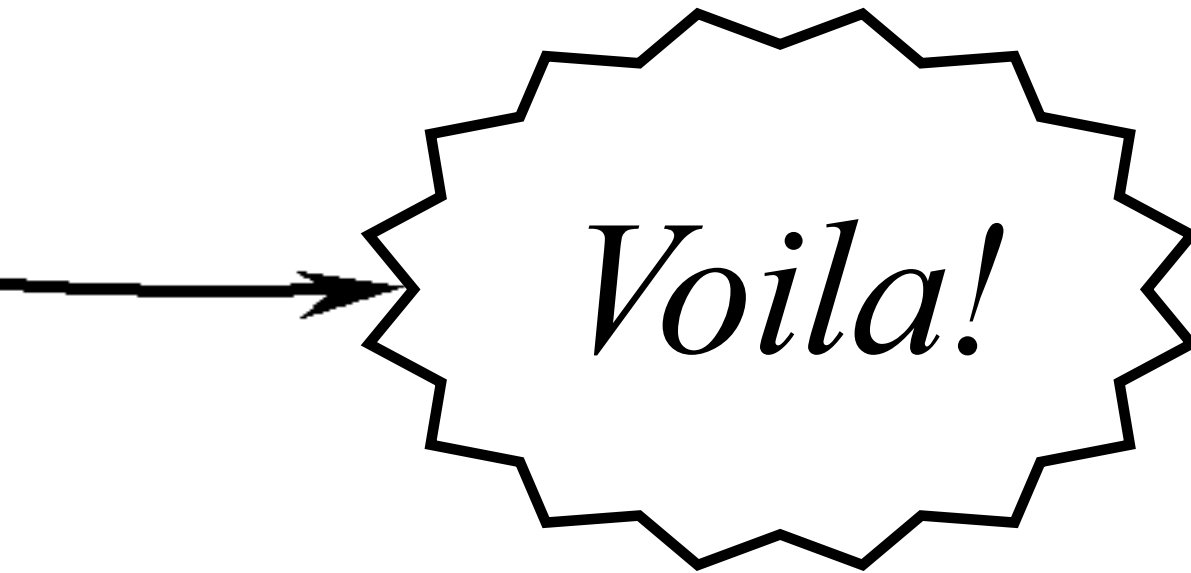
hell

```
all 1999/project3/cs736-project/dynit

/project3/cs736-project/dynit
MHOME=/s/frame FMARCH=sunxm.s5.sparc FM_FLS_H

... done.

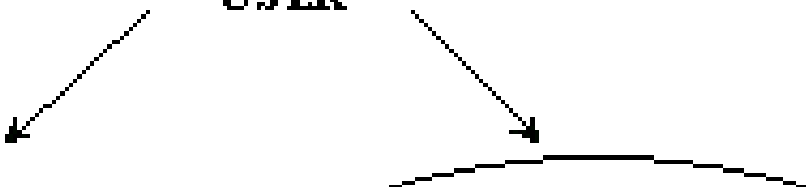
in the mutatee.
_fill_in
void_fill_in`.
_1_fill_in
```



with these powerful tools:

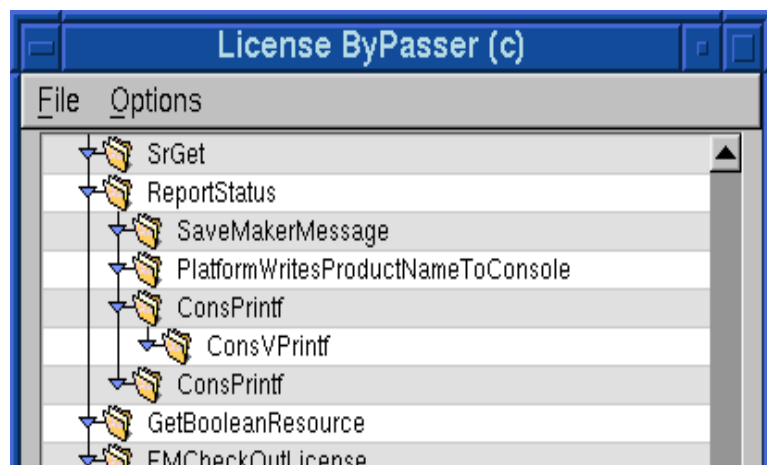


USER





ByPasser GUI



```

dynit> load library libcool_trace.so
=- Library 'libcool_trace.so' was successfully loaded in the m
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.fi
dynit> continue
=- Continuing the process...
maker: Using /s/frame/fmunit
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 information configuring FrameMaker products for use with various window man

