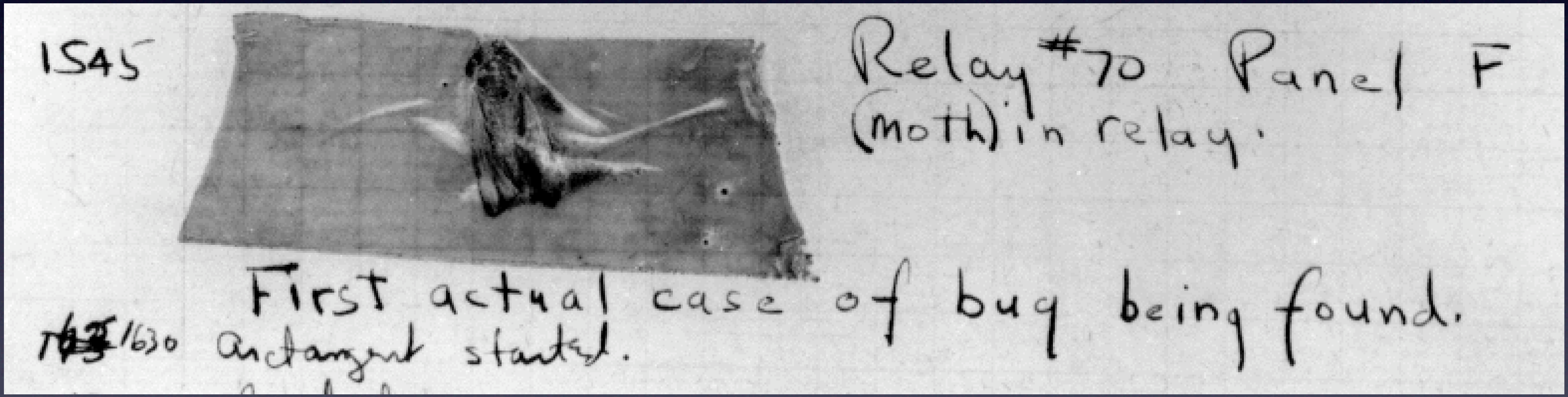
Defect Detection

Thomas Zimmermann

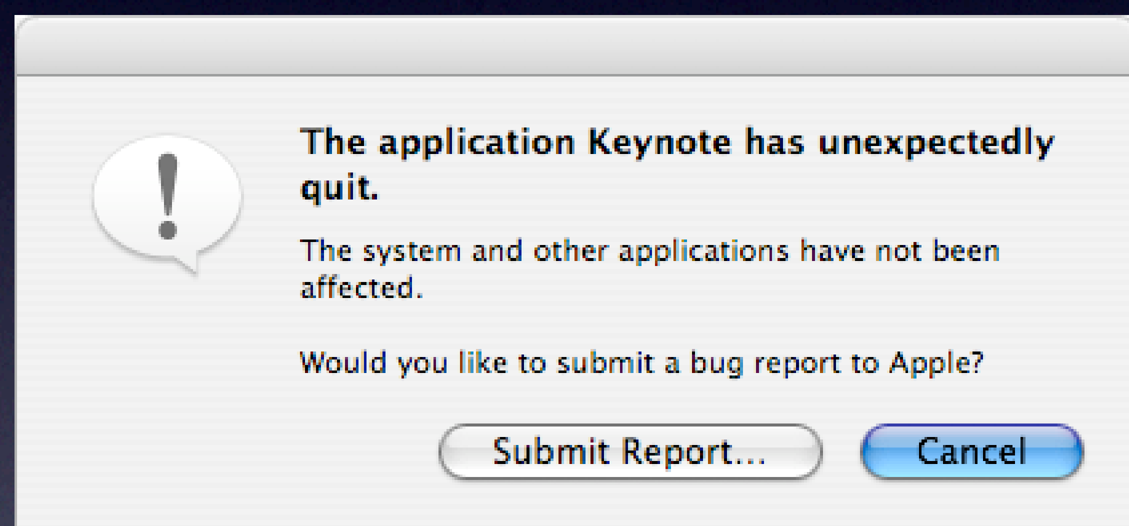
The First Bug

September 9, 1947

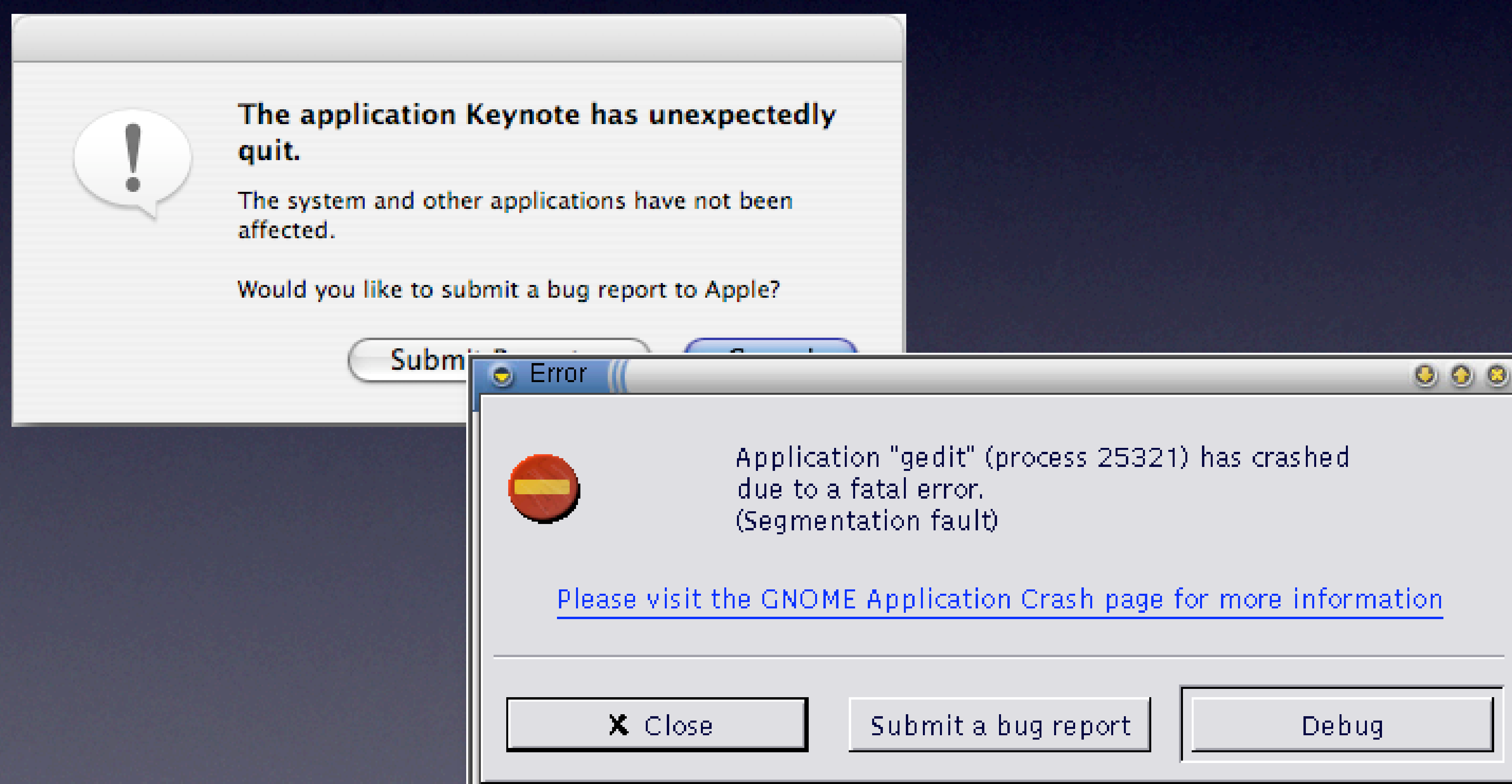


More Bugs

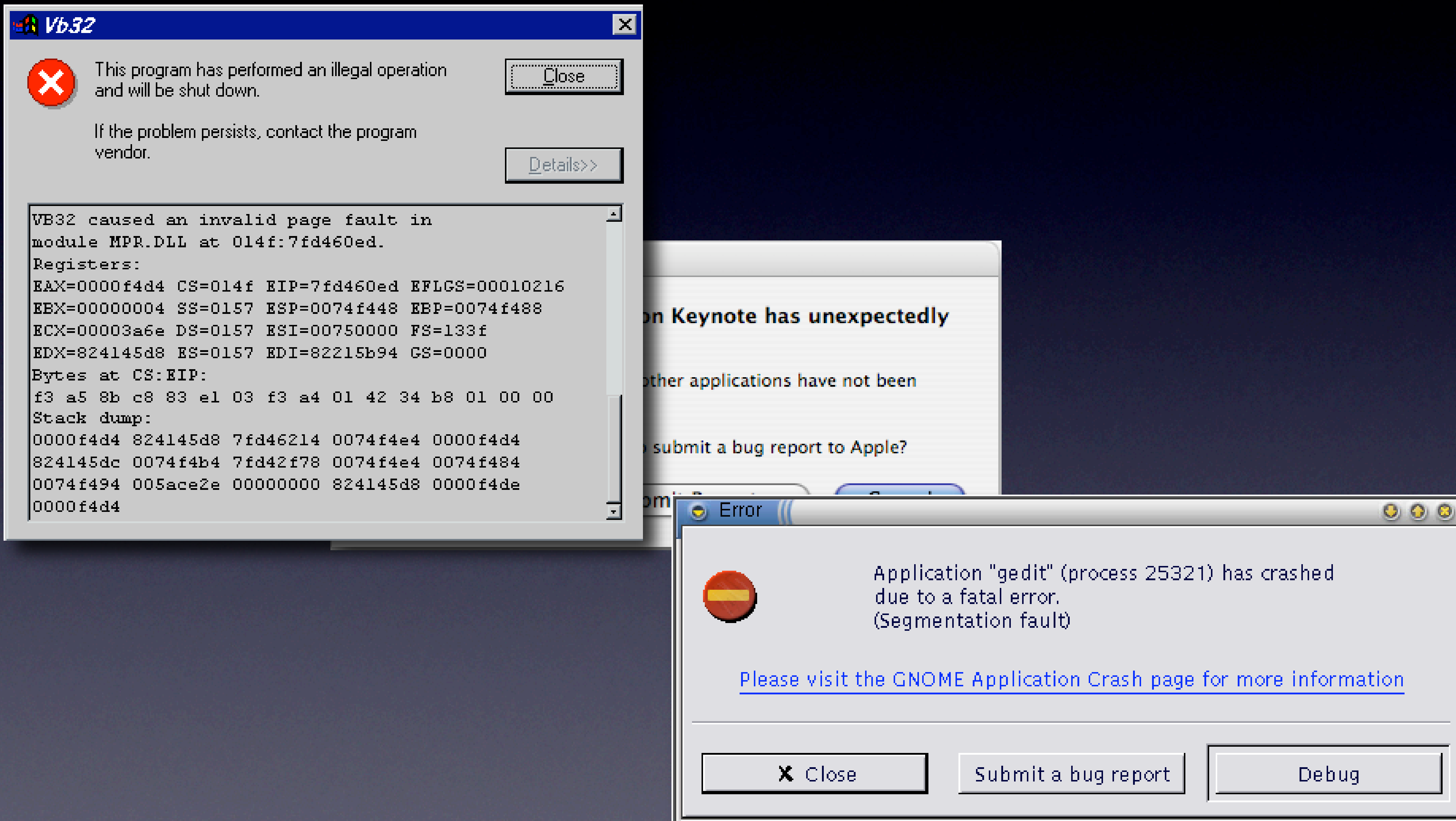
More Bugs


The application Keynote has unexpectedly quit.
The system and other applications have not been affected.
Would you like to submit a bug report to Apple?
Submit Report...
Cancel

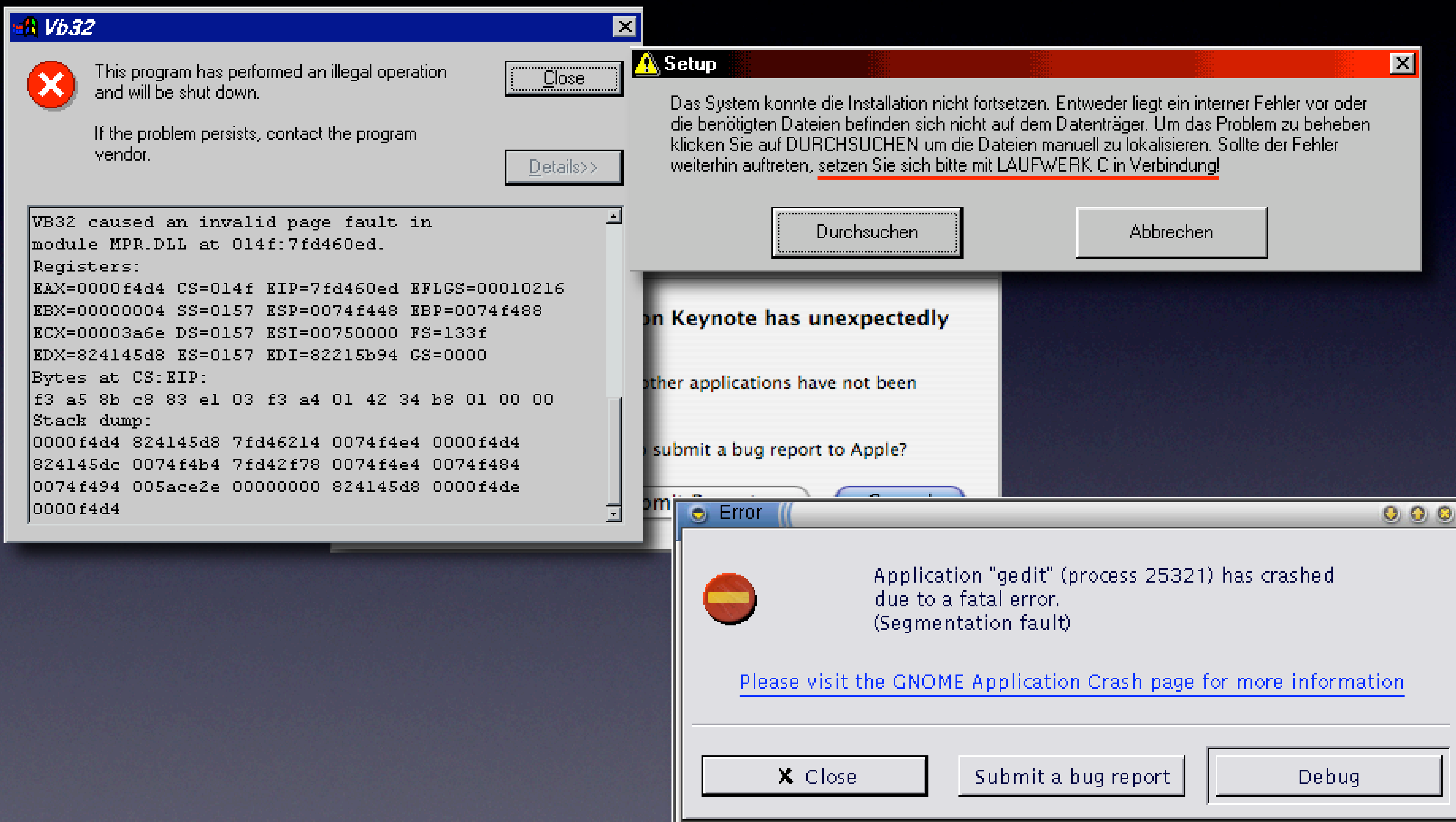
More Bugs


The application Keynote has unexpectedly quit.
The system and other applications have not been affected.
Would you like to submit a bug report to Apple?
Error
Application "gedit" (process 25321) has crashed due to a fatal error.
(Segmentation fault)
Please visit the GNOME Application Crash page for more information
Close
Submit a bug report
Debug

