Screen After Previous Screens: Spatial-Temporal Recreation of Android App Displays from Memory Images

Brendan Saltaformaggio, Rohit Bhatia, Xiangyu Zhang, Dongyan Xu, Golden G. Richard III*

Purdue University

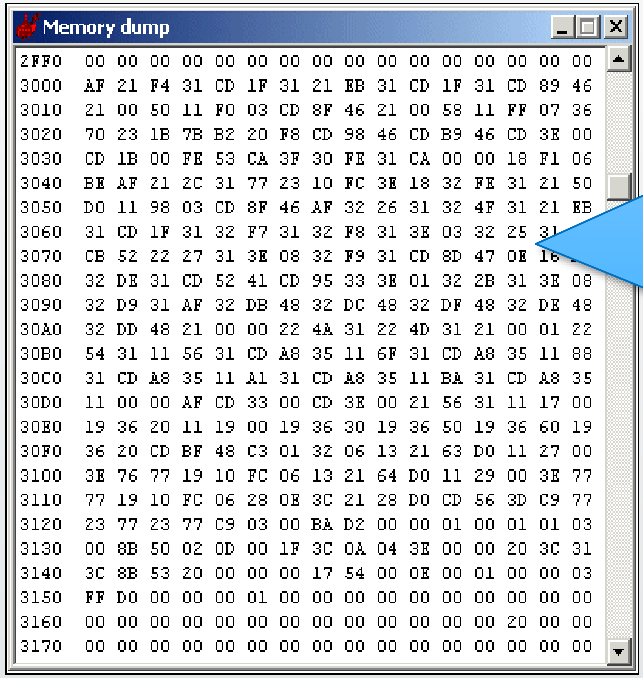
*University of New Orleans

A Crime To Investigate…

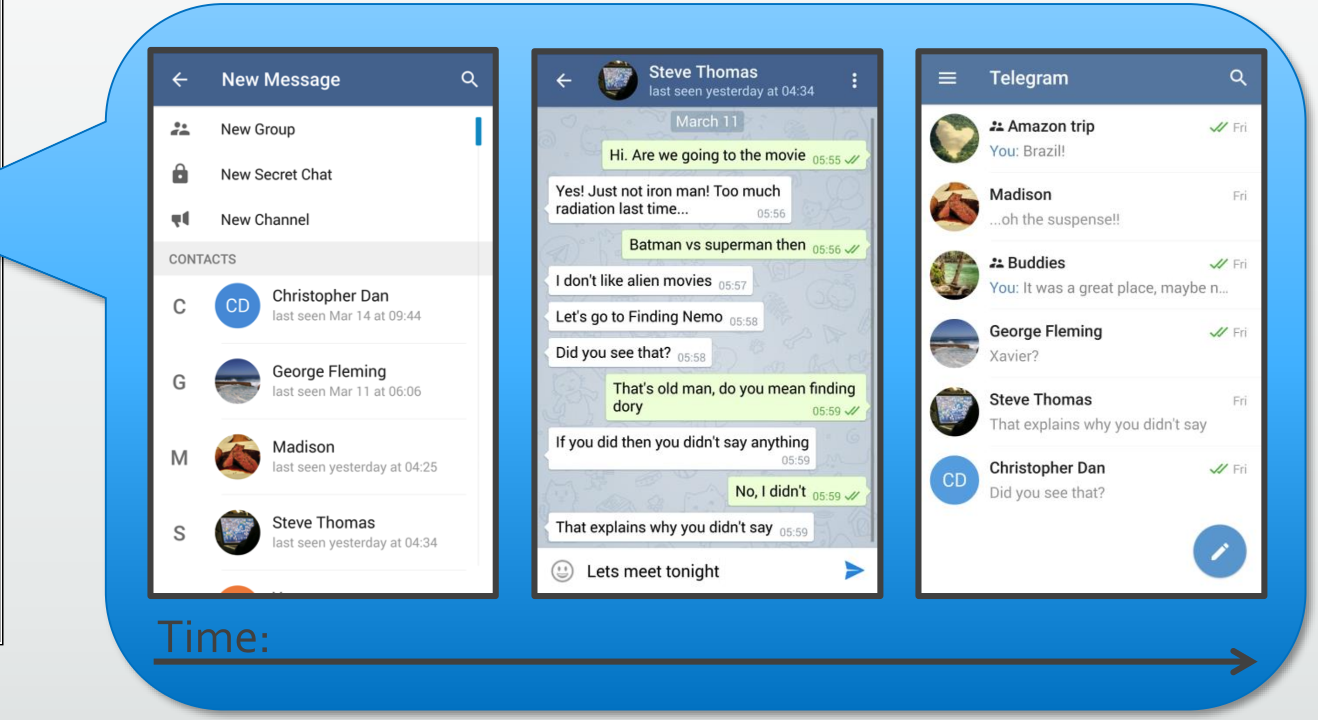
Before the investigation began,
the suspect was interacting
with their apps…

Without access to the suspect's password or breaking Telegram's fully encrypted storage!