```

maker: Finished loading
always_1_fill_in called.
always_1_fill_in called.

```

```

class x {
public: int open (string path, int flag, int mode) {}

public: static void main (string argv[]) {
    int test;
    test=1;
    if (test!=1) {
        open ("filename",0,mode) (0,mode,0);
    }
}
}

```

Java2DynInst **↓** Compiler

```

o match_function "openfunc = {codegen->findfunction} "open";
o match_macrocode match_macrocode "openfunc";

o match_variablecode "test = {codegen->evalloc} {codegen->findtype} "int";

o match_statementcode {statementcode} match_statement "test, o match_codegen {1}; //c-statement.

o match_codegen {path} {filename};
o match_codegen {flag} {mode} {0,mode};
o match_codegen {mode} {0,mode};

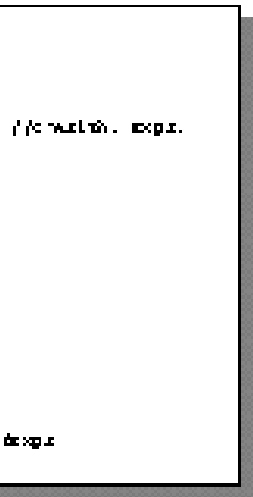
openfunc.push_back {path};
openfunc.push_back {flag};
openfunc.push_back {mode};

o match_functioncode {openfunc} {openfunc, openfunc}; //c-function call

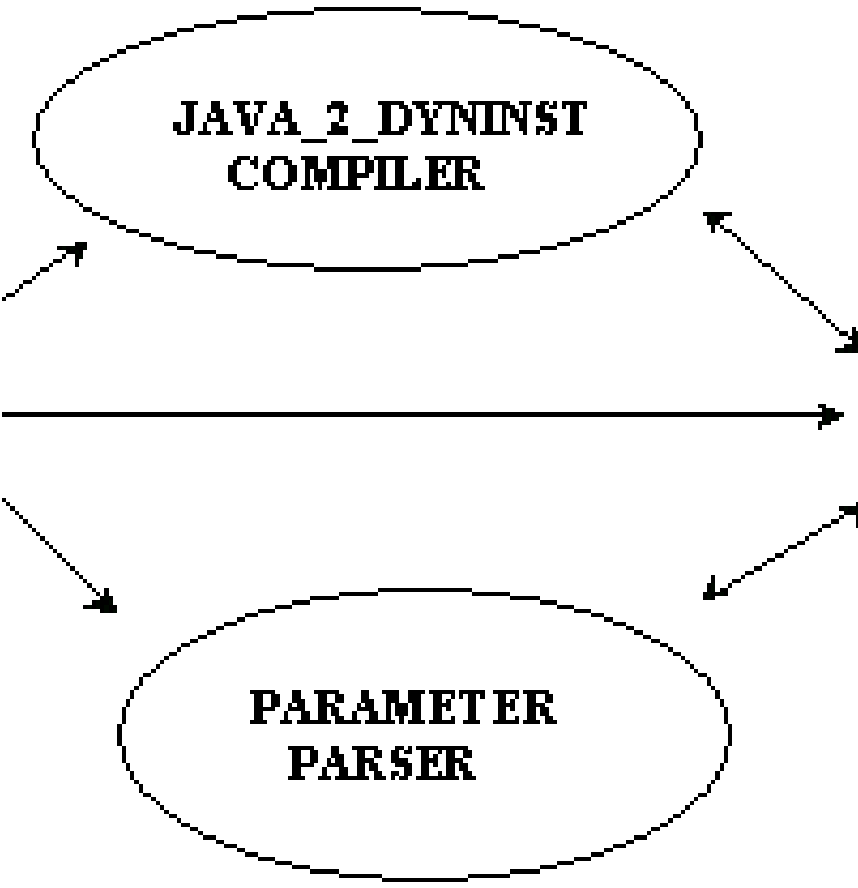
o match_macrocode match_macrocode {statementcode};
statementcode.push_back {statementcode} {statementcode};
o match_statementcode {statementcode} {statementcode};
o match_codegen {statementcode} {statementcode}; //c-statement

```