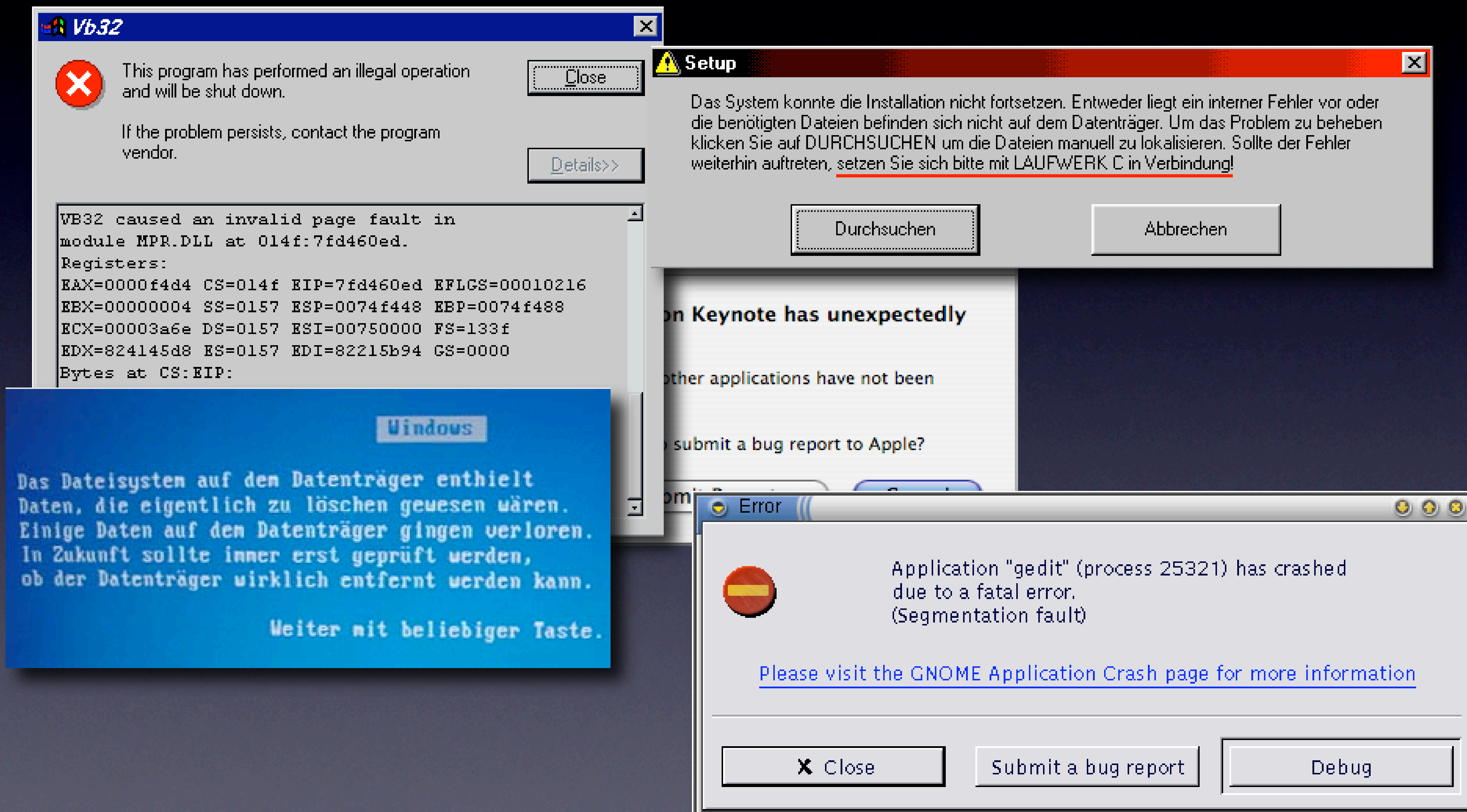
More Bugs


Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in
module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed EFLGS=00010216
EBX=00000004 SS=0157 ESP=0074f448 EBP=0074f488
ECX=00003a6e DS=0157 ESI=00750000 FS=133f
EDX=824145d8 ES=0157 EDI=82215b94 GS=0000
Bytes at CS:EIP:
f3 a5 8b c8 83 e1 03 f3 a4 01 42 34 b8 01 00 00
Stack dump:
0000f4d4 824145d8 7fd46214 0074f4e4 0000f4d4
824145dc 0074f4b4 7fd42f78 0074f4e4 0074f484
0074f494 005ace2e 00000000 824145d8 0000f4de
0000f4d4
Keynote has unexpectedly
applications have not been
submit a bug report to Apple?
Error
Application "gedit" (process 25321) has crashed
due to a fatal error.
(Segmentation fault)
Please visit the GNOME Application Crash page for more information
Close
Submit a bug report
Debug

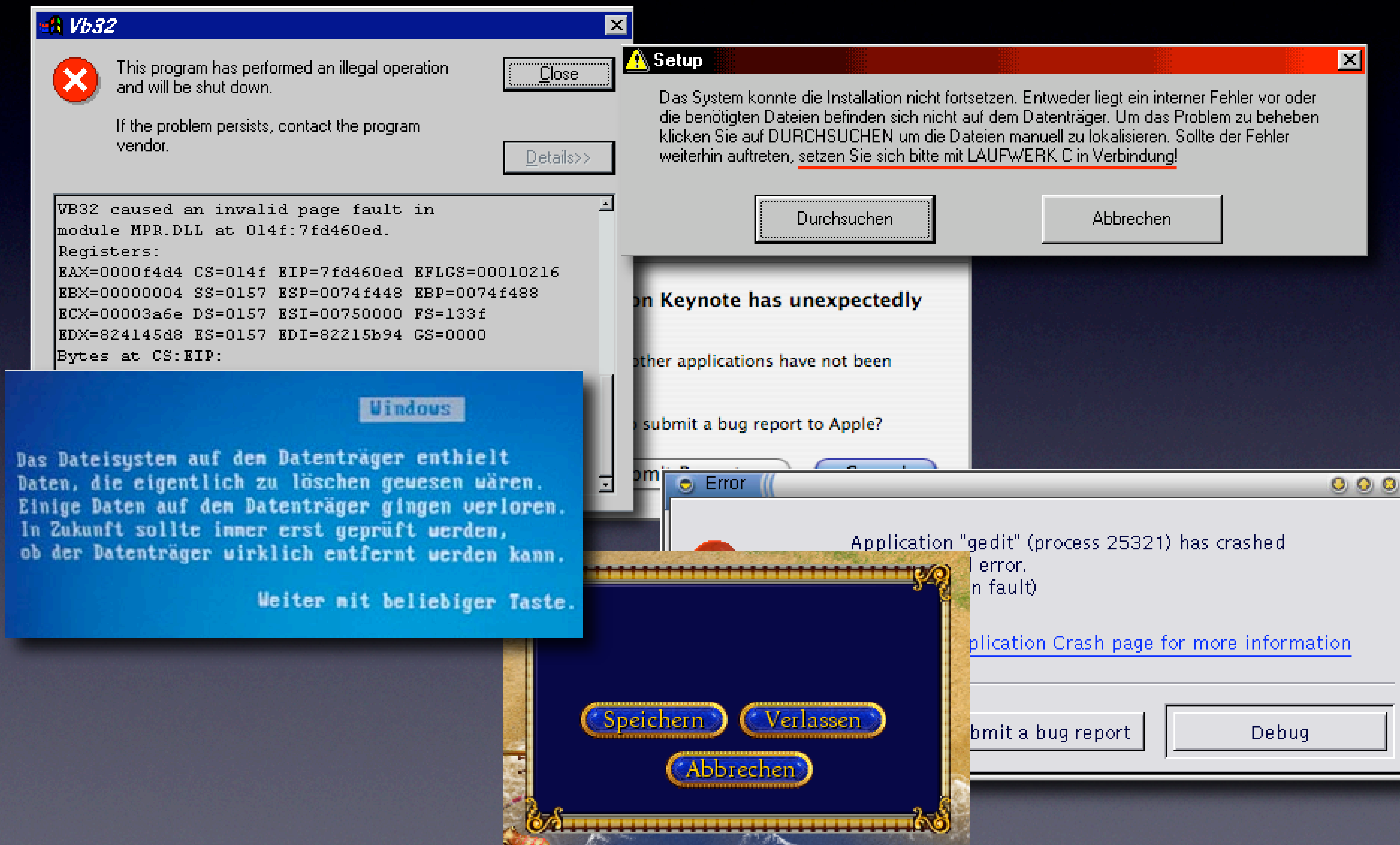
More Bugs


Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in
module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed EFLGS=00010216
EBX=00000004 SS=0157 ESP=0074f448 EBP=0074f488
ECX=00003a6e DS=0157 ESI=00750000 FS=133f
EDX=824145d8 ES=0157 EDI=82215b94 GS=0000
Bytes at CS:EIP:
f3 a5 8b c8 83 e1 03 f3 a4 01 42 34 b8 01 00 00
Stack dump:
0000f4d4 824145d8 7fd46214 0074f4e4 0000f4d4
824145dc 0074f4b4 7fd42f78 0074f4e4 0074f484
0074f494 005ace2e 00000000 824145d8 0000f4de
0000f4d4
Setup
Das System konnte die Installation nicht fortsetzen. Entweder liegt ein interner Fehler vor oder die benötigten Dateien befinden sich nicht auf dem Datenträger. Um das Problem zu beheben klicken Sie auf DURCHSUCHEN um die Dateien manuell zu lokalisieren. Sollte der Fehler weiterhin auftreten, setzen Sie sich bitte mit LAUFWERK C in Verbindung!
Durchsuchen
Abbrechen
n Keynote has unexpectedly
ther applications have not been
submit a bug report to Apple?
Error
Application "gedit" (process 25321) has crashed due to a fatal error. (Segmentation fault)
Please visit the GNOME Application Crash page for more information
Close
Submit a bug report
Debug

More Bugs

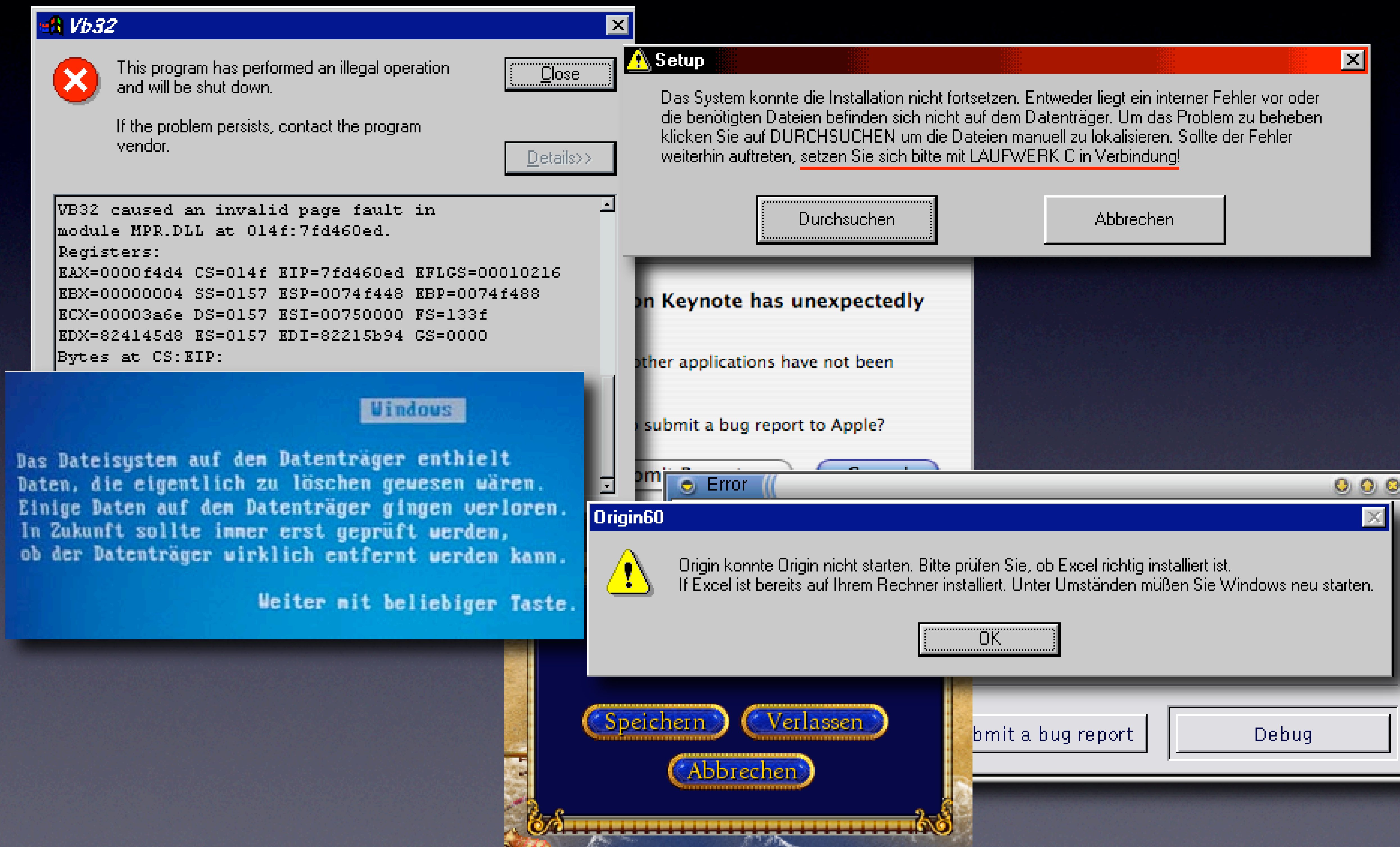

Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in
module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed EFLGS=00010216
EBX=00000004 SS=0157 ESP=0074f448 EBP=0074f488
ECX=00003a6e DS=0157 ESI=00750000 FS=133f
EDX=824145d8 ES=0157 EDI=82215b94 GS=0000
Bytes at CS:EIP:
Setup
Das System konnte die Installation nicht fortsetzen. Entweder liegt ein interner Fehler vor oder die benötigten Dateien befinden sich nicht auf dem Datenträger. Um das Problem zu beheben klicken Sie auf DURCHSUCHEN um die Dateien manuell zu lokalisieren. Sollte der Fehler weiterhin auftreten, setzen Sie sich bitte mit LAUFWERK C in Verbindung!
Durchsuchen
Abbrechen
n Keynote has unexpectedly
ther applications have not been
submit a bug report to Apple?
Windows
Das Dateisystem auf dem Datenträger enthielt
Daten, die eigentlich zu löschen gewesen wären.
Einige Daten auf dem Datenträger gingen verloren.
In Zukunft sollte immer erst geprüft werden,
ob der Datenträger wirklich entfernt werden kann.
Weiter mit beliebiger Taste.
Error
Application "gedit" (process 25321) has crashed due to a fatal error.
(Segmentation fault)
Please visit the GNOME Application Crash page for more information
Close
Submit a bug report
Debug