Memory Forensics …or Mission Impossible?


Memory dump

```
2FF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000   AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010   21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020   70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030   CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040   BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050   D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060   31 CD 1F 31 32 F7 31 32 F8 31 3E 03 32 25 31
3070   CB 52 22 27 31 3E 08 32 F9 31 CD 8D 47 0E 16
3080   32 DE 31 CD 52 41 CD 95 33 3E 01 32 2B 31 3E 08
3090   32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 32 DE 48
30A0   32 DD 48 21 00 00 22 4A 31 22 4D 31 21 00 01 22
30B0   54 31 11 56 31 CD A8 35 11 6F 31 CD A8 35 11 88
30C0   31 CD A8 35 11 A1 31 CD A8 35 11 BA 31 CD A8 35
30D0   11 00 00 AF CD 33 00 CD 3E 00 21 56 31 11 17 00
30E0   19 36 20 11 19 00 19 36 30 19 36 50 19 36 60 19
30F0   36 20 CD BF 48 C3 01 32 06 13 21 63 D0 11 27 00
3100   3E 76 77 19 10 FC 06 13 21 64 D0 11 29 00 3E 77
3110   77 19 10 FC 06 28 0E 3C 21 28 D0 CD 56 3D C9 77
3120   23 77 23 77 C9 03 00 BA D2 00 00 01 00 01 01 03
3130   00 8B 50 02 0D 00 1F 3C 0A 04 3E 00 00 20 3C 31
3140   3C 8B 53 20 00 00 00 17 54 00 0E 00 01 00 00 03
3150   FF D0 00 00 00 01 00 00 00 00 00 00 00 00 00 00
3160   00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00
3170   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```


New Message

New Group

New Secret Chat

New Channel

CONTACTS

C Christopher Dan – last seen Mar 14 at 09:44

G George Fleming – last seen Mar 11 at 06:06

M Madison – last seen yesterday at 04:25

S Steve Thomas – last seen yesterday at 04:34

Steve Thomas – last seen yesterday at 04:34

March 11

Hi. Are we going to the movie 05:55

Yes! Just not iron man! Too much radiation last time... 05:56

Batman vs superman then 05:56

I don't like alien movies 05:57

Let's go to Finding Nemo 05:58