```
in the mutatee.  
_fill_in  
void_fill_in'.  
_1_fill_in  
ways_1_fill_in'.  
  
1998 Adobe Systems Incorporated.  
  
o read  
or information on  
window managers.
```

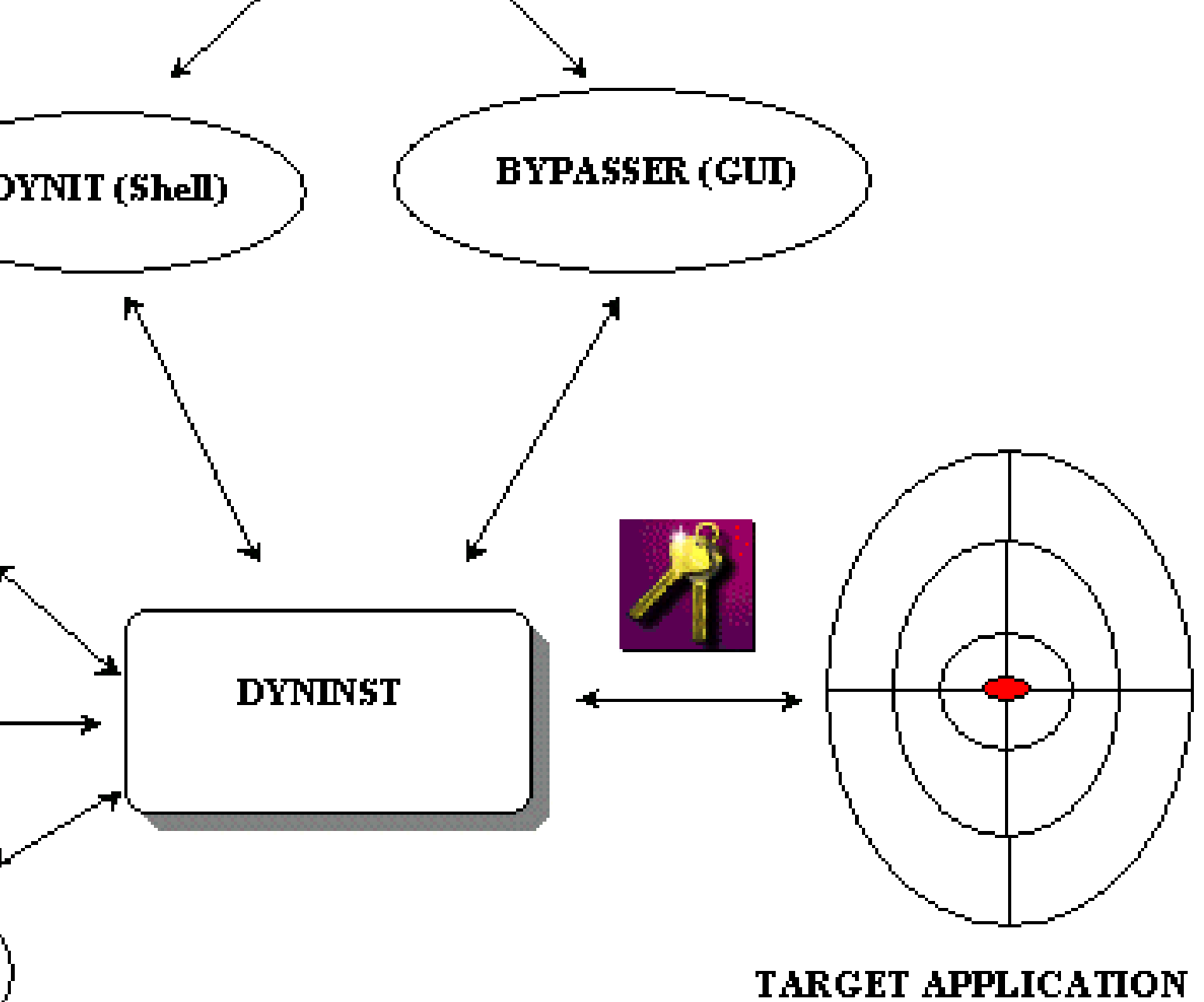


PROGRAMMER



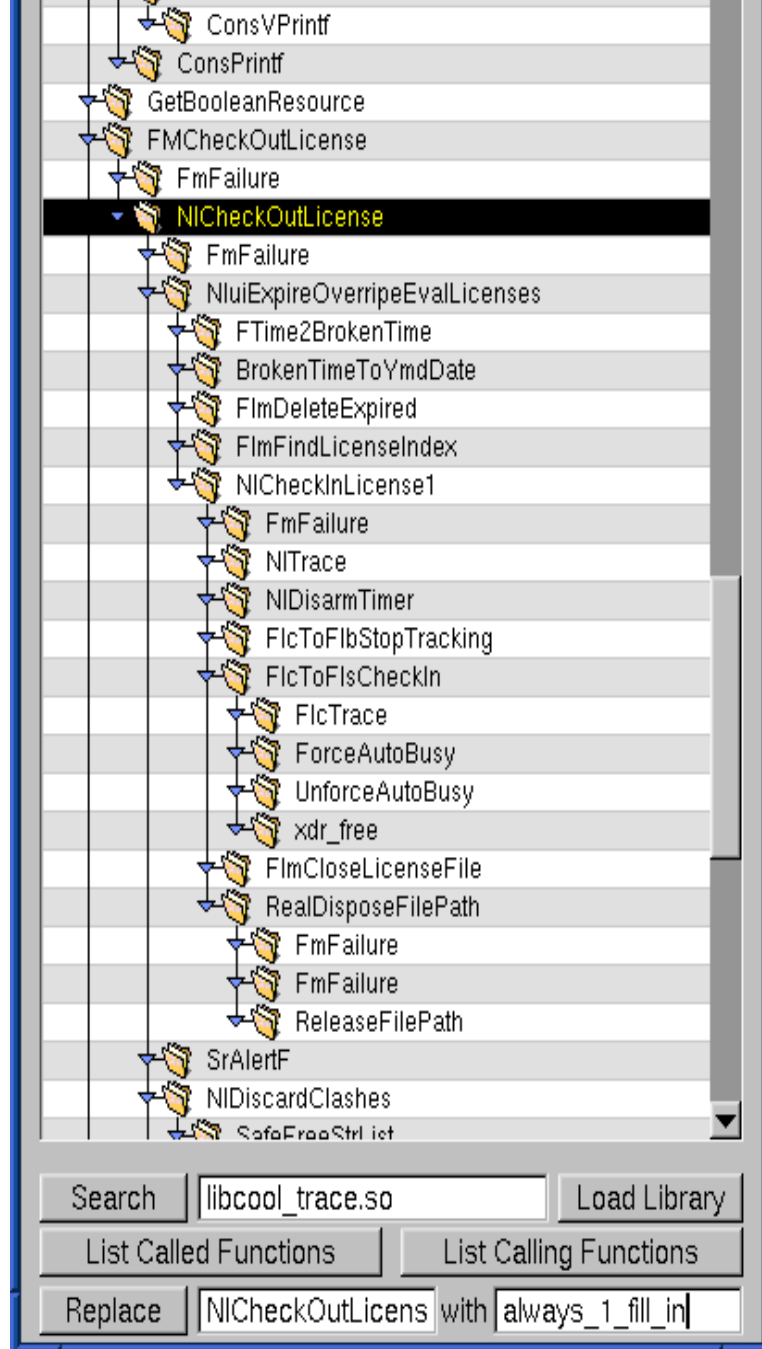
DYNIT





Note: portions of this poster were designed using P





using *FrameMaker* without a valid license.