More Bugs

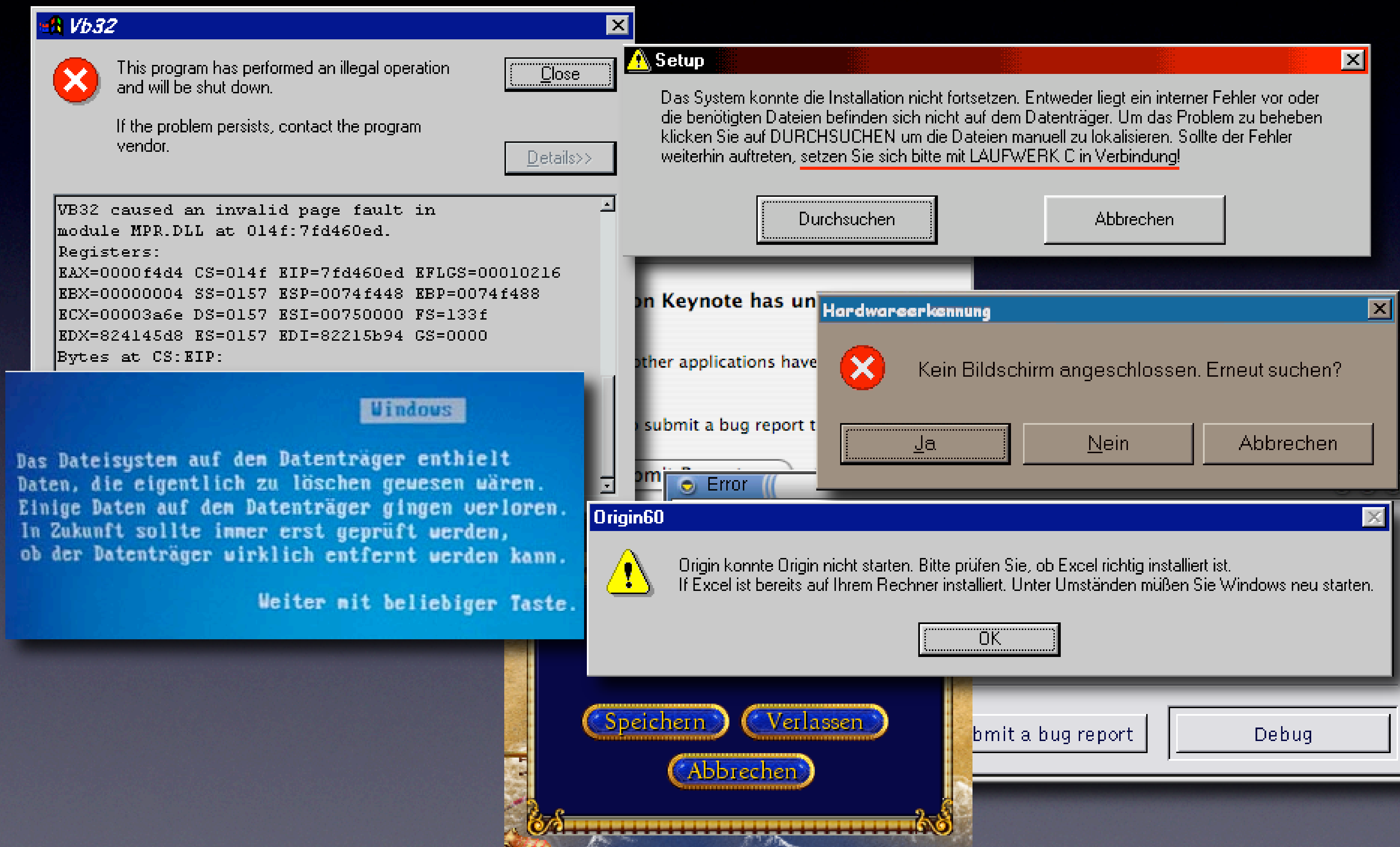


Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in
module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed EFLGS=00010216
EBX=00000004 SS=0157 ESP=0074f448 EBP=0074f488
ECX=00003a6e DS=0157 ESI=00750000 FS=133f
EDX=824145d8 ES=0157 EDI=82215b94 GS=0000
Bytes at CS:EIP:
Setup
Das System konnte die Installation nicht fortsetzen. Entweder liegt ein interner Fehler vor oder die benötigten Dateien befinden sich nicht auf dem Datenträger. Um das Problem zu beheben klicken Sie auf DURCHSUCHEN um die Dateien manuell zu lokalisieren. Sollte der Fehler weiterhin auftreten, setzen Sie sich bitte mit LAUFWERK C in Verbindung!
Durchsuchen
Abbrechen
n Keynote has unexpectedly
other applications have not been
submit a bug report to Apple?
Windows
Das Dateisystem auf dem Datenträger enthielt Daten, die eigentlich zu löschen gewesen wären. Einige Daten auf dem Datenträger gingen verloren. In Zukunft sollte immer erst geprüft werden, ob der Datenträger wirklich entfernt werden kann.
Weiter mit beliebiger Taste.
Error
Application "gedit" (process 25321) has crashed
error.
n fault)
plication Crash page for more information
bmit a bug report
Debug
Speichern
Verlassen
Abbrechen

More Bugs

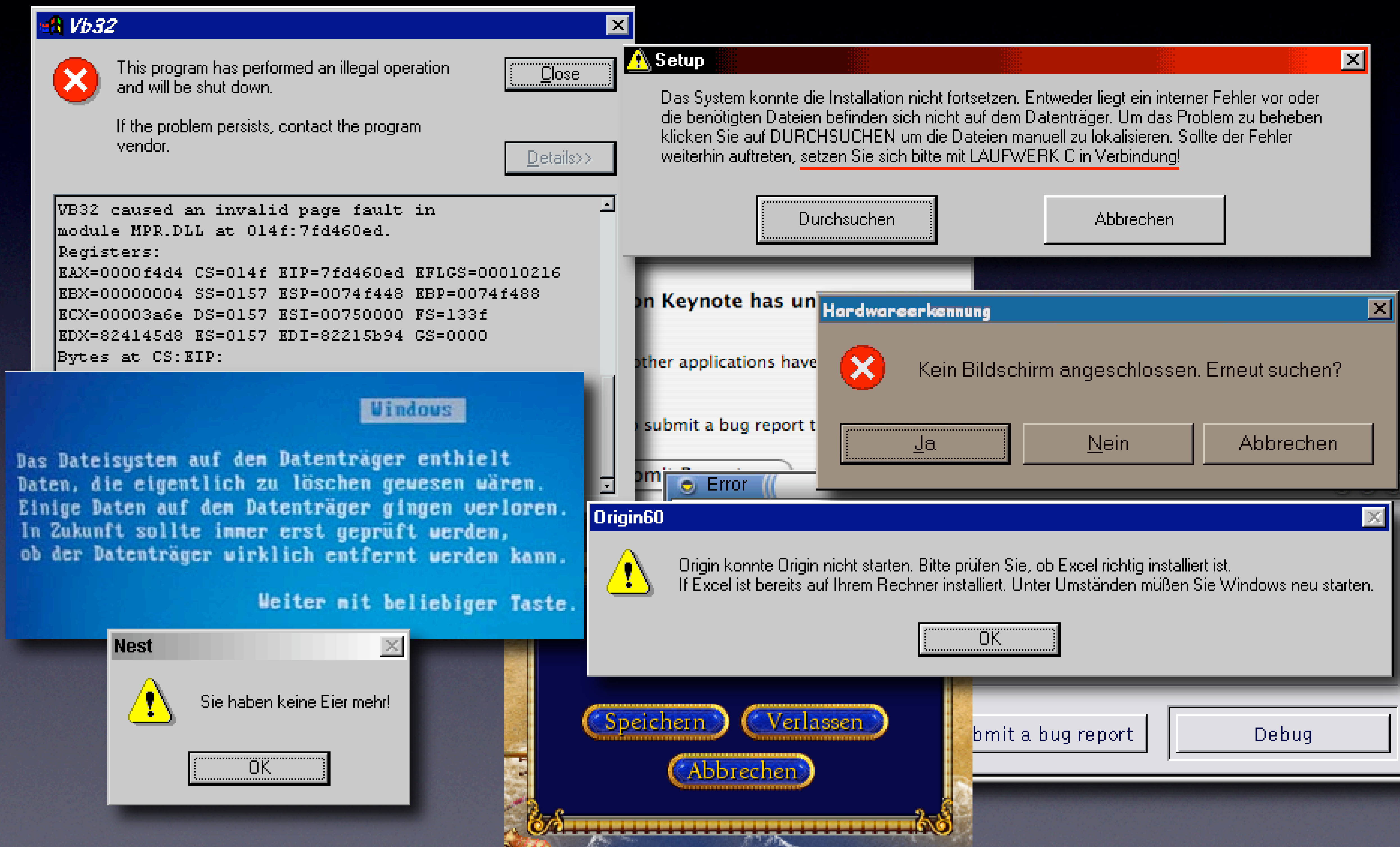

Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in
module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed EFLGS=00010216
EBX=00000004 SS=0157 ESP=0074f448 EBP=0074f488
ECX=00003a6e DS=0157 ESI=00750000 FS=133f
EDX=824145d8 ES=0157 EDI=82215b94 GS=0000
Bytes at CS:EIP:
Setup
Das System konnte die Installation nicht fortsetzen. Entweder liegt ein interner Fehler vor oder die benötigten Dateien befinden sich nicht auf dem Datenträger. Um das Problem zu beheben klicken Sie auf DURCHSUCHEN um die Dateien manuell zu lokalisieren. Sollte der Fehler weiterhin auftreten, setzen Sie sich bitte mit LAUFWERK C in Verbindung!
Durchsuchen
Abbrechen
on Keynote has unexpectedly
other applications have not been
submit a bug report to Apple?
Windows
Das Dateisystem auf dem Datenträger enthielt Daten, die eigentlich zu löschen gewesen wären. Einige Daten auf dem Datenträger gingen verloren. In Zukunft sollte immer erst geprüft werden, ob der Datenträger wirklich entfernt werden kann.
Weiter mit beliebiger Taste.
Error
Origin60
Origin konnte Origin nicht starten. Bitte prüfen Sie, ob Excel richtig installiert ist.
If Excel ist bereits auf Ihrem Rechner installiert. Unter Umständen müßen Sie Windows neu starten.
OK
Speichern
Verlassen
Abbrechen
bmit a bug report
Debug