Did you see that? 05:58

That's old man, do you mean finding dory 05:59

If you did then you didn't say anything 05:59

No, I didn't 05:59

That explains why you didn't say 05:59

Lets meet tonight

Telegram

Amazon trip – You: Brazil! – Fri

Madison – ...oh the suspense!! – Fri

Buddies – You: It was a great place, maybe n... – Fri

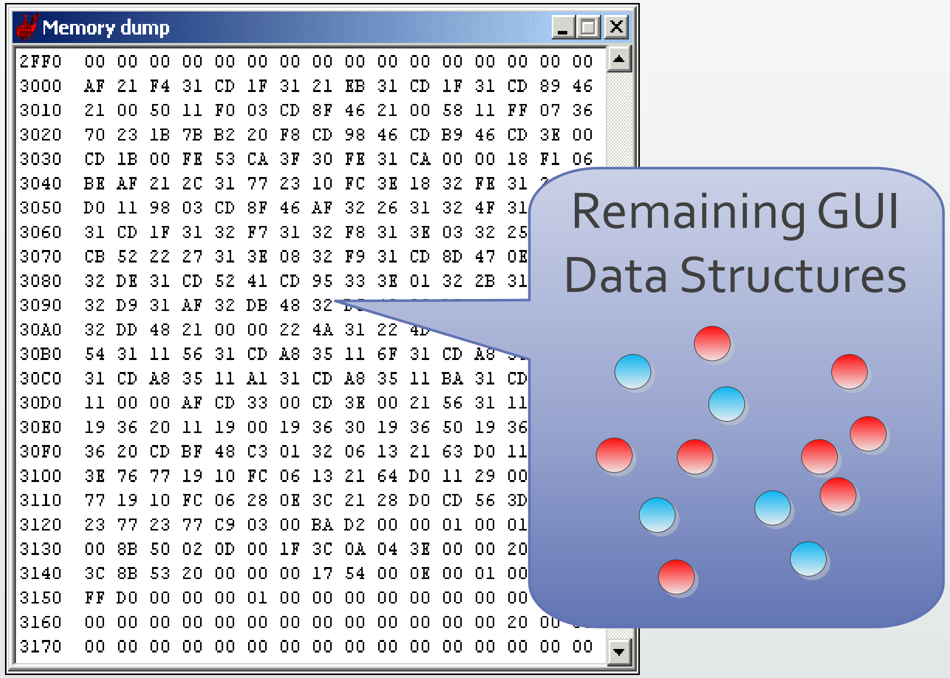
George Fleming – Xavier? – Fri

Steve Thomas – That explains why you didn't say – Fri

Christopher Dan – Did you see that? – Fri

State of the Art: GUITAR - GUI Tree ARchaeology

[CCS ’15, Best Paper]

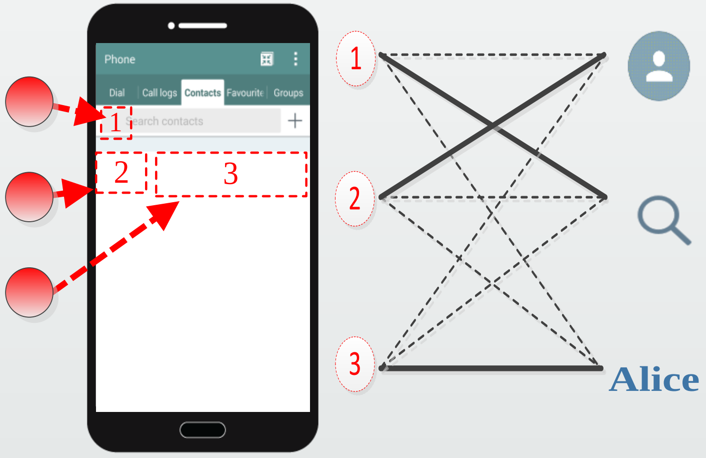


Memory dump

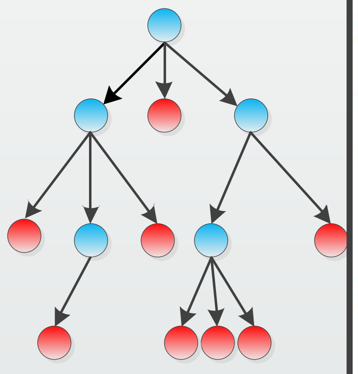
```
2FF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000   AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010   21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020   70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030   CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040   BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31
3050   D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31
3060   31 CD 1F 31 32 F7 31 32 F8 31 3E 03 32 25
3070   CB 52 22 27 31 3E 08 32 F9 31 CD 8D 47 0E
3080   32 DE 31 CD 52 41 CD 95 33 3E 01 32 2B 31
3090   32 D9 31 AF 32 DB 48 32
30A0   32 DD 48 21 00 00 22 4A 31 22
30B0   54 31 11 56 31 CD A8 35 11 6F 31 CD A8
30C0   31 CD A8 35 11 A1 31 CD A8 35 11 BA 31 CD
30D0   11 00 00 AF CD 33 00 CD 3E 00 21 56 31 11
30E0   19 36 20 11 19 00 19 36 30 19 36 50 19 36
30F0   36 20 CD BF 48 C3 01 32 06 13 21 63 D0 11
3100   3E 76 77 19 10 FC 06 13 21 64 D0 11 29 00
3110   77 19 10 FC 06 28 0E 3C 21 28 D0 CD 56 3D
3120   23 77 23 77 C9 03 00 BA D2 00 00 01 00 01
3130   00 8B 50 02 0D 00 1F 3C 0A 04 3E 00 00 20
3140   3C 8B 53 20 00 00 00 17 54 00 0E 00 01 00
3150   FF D0 00 00 00 01 00 00 00 00 00 00 00 00
3160   00 00 00 00 00 00 00 00 00 00 00 00 00 20 00
3170   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