More Bugs

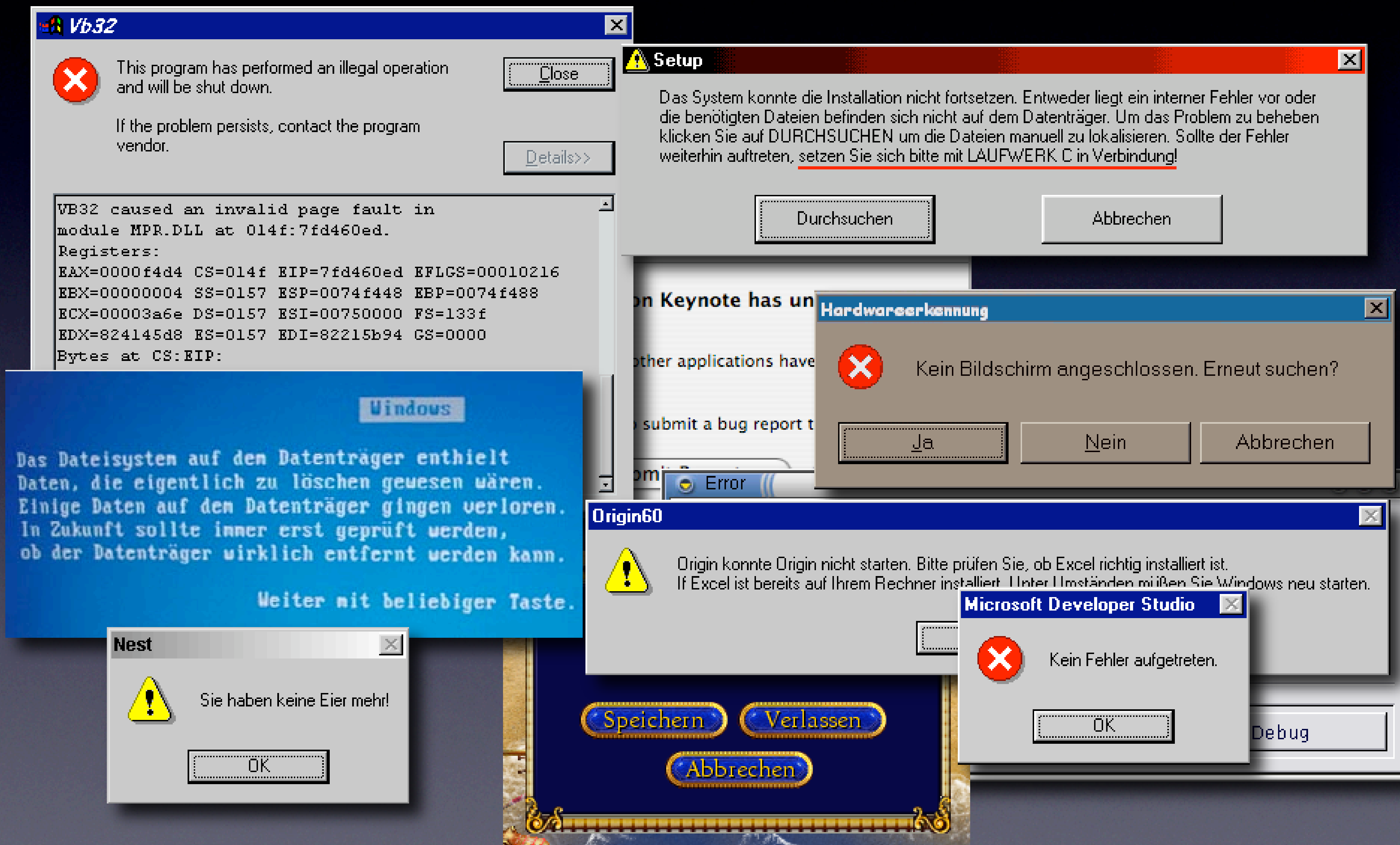


Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in
module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed EFLGS=00010216
EBX=00000004 SS=0157 ESP=0074f448 EBP=0074f488
ECX=00003a6e DS=0157 ESI=00750000 FS=133f
EDX=824145d8 ES=0157 EDI=82215b94 GS=0000
Bytes at CS:EIP:
Setup
Das System konnte die Installation nicht fortsetzen. Entweder liegt ein interner Fehler vor oder die benötigten Dateien befinden sich nicht auf dem Datenträger. Um das Problem zu beheben klicken Sie auf DURCHSUCHEN um die Dateien manuell zu lokalisieren. Sollte der Fehler weiterhin auftreten, setzen Sie sich bitte mit LAUFWERK C in Verbindung!
Durchsuchen
Abbrechen
Hardwareerkennung
Kein Bildschirm angeschlossen. Erneut suchen?
Ja
Nein
Abbrechen
Windows
Das Dateisystem auf dem Datenträger enthielt
Daten, die eigentlich zu löschen gewesen wären.
Einige Daten auf dem Datenträger gingen verloren.
In Zukunft sollte immer erst geprüft werden,
ob der Datenträger wirklich entfernt werden kann.
Weiter mit beliebiger Taste.
Error
Origin60
Origin konnte Origin nicht starten. Bitte prüfen Sie, ob Excel richtig installiert ist.
If Excel ist bereits auf Ihrem Rechner installiert. Unter Umständen müßen Sie Windows neu starten.
OK
Speichern
Verlassen
Abbrechen
Debug

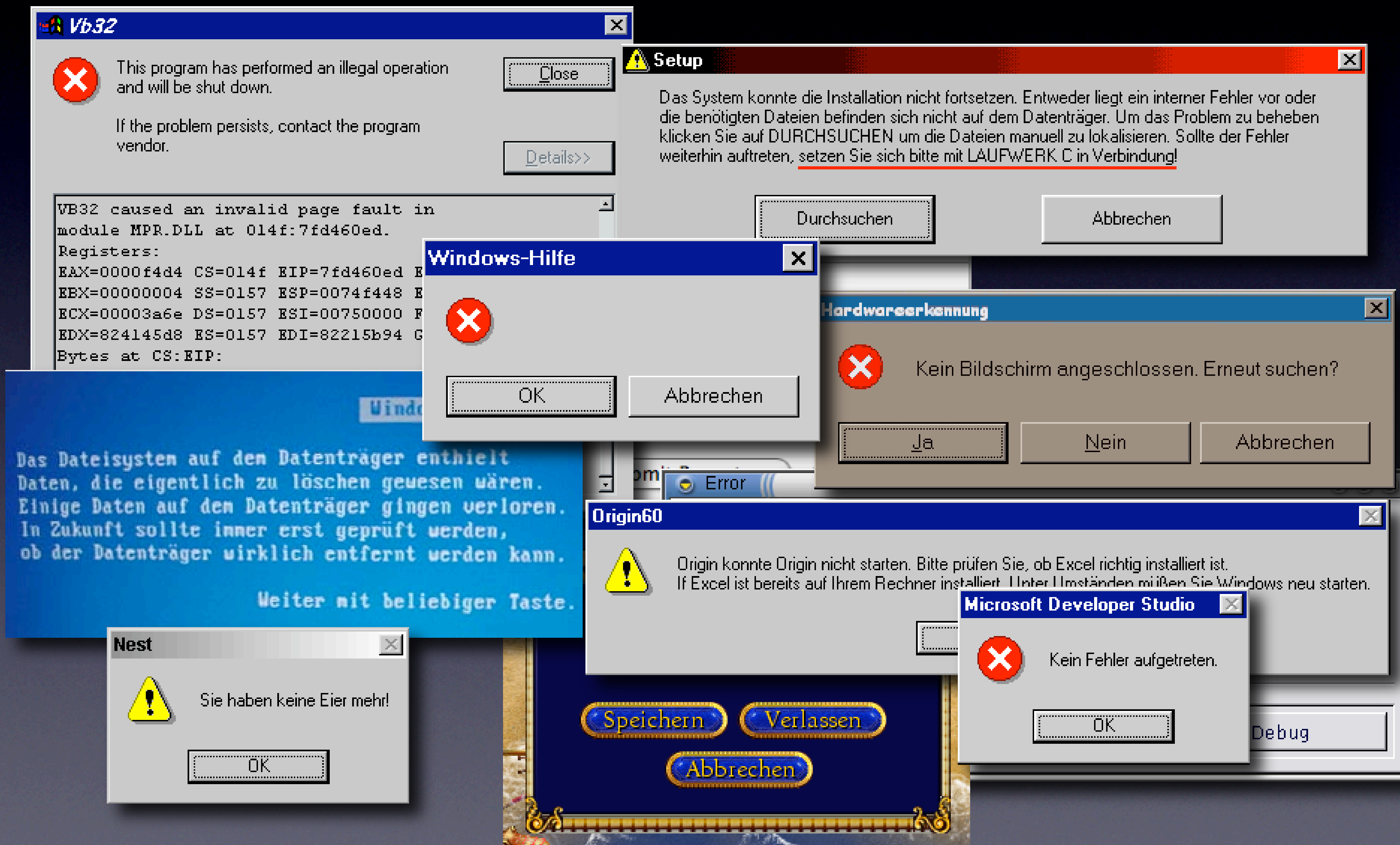
More Bugs


Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed EFLGS=00010216
EBX=00000004 SS=0157 ESP=0074f448 EBP=0074f488
ECX=00003a6e DS=0157 ESI=00750000 FS=133f
EDX=824145d8 ES=0157 EDI=82215b94 GS=0000
Bytes at CS:EIP:
Setup
Das System konnte die Installation nicht fortsetzen. Entweder liegt ein interner Fehler vor oder die benötigten Dateien befinden sich nicht auf dem Datenträger. Um das Problem zu beheben klicken Sie auf DURCHSUCHEN um die Dateien manuell zu lokalisieren. Sollte der Fehler weiterhin auftreten, setzen Sie sich bitte mit LAUFWERK C in Verbindung!
Durchsuchen
Abbrechen
Hardwareerkennung
Kein Bildschirm angeschlossen. Erneut suchen?
Ja
Nein
Abbrechen
Windows
Das Dateisystem auf dem Datenträger enthielt Daten, die eigentlich zu löschen gewesen wären. Einige Daten auf dem Datenträger gingen verloren. In Zukunft sollte immer erst geprüft werden, ob der Datenträger wirklich entfernt werden kann.
Weiter mit beliebiger Taste.
Error
Origin60
Origin konnte Origin nicht starten. Bitte prüfen Sie, ob Excel richtig installiert ist.
If Excel ist bereits auf Ihrem Rechner installiert. Unter Umständen müßen Sie Windows neu starten.
OK
Nest
Sie haben keine Eier mehr!
OK
Speichern
Verlassen
Abbrechen
bmit a bug report
Debug

More Bugs


Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed EFLGS=00010216
EBX=00000004 SS=0157 ESP=0074f448 EBP=0074f488
ECX=00003a6e DS=0157 ESI=00750000 FS=133f
EDX=824145d8 ES=0157 EDI=82215b94 GS=0000
Bytes at CS:EIP:
Setup
Das System konnte die Installation nicht fortsetzen. Entweder liegt ein interner Fehler vor oder die benötigten Dateien befinden sich nicht auf dem Datenträger. Um das Problem zu beheben klicken Sie auf DURCHSUCHEN um die Dateien manuell zu lokalisieren. Sollte der Fehler weiterhin auftreten, setzen Sie sich bitte mit LAUFWERK C in Verbindung!
Durchsuchen
Abbrechen
Hardwareerkennung
Kein Bildschirm angeschlossen. Erneut suchen?
Ja
Nein
Abbrechen
Windows
Das Dateisystem auf dem Datenträger enthielt Daten, die eigentlich zu löschen gewesen wären. Einige Daten auf dem Datenträger gingen verloren. In Zukunft sollte immer erst geprüft werden, ob der Datenträger wirklich entfernt werden kann.
Weiter mit beliebiger Taste.
Error
Origin60
Origin konnte Origin nicht starten. Bitte prüfen Sie, ob Excel richtig installiert ist.
Microsoft Developer Studio
Kein Fehler aufgetreten.
OK
Debug
Nest
Sie haben keine Eier mehr!
OK
Speichern
Verlassen
Abbrechen

More Bugs



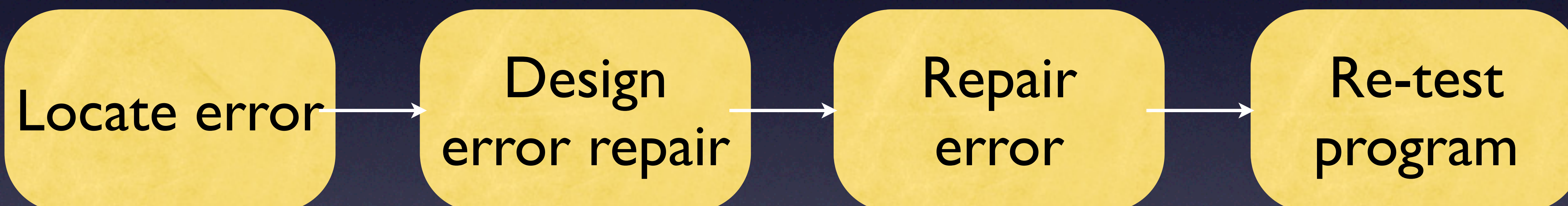
Vb32
This program has performed an illegal operation and will be shut down.
If the problem persists, contact the program vendor.
Close
Details>>
VB32 caused an invalid page fault in module MPR.DLL at 014f:7fd460ed.
Registers:
EAX=0000f4d4 CS=014f EIP=7fd460ed
EBX=00000004 SS=0157 ESP=0074f448
ECX=00003a6e DS=0157 ESI=00750000
EDX=824145d8 ES=0157 EDI=82215b94
Bytes at CS:EIP:
Setup
Das System konnte die Installation nicht fortsetzen. Entweder liegt ein interner Fehler vor oder die benötigten Dateien befinden sich nicht auf dem Datenträger. Um das Problem zu beheben klicken Sie auf DURCHSUCHEN um die Dateien manuell zu lokalisieren. Sollte der Fehler weiterhin auftreten, setzen Sie sich bitte mit LAUFWERK C in Verbindung!
Durchsuchen
Abbrechen
Windows-Hilfe
OK
Abbrechen
Hardwareerkennung
Kein Bildschirm angeschlossen. Erneut suchen?
Ja
Nein
Abbrechen
Das Dateisystem auf dem Datenträger enthielt Daten, die eigentlich zu löschen gewesen wären. Einige Daten auf dem Datenträger gingen verloren. In Zukunft sollte immer erst geprüft werden, ob der Datenträger wirklich entfernt werden kann.
Weiter mit beliebiger Taste.
Error
Origin60
Origin konnte Origin nicht starten. Bitte prüfen Sie, ob Excel richtig installiert ist.
Microsoft Developer Studio
Kein Fehler aufgetreten.
OK
Debug
Nest
Sie haben keine Eier mehr!
OK
Speichern
Verlassen
Abbrechen

Facts on Debugging

- Software bugs are costing ~60 bln US$/yr
- Improvements could reduce cost by 30%
- Validation (including debugging) can easily take up to 50-75% of the development time
- When debugging, some people are three times as efficient than others

How to Debug

(Sommerville 2004)



The Traffic Principle

The Traffic Principle

T
R
A
F
F
I
C

The Traffic Principle

T rack the problem

R

A

F

F

I

C

The Traffic Principle

T rack the problem

R eproduce

A

F

F

I

C

The Traffic Principle

T rack the problem
R eproduce
A utomate
F
F
I
C

The Traffic Principle

T rack the problem

R eproduce

A utomate

F ind Origins

F

I

C

The Traffic Principle

T rack the problem
R eproduce
A utomate
F ind Origins
F ocus
I
C

The Traffic Principle

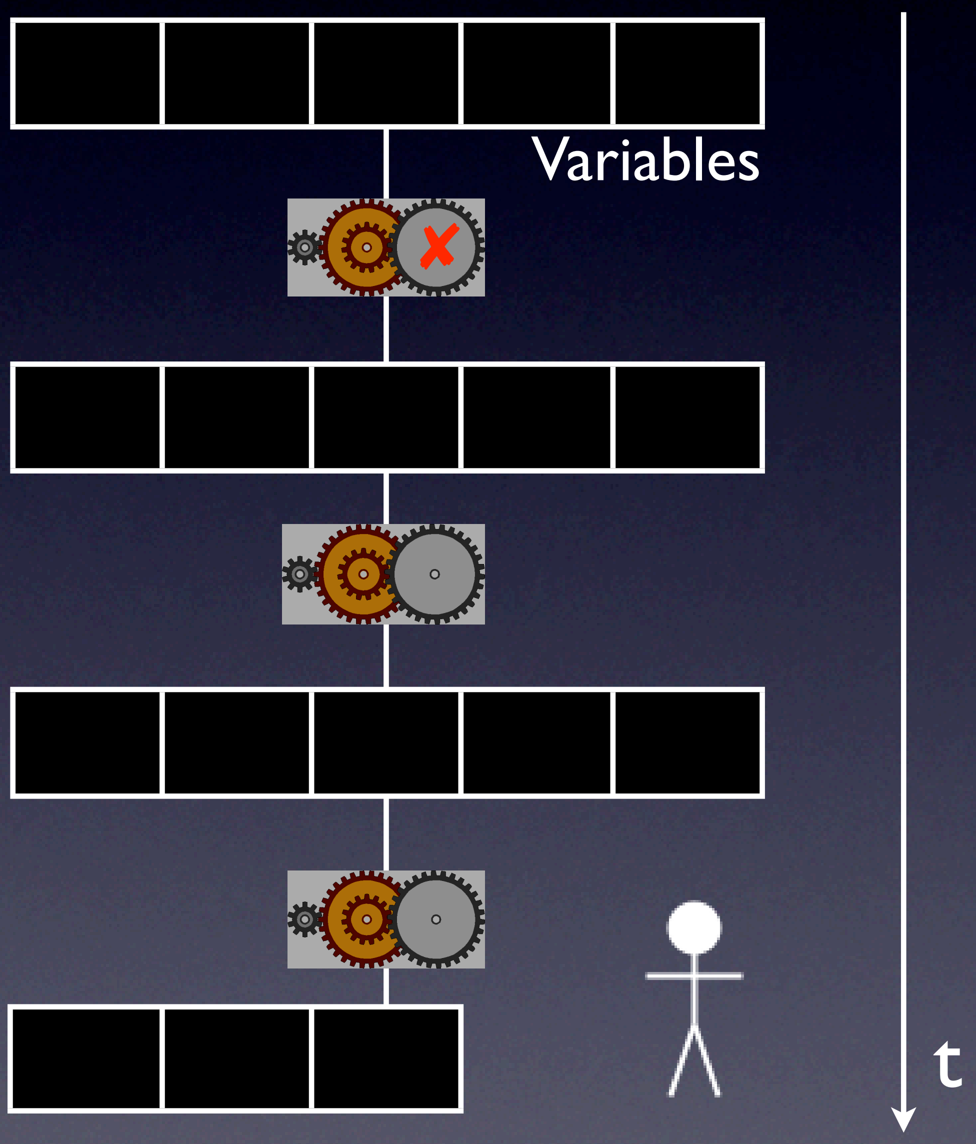
T rack the problem
R eproduce
A utomate
F ind Origins
F ocus
I solate
C

The Traffic Principle

- **T** rack the problem
- **R** eproduce
- **A** utomate
- **F** ind Origins
- **F** ocus
- **I** solate
- **C** orrect

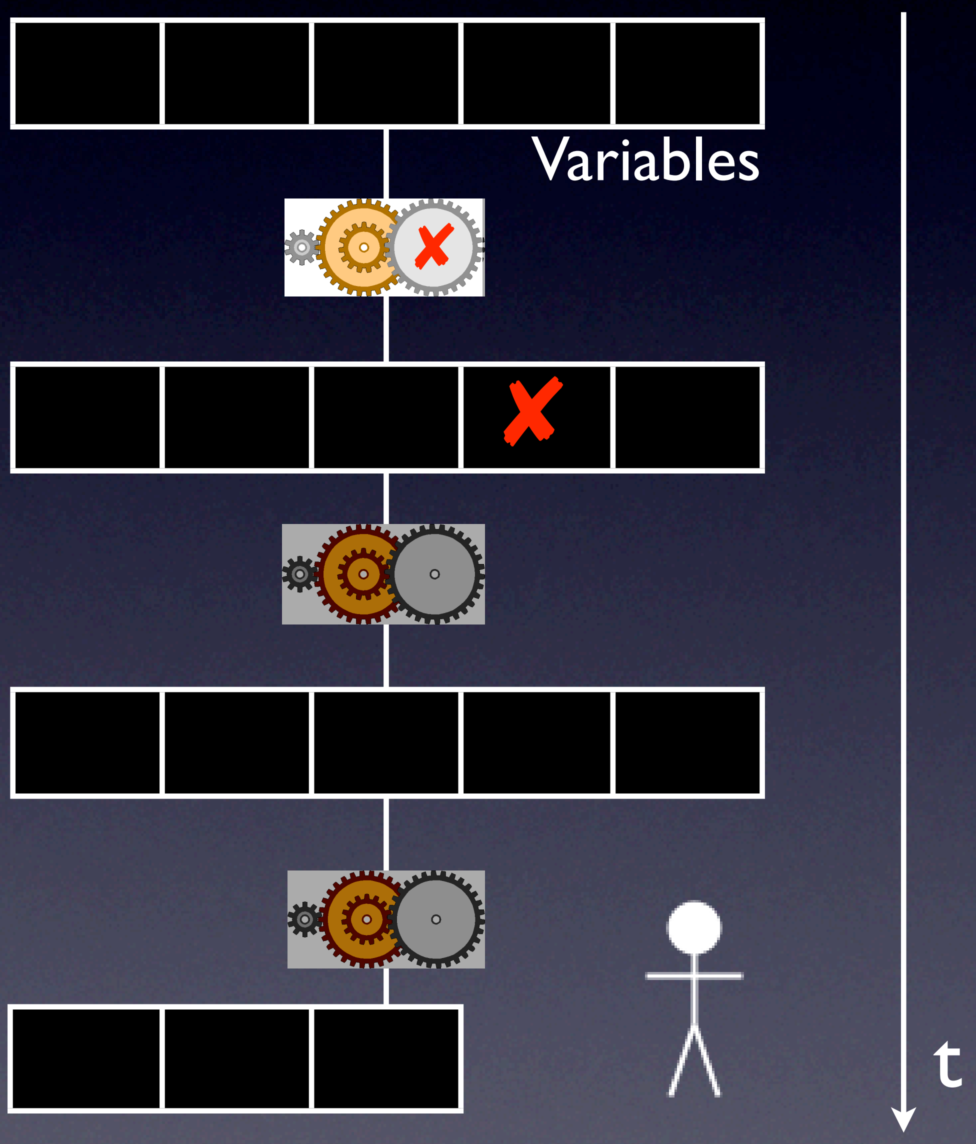
From Defect to Failure

1. The programmer creates a *defect* – an error in the code.
2. When executed, the defect creates an *infection* – an error in the state.
3. The infection *propagates*.
4. The infection causes a *failure*.



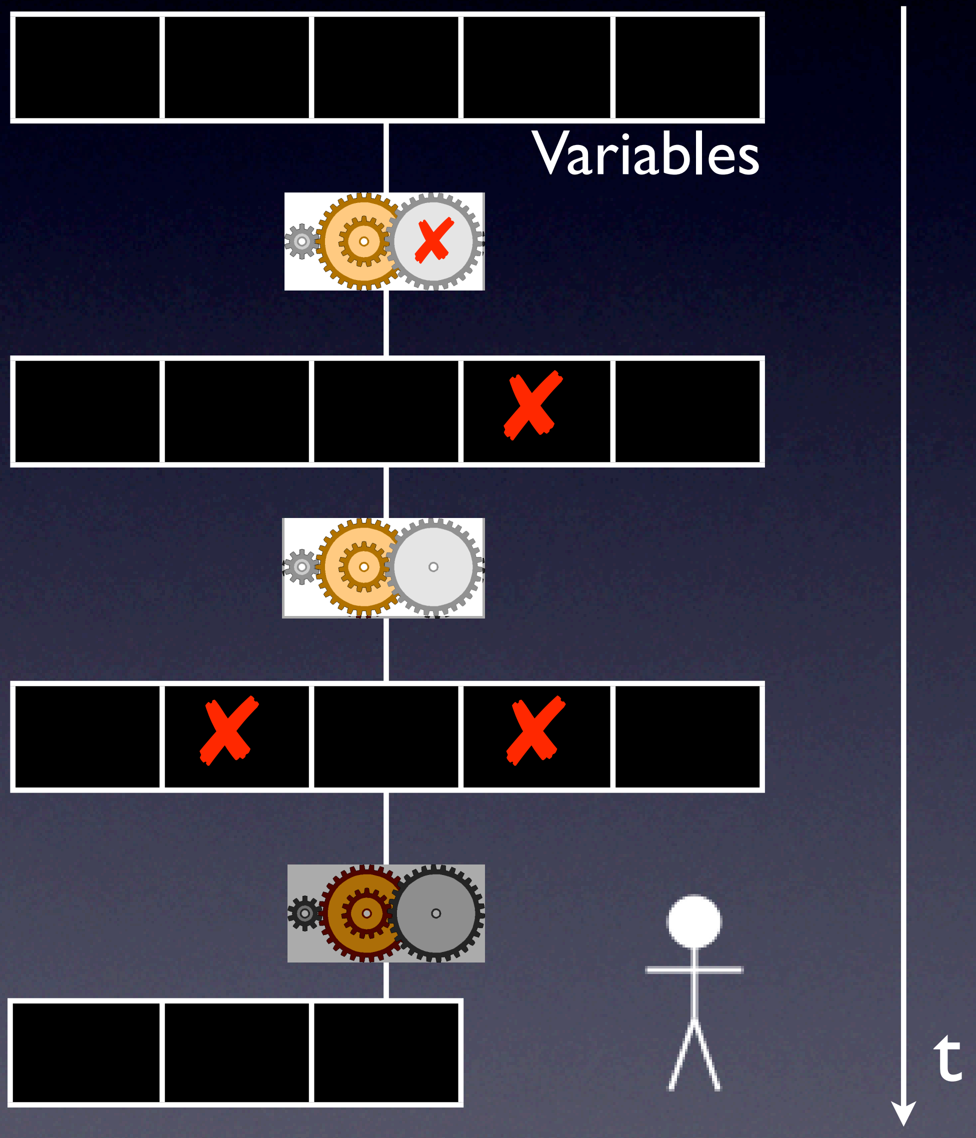
From Defect to Failure

1. The programmer creates a *defect* – an error in the code.
2. When executed, the defect creates an *infection* – an error in the state.
3. The infection *propagates*.
4. The infection causes a *failure*.



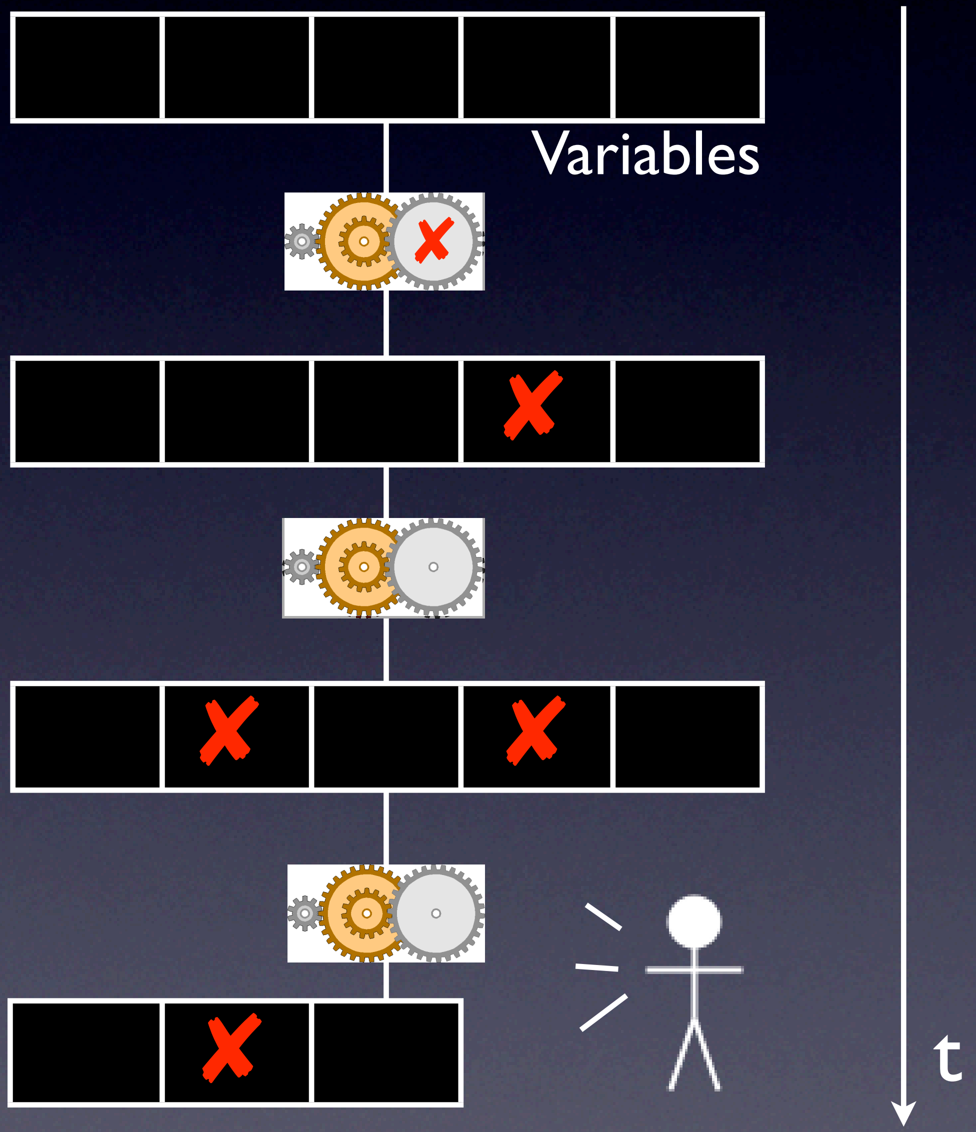
From Defect to Failure

1. The programmer creates a *defect* – an error in the code.
2. When executed, the defect creates an *infection* – an error in the state.
3. The infection *propagates*.
4. The infection causes a *failure*.



From Defect to Failure

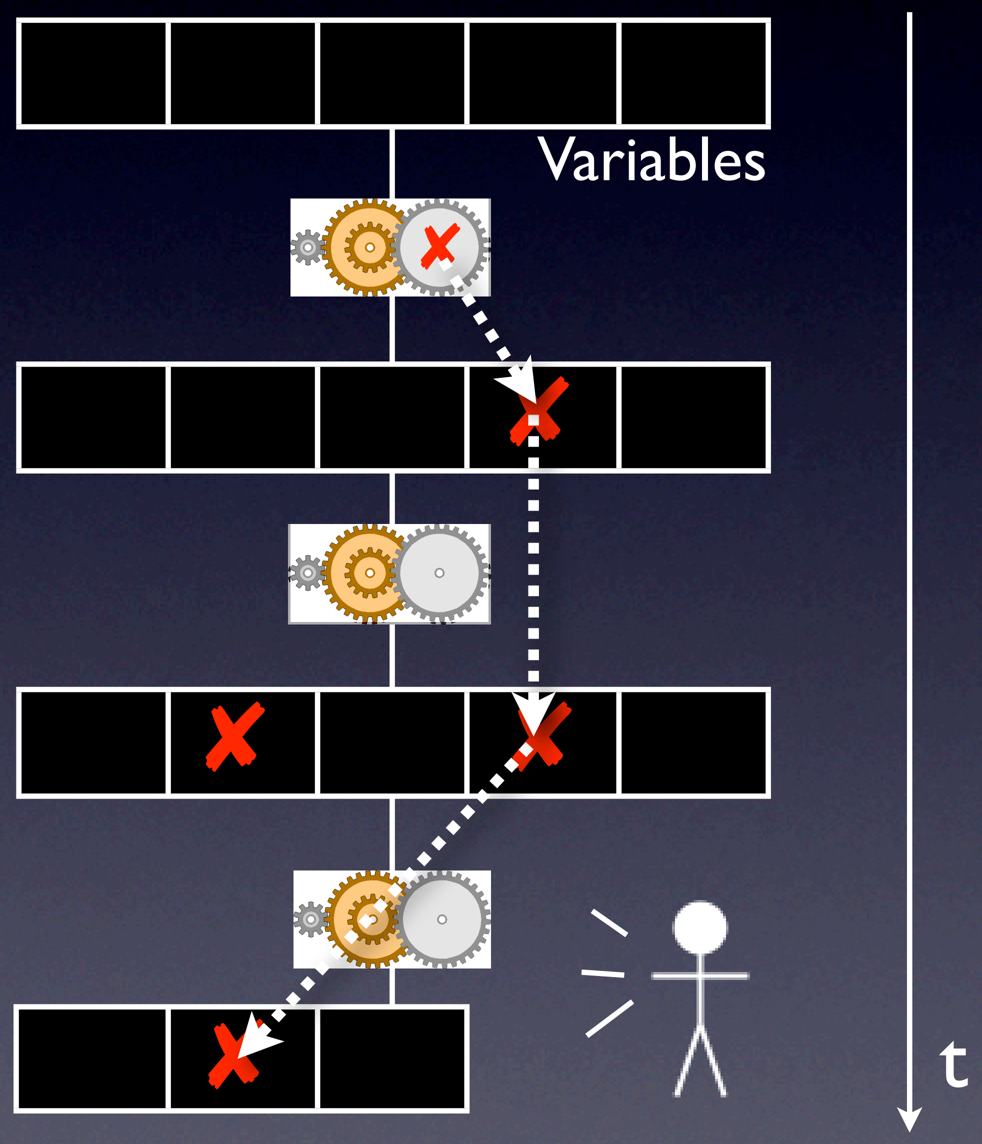
1. The programmer creates a *defect* – an error in the code.
2. When executed, the defect creates an *infection* – an error in the state.
3. The infection *propagates*.
4. The infection causes a *failure*.



From Defect to Failure

1. The programmer creates a *defect* – an error in the code.
2. When executed, the defect creates an *infection* – an error in the state.
3. The infection *propagates*.
4. The infection causes a *failure*.

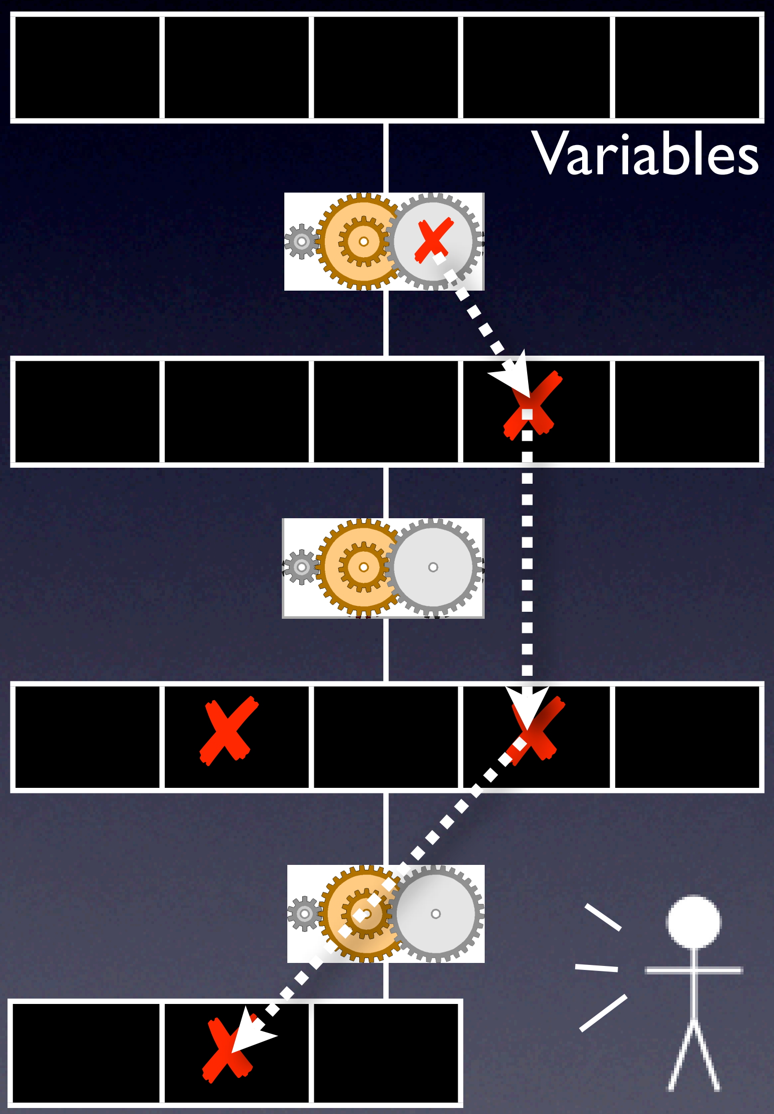
This infection chain must be traced back – and broken.



The Curse of Testing

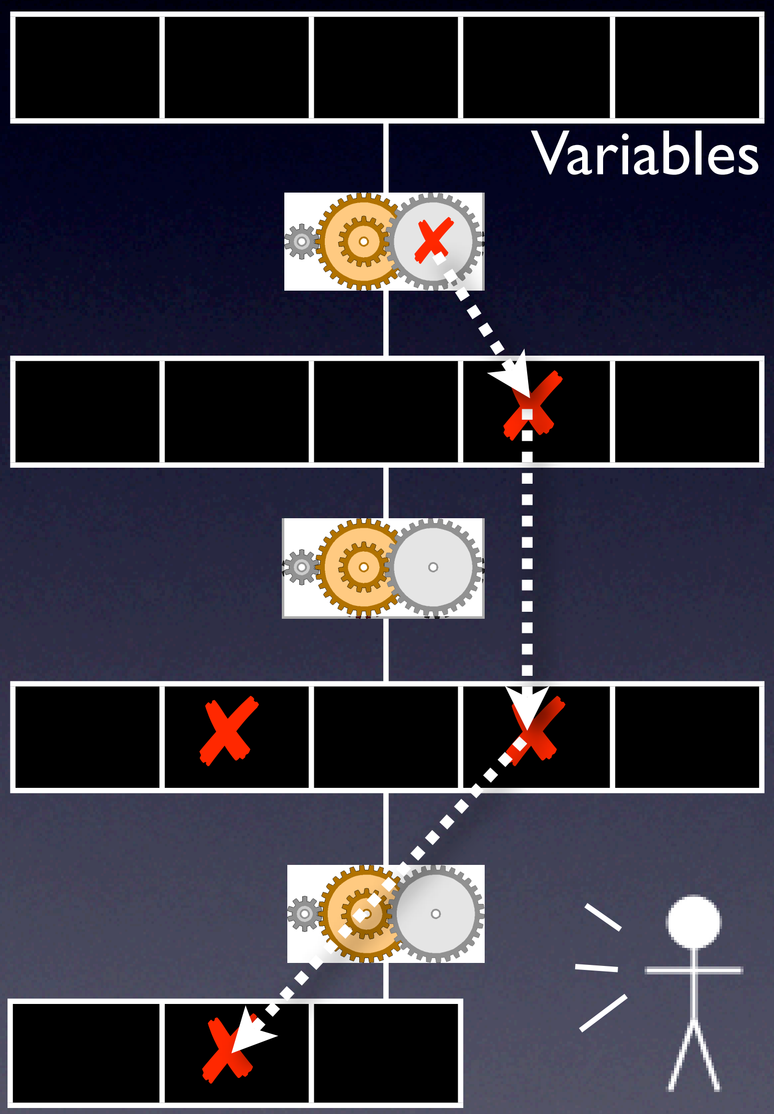
- Not every defect causes a failure!
- *Testing can only show the presence of errors – not their absence.*

  (Dijkstra 1972)

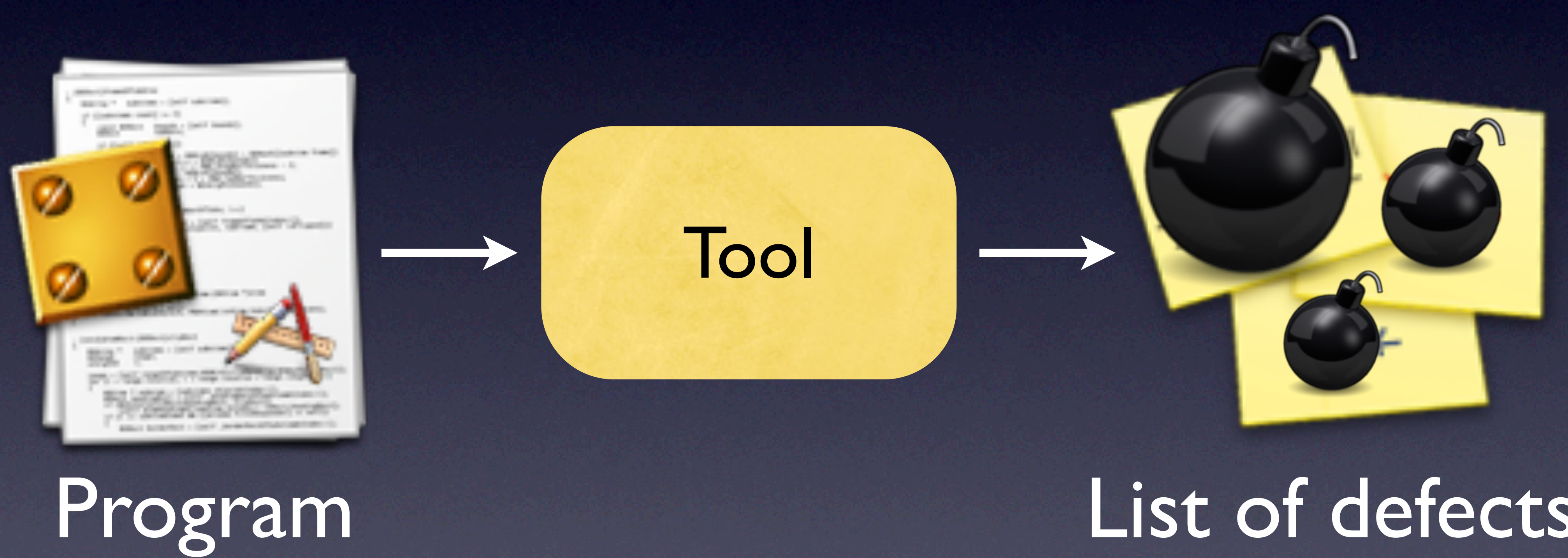


Debugging

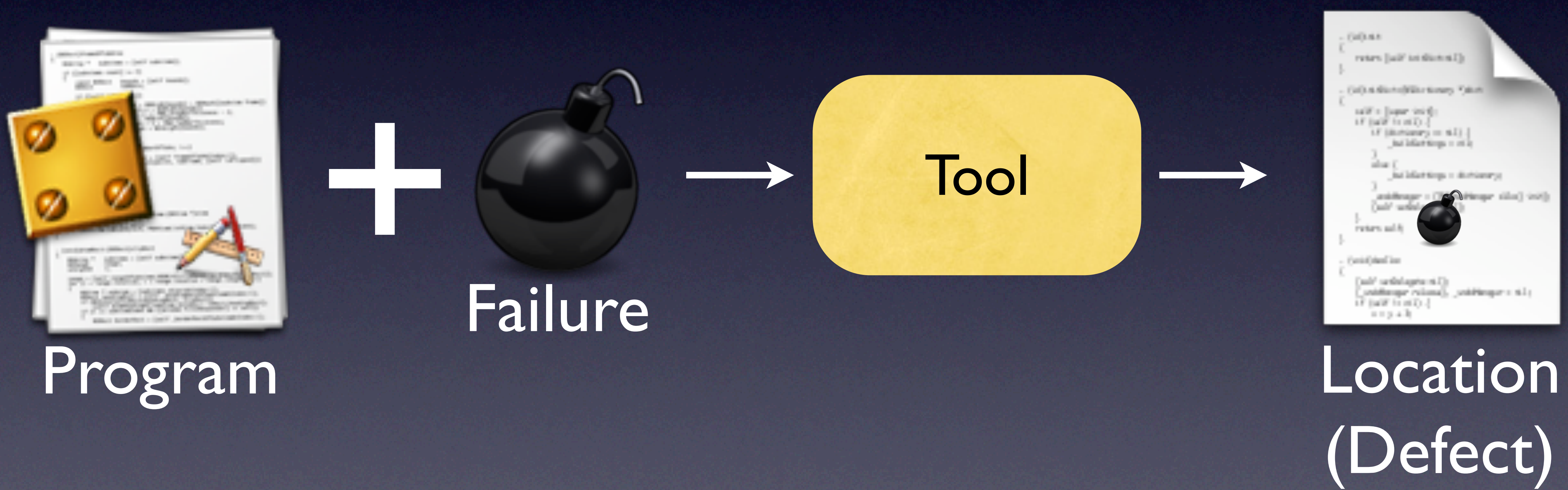
- Every *failure* can be traced back to some *infection*, and every *infection* is caused by some *defect*.
- *Debugging* means to *relate a given failure to the defect* – and to remove the defect.



Defect detection



Defect localization



Outline

Redundancies (Engler et al.)	FindBugs (Pugh et al.)
Models (Invited talk: A. Wasylkowski)	Statistical (Liblit et al.)

Dawson Engler

Co-founder of Coverity

redundancies
flag errors

Idempotent operations

Flag idempotent operations.

- variable is assigned to itself: x=x
- variable is divided by itself: x/x
- variable is bitwise or'd with itself: x|x
- variable is bitwise and'd with itself: x&x

Idempotent operations

/* 2.4.1/net/appletalk/aarp.c:aarp_rcv */

```
...
else { /* We need to make a copy of the entry. */
  da.s_node = sa.s_node;
  da.s_net = da.s_net;
  ...
```

System	Bugs	Minor	False
Linux	7	6	3

Redundant assignments

Flag cases where a value assigned to a variable is subsequently not used.

System	Bugs	False	Uninspected
Linux	129	26	1840
xgcc	13	1	0

Redundant assignments

/* 2.4.1/net/decnet/af_decnet.c:dn_wait_run */

```
do {
  ...
  if (signal_pending(current)) {
     err = -ERESTARTSYS;
     break;
  }
  SOCK_SLEEP_PRE(sk)
  if (scp->state != DN_RUN)
       schedule();
  SOCK_SLEEP_POST(sk)
} while(scp->state != DN_RUN);
return 0;
```

Redundant assignments

/* 2.4.1/net/decnet/af_decnet.c:dn_wait_run */

```
do {
  ...
  if (signal_pending(current)) {
     err = -ERESTARTSYS; /* BUG: lost value */
     break;
  }
  SOCK_SLEEP_PRE(sk)
  if (scp->state != DN_RUN)
       schedule();
  SOCK_SLEEP_POST(sk)
} while(scp->state != DN_RUN);
return 0;
```

Unintentionally discarded

Redundant assignments

/* 2.4.1/net/atm/lec.c:lec_addr_delete: */

```
for(entry=priv->lec_arp_tables[i];
    entry != NULL;
    entry=next) {
  next = entry->next;
  if (...) {
      lec_arp_remove(priv->lec_arp_tables, entry);
      kfree(entry);
  }
  lec_arp_unlock(priv);
  return 0;
}
```

Redundant assignments

/* 2.4.1/net/atm/lec.c:lec_addr_delete: */

```
for(entry=priv->lec_arp_tables[i];
    entry != NULL;
    entry=next) { /* BUG: never reached */
  next = entry->next;
  if (...) {
      lec_arp_remove(priv->lec_arp_tables, entry);
      kfree(entry);
  }
  lec_arp_unlock(priv);
  return 0;
}
```

Surprising control flow

Dead code

Flag dead code (i.e., code that is never executed).

System	Bugs	False
Linux	66	26

Dead code

/* 2.4.5-ac8/fs/ntfs/unistr.c:ntfs_collate_names */

```
for (cnt = 0; cnt < min(name1_len, name2_len); ++cnt) {
   c1 = le16_to_cpu(*name1++);
   c2 = le16_to_cpu(*name2++);
   if (ic) {
       if (c1 < upcase_len)
           c1 = le16_to_cpu(upcase[c1]);
       if (c2 < upcase_len)
           c2 = le16_to_cpu(upcase[c2]);
   }

   if (c1 < 64 && legal_ansi_char_array[c1] & 8);
       return err_val;
   if (c1 < c2)
       return -1;
   ...
```

Dead code

```
/* 2.4.5-ac8/fs/ntfs/unistr.c:ntfs_collate_names */
for (cnt = 0; cnt < min(name1_len, name2_len); ++cnt) {
   c1 = le16_to_cpu(*name1++);
   c2 = le16_to_cpu(*name2++);
   if (ic) {
       if (c1 < upcase_len)
           c1 = le16_to_cpu(upcase[c1]);
       if (c2 < upcase_len)
           c2 = le16_to_cpu(upcase[c2]);
   }
   /* [META] stray terminator! */
   if (c1 < 64 && legal_ansi_char_array[c1] & 8);
       return err_val;
   if (c1 < c2)
       return -1;
   ...
```

Redundant conditionals

Flag redundant branch conditionals from
(1) branch statements with non-constant conditionals that always evaluate to either true or false
(2) switch statements with impossible cases

System	Bugs	False	Uninspected
Linux	49	52	169

Redundant conditionals

/* 2.4.1/drivers/fc/iph5526.c:rscn_handler */

```
if ((login_state == NODE_LOGGED_IN) ||
    (login_state == NODE_PROCESS_LOGGED_IN)) {
    ...
}
else
if (login_state == NODE_LOGGED_OUT)
    tx_adisc(fi, ELS_ADISC, node_id,
             OX_ID_FIRST_SEQUENCE);
else /* BUG: redundant conditional */
if (login_state == NODE_LOGGED_OUT)
    tx_logi(fi, ELS_PLOGI, node_id);
```

Redundant conditionals

/* 2.4.1/drivers/fc/iph5526.c:rscn_handler */

```
if ((logi
    (logi
    ...
}
else
if (login
    tx_ad
          OX_ID_FIRST_SEQUENCE);
else /* B
if (login
    tx_lo
```

Overly cautious programming style (confused programmer)

Single iteration loop

Cut-and-paste errors

Correlation to hard bugs

Hard bugs can crash a system (use of freed memory, dereferences of null pointers, potential deadlocks, unreleased locks, and security violations)

A	B: True	B: False	Totals
True	o_{11}	o_{12}	$n_{1\cdot}$
False	o_{21}	o_{22}	$n_{2\cdot}$
Totals	$n_{\cdot 1}$	$n_{\cdot 2}$	$n_{\cdot\cdot}$

Chi-Square test

Null hypothesis: "A and B are mutually independent"

Correlation to hard bugs

Redundant Assignments	Hard Bugs Yes	Hard Bugs No	Totals
Yes	345	435	780
No	206	1069	1275
Totals	551	1504	2055

$T = 194.37$, p-value $= 0.00$

Correlation to hard bugs

Redundant Assignments	Hard Bugs Yes	Hard Bugs No	Totals
Yes	345	435	780
No	206	1069	1275
Totals	551	1504	2055

$T = 194.37$, p-value $= 0.00$

dependant

Correlation to hard bugs

Redundant Assignments	Hard Bugs Yes	Hard Bugs No	Totals
Yes	345	435	780
No	206	1069	1275
Totals	551	1504	2055

$T = 194.37$, p-value $= 0.00$

dependant

Redundant Conditionals	Hard Bugs Yes	Hard Bugs No	Totals
Yes	75	79	154
No	476	1425	1901
Totals	551	1504	2055

$T = 40.65$, p-value $= 0.00$

dependant

Correlation to hard bugs

Redundant Assignments	Hard Bugs Yes	Hard Bugs No	Totals
Yes	345	435	780
No	206	1069	1275
Totals	551	1504	2055

$T = 194.37$, p-value $= 0.00$

dependant

Redundant Conditionals	Hard Bugs Yes	Hard Bugs No	Totals
Yes	75	79	154
No	476	1425	1901
Totals	551	1504	2055

$T = 40.65$, p-value $= 0.00$

dependant

Dead Code	Hard Bugs Yes	Hard Bugs No	Totals
Yes	133	135	268
No	418	1369	1787
Totals	551	1504	2055

$T = 81.74$, p-value $= 0.00$

dependant

Correlation to hard bugs

Redundant Assignments	Hard Bugs Yes	Hard Bugs No	Totals
Yes	345	435	780
No	206	1069	1275
Totals	551	1504	2055

$T = 194.37$, p-value $= 0.00$

dependant

Redundant Conditionals	Hard Bugs Yes	Hard Bugs No	Totals
Yes	75	79	154
No	476	1425	1901
Totals	551	1504	2055

$T = 40.65$, p-value $= 0.00$

dependant

Dead Code	Hard Bugs Yes	Hard Bugs No	Totals
Yes	133	135	268
No	418	1369	1787
Totals	551	1504	2055

$T = 81.74$, p-value $= 0.00$

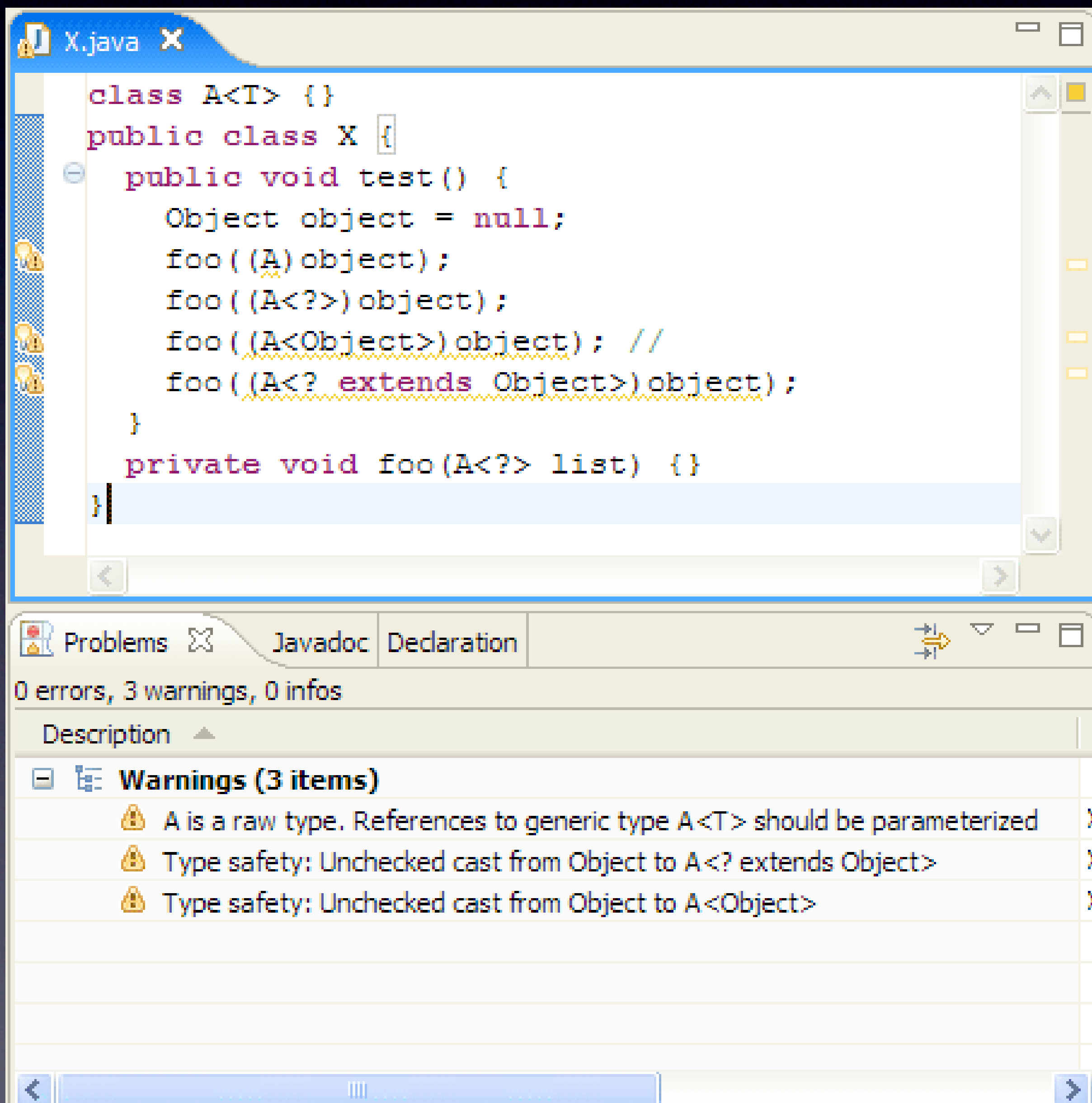
dependant

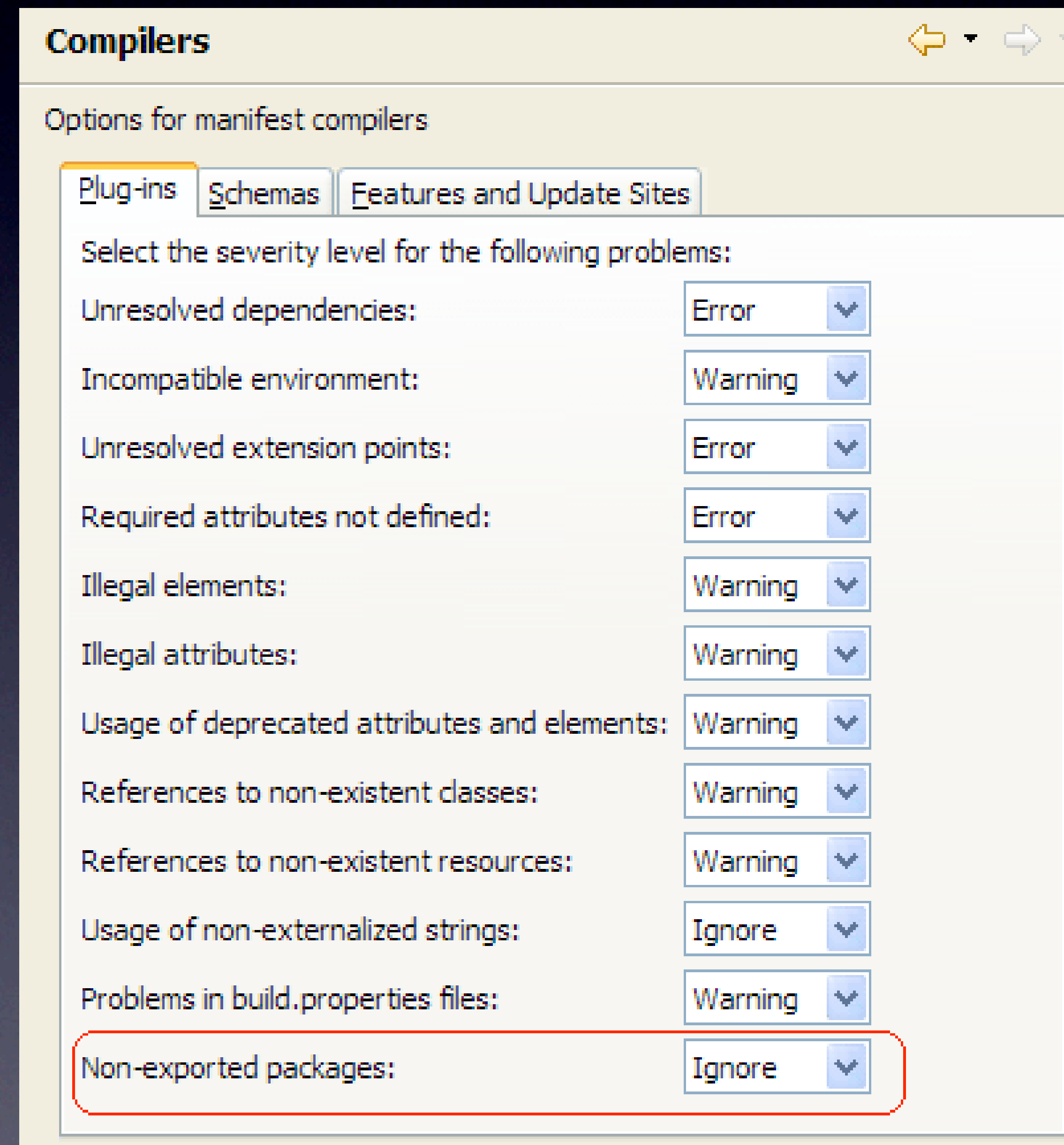
Aggregate	Hard Bugs Yes	Hard Bugs No	Totals
Yes	372	573	945
No	179	931	1110
Totals	551	1504	2055

$T = 140.48$, p-value $= 0.00$

dependant

Eclipse


X.java
class A<T> {}
public class X {
public void test() {
Object object = null;
foo((A)object);
foo((A<?>)object);
foo((A<Object>)object); //
foo((A<? extends Object>)object);
}
private void foo(A<?> list) {}
}
Problems
Javadoc
Declaration
0 errors, 3 warnings, 0 infos
Description
Warnings (3 items)
A is a raw type. References to generic type A<T> should be parameterized
Type safety: Unchecked cast from Object to A<? extends Object>
Type safety: Unchecked cast from Object to A<Object>


Compilers
Options for manifest compilers
Plug-ins
Schemas
Features and Update Sites
Select the severity level for the following problems:
Unresolved dependencies: Error
Incompatible environment: Warning
Unresolved extension points: Error
Required attributes not defined: Error
Illegal elements: Warning
Illegal attributes: Warning
Usage of deprecated attributes and elements: Warning
References to non-existent classes: Warning
References to non-existent resources: Warning
Usage of non-externalized strings: Ignore
Problems in build.properties files: Warning
Non-exported packages: Ignore

FindBugs

Bill Pugh

FindBugs: Bug patterns

FindBugs recognizes 284 different bug patterns

http://findbugs.sourceforge.net/bugDescriptions.html

AM: Creates an empty jar file entry; AM: Creates an empty zip file entry; BC: Equals method should not assume anything about the type of its argument; BC: Random object created and used only once; CN: Class implements Cloneable but does not define or use clone method; CN: clone method does not call super.clone(); Co: Abstract class defines covariant compareTo() method; Co: Covariant compareTo() method defined; DE: Method might drop exception; DE: Method might ignore exception; DP: Classloaders should only be created inside doPrivileged block; DP: Method invoked that should be only be invoked inside a doPrivileged block; Dm: Method invokes System.exit(...); Dm: Method invokes dangerous method runFinalizersOnExit; ES: Comparison of String parameter using == or !=; ES: Comparison of String objects using == or !=; Eq: Abstract class defines covariant equals() method; Eq: Class defines compareTo(...) and uses Object.equals(); Eq: Covariant equals() method defined; Eq: Covariant equals() method defined, Object.equals(Object) inherited; FI: Empty finalizer should be deleted; FI: Explicit invocation of finalizer; FI: Finalizer nulls fields; FI: Finalizer only nulls fields; FI: Finalizer does not call superclass finalizer; FI: Finalizer nullifies superclass finalizer; FI: Finalizer does nothing but call superclass finalizer; HE: Class defines equals() but not hashCode(); HE: Class defines equals() and uses Object.hashCode(); HE: Class defines hashCode() but not equals(); HE: Class defines hashCode() and uses Object.equals(); HE: Class inherits equals() and uses Object.hashCode(); IC: Superclass uses subclass during initialization; IMSE: Dubious catching of IllegalMonitorStateException; ISC: Needless instantiation of class that only supplies static methods; It: Iterator next() method can't throw NoSuchElement exception; J2EE: Store of non serializable object into HttpSession; NP: Clone method may return null; NP: equals() method does not check for null argument; NP: toString method may return null; NS: Questionable use of non-short-circuit logic; Nm: Class names should start with an upper case letter; Nm: Class is not derived from an Exception, even though it is named as such; Nm: Confusing method names; Nm: Field names should start with an lower case letter; Nm: Use of identifier that is a keyword in later versions of Java; Nm: Use of identifier that is a keyword in later versions of Java; Nm: Method names should start with an lower case letter; Nm: Very confusing method names (but intentional); ODR: Method may fail to close database resource; ODR: Method may fail to close database resource on exception; OS: Method may fail to close stream; OS: Method may fail to close stream on exception; RR: Method ignores results of InputStream.read(); RR: Method ignores results of InputStream.skip(); SI: Static initializer creates instance before all static final fields assigned; SQL: Nonconstant string passed to execute method on an SQL statement; SQL: A prepared statement is generated from a nonconstant String; SW: Certain swing methods needs to be invoked in Swing thread; Se: Non-transient non-serializable instance field in serializable class; Se: Non-serializable class has a serializable inner class; Se: Non-serializable value stored into instance field of a serializable class; Se: Comparator doesn't implement Serializable; Se: Serializable inner class; Se: Method must be private in order for serialization to work; Se: serialVersionUID isn't final; Se: serialVersionUID isn't long; Se: serialVersionUID isn't static; Se: Class is Serializable but its superclass doesn't define a void constructor; Se: Class is Externalizabl … tion.; SnVI: Class is Serializable, but doesn't define serialVersionUID; UI: Usage of GetResource may be unsa … masks; BIT: Bitwise OR of signed byte value; BOA: Class overrides a method implemented in super class Adapter … vokes next; DMI: Invocation of toString on an array; DMI: Double.longBitsToDouble invoked on an int; Dm: Can … hich is equivalent to ==; EC: Call to equals() with null argument; EC: Call to equals() comparing unrelated … num; FE: Doomed test for equality to NaN; GC: No relationship between generic parameter and method ar … uble and then passed to Math.ceil; ICAST: int value cast to float and then passed to Math.round; IJU: JUnit assert … uper.setUp(); IJU: TestCase implements a non-static suite method; IJU: TestCase implements tearDown but doesn' … mainder; INT: Bad comparison of nonnegative value with negative constant; INT: Bad comparison of signed byte; … field that masks a superclass field; MF: Method defines a variable that obscures a field; NP: Null pointer deref … P: Value is null and guaranteed to be dereferenced on exception path; NP: Method call passes null to a nonn … dereference; NP: Possible null pointer dereference in method on exception path; NP: Method call passes null … nconditionally dereferenced parameter; NP: Store of null value into field annotated NonNull; NP: Read of unwritten field; NS: Potentially dangerous use of non-short-circuit logic; Nm: Class defines equal(); should it be equals()?; Nm: Class defines hashcode(); should it be hashCode()?; Nm: Class defines tostring(); should it be toString()?; Nm: Apparent method/constructor confusion; Nm: Very confusing method names; QBA: Method assigns boolean literal in boolean expression; RC: Suspicious reference comparison; RCN: Nullcheck of value previously dereferenced; RE: Invalid syntax for regular expression; RE: File.separator used for regular expression; RE: "." used for regular expression; RV: Random value from 0 to 1 is coerced to the integer 0; RV: Bad attempt to compute absolute value of signed 32-bit hashcode; RV: Bad attempt to compute absolute value of signed 32-bit random integer; RV: Method discards result of readLine after checking if it is nonnull; RV: Method ignores return value; SA: Double assignment of field; SA: Self assignment of field; SA: Self comparison of field with itself; SA: Nonsensical self computation involving a field (e.g., x & x); SA: Double assignment of local variable; SA: Self comparison o … ck done using instanceof operator; SQL: Method attempts to access a prepared statement parameter with index 0; … d invoked on thread instance; UCF: Useless control flow to next line; UMAC: Uncallable method defined in anon … iable number of object arguments; Dm: Consider using Locale parameterized version of invoked method; EI: Ma … nalizer should be protected, not public; MS: May expose internal static state by storing a mutable object into a s … ould be both final and package protected; MS: Field is a mutable array; MS: Field is a mutable Hashtable; MS: Field … k of field; Dm: Monitor wait() called on Condition; Dm: A thread was created using the default empty run metho … rrent Lock; LI: Incorrect lazy initialization of static field; ML: Method synchronizes on an updated field; MWN: M … s readObject() method is synchronized; Ru: Invokes run on a thread (did you mean to start it instead?); SC: Con … teFormat; SWL: Method calls Thread.sleep() with a lock held; TLW: Wait with two locks held; UG: Unsynchroniz … wait; VO: A volatile reference to an array doesn't treat the array elements as volatile; WS: Class's writeObject() … mitive value is boxed then unboxed to perform primative coercion; Bx: Method allocates a boxed primitive just to … se static valueOf instead; Dm: The equals and hashCode methods of URL are blocking; Dm: Maps and sets of URLs can be performance hogs; Dm: Method invokes inefficient Boolean constructor; use Boolean.valueOf(...) instead; Dm: Explicit garbage collection; extremely dubious except in benchmarking code; Dm: Method allocates an object, only to get the class object; Dm: Use the nextInt method of Random rather than nextDouble to generate a random integer; Dm: Method invokes inefficient new String(String) constructor; Dm: Method invokes inefficient String.equals(""); use String.length() == 0 instead; Dm: Method invokes toString() method on a String; Dm: Method invokes inefficient new String() constructor; HSC: Huge string constants is duplicated across multiple class files; ITA: Method uses toArray() with zero-length array argument; SBSC: Method concatenates strings using + in a loop; SIC: Should be a static inner class; SIC: Could be refactored into a named static inner class; SIC: Could be refactored into a static inner class; SS: Unread field: should this field be static?; UM: Method calls static Math class method on a constant value; UPM: Private method is never called; UrF: Unread field; UuF: Unused field; WMI: Inefficient use of keySet iterator instead of entrySet iterator; BC: Questionable cast to abstract collection; BC: Questionable cast to concrete collection; BC: Unchecked/unconfirmed cast; BC: instanceof will always return true; CI: Class is final but declares protected field; DB: Method uses the same code for two branches; DB: Method uses the same code for two switch clauses; DLS: Dead store to local variable; DLS: Dead store of null to local variable; DMI: Code contains a hard coded reference to an absolute pathname; DMI: Non serializable object written to ObjectOutput; DMI: Invocation of substring(0), which returns the original value; Dm: Thread passed where Runnable expected; FE: Test for floating point equality; IA: Ambiguous invocation of either an inherited or outer method; IC: Initialization circularity; ICAST: int division result cast to double or float; ICAST: Result of integer multiplication cast to long; ICAST: Unsigned right shift cast to short/byte; IM: Computation of average could overflow; IM: Check for oddness that won't work for negative numbers; INT: Vacuous comparison of integer value; MTIA: Class extends Servlet class and uses instance variables; MTIA: Class extends Struts Action class and uses instance variables; NP: Immediate dereference of the result of readLine(); NP: Load of known null value; NP: Possible null pointer dereference due to return value of called method; PZLA: Consider returning a zero length array rather than null; QF: Complicated, subtle or wrong increment in for-loop; RCN: Redundant comparison of non-null value to null; RCN: Redundant comparison of two null values; RCN: Redundant nullcheck of value known to be non-null; RCN: Redundant nullcheck of value known to be null; REC: Exception is caught when Exception is not thrown; RI: Class implements same interface as superclass; RV: Method checks to see if result of String.indexOf is positive; RV: Remainder of hashCode could be negative; RV: Remainder of 32-bit signed random integer; SA: Self assignment of local variable; SF: Switch statement found where one case falls through to the next case; ST: Write to static field from instance method; Se: Transient field of class that isn't Serializable.; UCF: Useless control flow; UwF: Field not initialized in constructor; XFB: Method directly allocates a specific implementation of xml interfaces

FindBugs: Infinite Loops

- Students are good bug generators:
```
public WebSpider() {
    WebSpider w = new WebSpider();
}
```
- Five infinite loops in JDK1.6.0-b13,
27 across all versions of JDK,
31 in Google's Java code

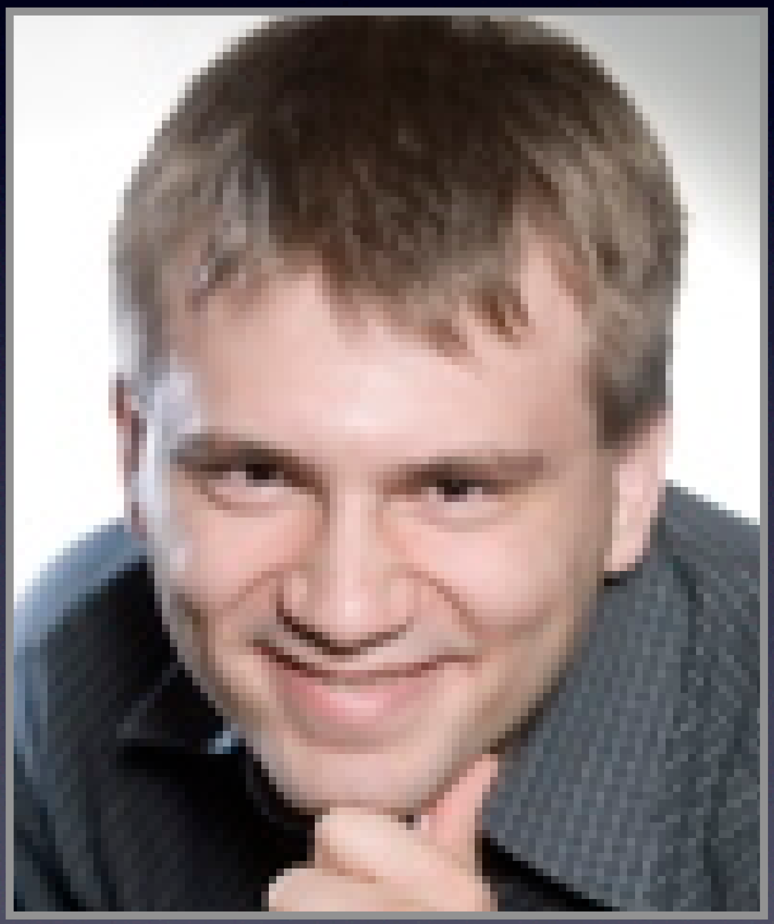
More: http://findbugs.cs.umd.edu/talks/JavaOne2007-TS2007.pdf

Use of history

- Track warnings across releases
  Jaime Spacco, David Hovemeyer, William Pugh: Tracking defect warnings across versions. MSR 2006: 133-136
- Rank warnings with historic data
  Chadd C. Williams, Jeffrey K. Hollingsworth: Automatic Mining of Source Code Repositories to Improve Bug Finding Techniques. IEEE Trans. Software Eng. 31(6): 466-480 (2005)

  Sunghun Kim, Michael D. Ernst: "Which Warnings Should I Fix First?" ESEC/FSE 2007, to appear

Meet & Greet



Andrzej
Wasylkowski

Slides will be available
on the lecture web-page.

Statistical bug isolation

Ben Liblit

PLDI 2005 Slides at http://pages.cs.wisc.edu/~liblit/pldi-2005/

References

- Yichen Xie, Dawson R. Engler: Using redundancies to find errors. SIGSOFT FSE 2002: 51-60
- Bill Pugh: FindBugs™ - Find Bugs in Java Programs. http://findbugs.sourceforge.net/
- Andrzej Wasylkowski, Andreas Zeller: Detecting Object Usage Anomalies. ESEC/FSE 2007, to appear
- Ben Liblit, Mayur Naik, Alice X. Zheng, Alexander Aiken, Michael I. Jordan: Scalable statistical bug isolation. PLDI 2005: 15-26