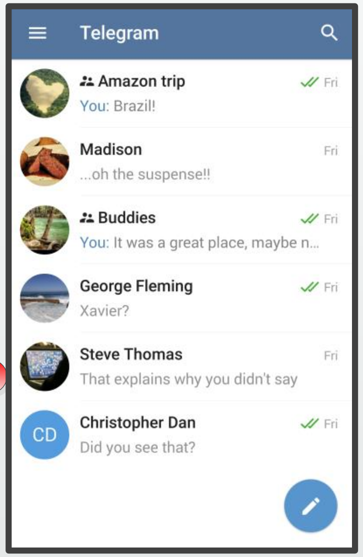
Remaining GUI Data Structures

Drawing-Content-Based Bipartite Graph Matching



GUI Tree





Telegram

Amazon trip — You: Brazil! — Fri

Madison — ...oh the suspense!! — Fri

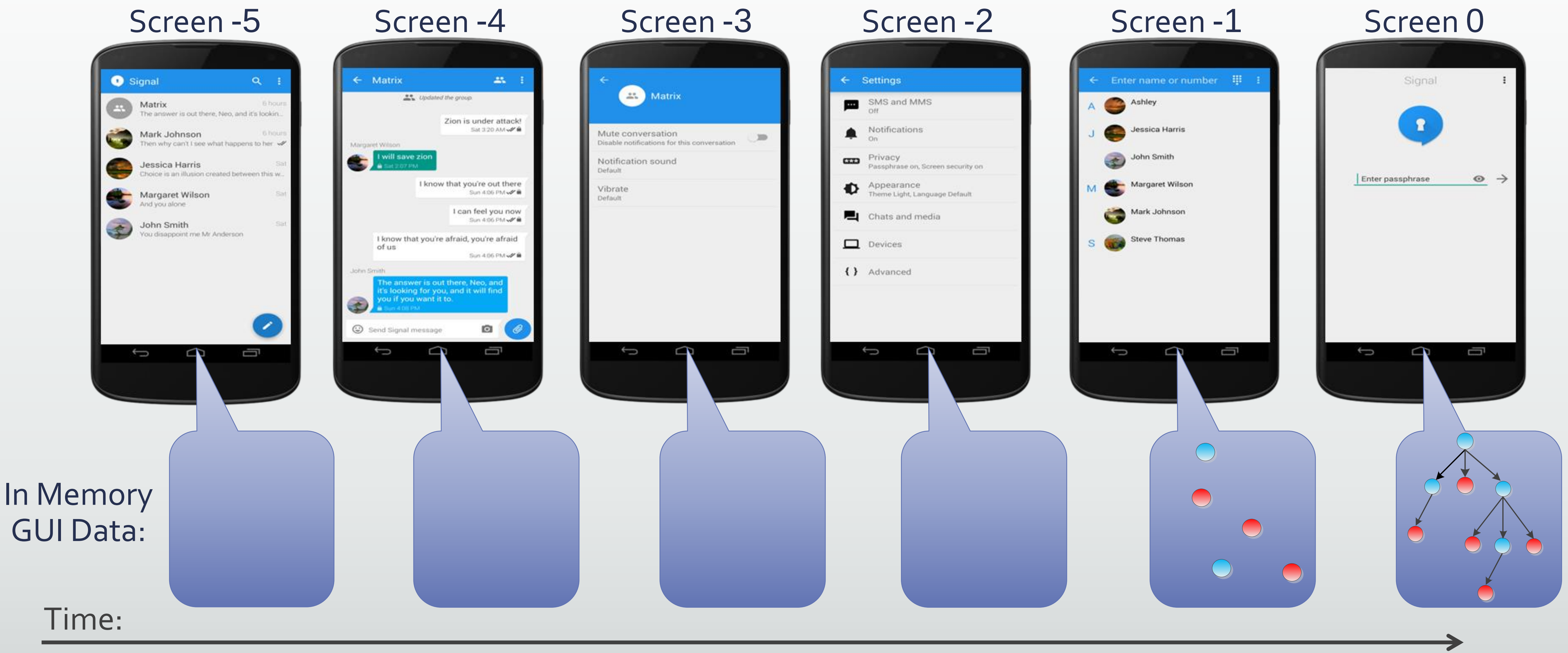
Buddies — You: It was a great place, maybe n... — Fri

George Fleming — Xavier? — Fri

Steve Thomas — That explains why you didn't say — Fri

CD Christopher Dan — Did you see that? — Fri

The “Screen 0” Limitation of GUITAR



Screen -5

Signal

Matrix 6 hours
The answer is out there, Neo, and it's lookin...

Mark Johnson 6 hours
Then why can't I see what happens to her

Jessica Harris Sat
Choice is an illusion created between this w...

Margaret Wilson Sat
And you alone

John Smith Sat
You disappoint me Mr Anderson

Screen -4

Matrix

Updated the group

Zion is under attack!
Sat 3:20 AM

Margaret Wilson
I will save zion
Sat 2:07 PM

I know that you're out there
Sun 4:06 PM

I can feel you now
Sun 4:06 PM

I know that you're afraid, you're afraid of us
Sun 4:06 PM

John Smith
The answer is out there, Neo, and it's looking for you, and it will find you if you want it to.
Sun 4:08 PM

Send Signal message

Screen -3

Matrix

Mute conversation
Disable notifications for this conversation

Notification sound
Default

Vibrate
Default

Screen -2

Settings

SMS and MMS
Off

Notifications
On

Privacy
Passphrase on, Screen security on

Appearance
Theme Light, Language Default

Chats and media

Devices

Advanced

Screen -1

Enter name or number

A Ashley

J Jessica Harris

John Smith

M Margaret Wilson

Mark Johnson

S Steve Thomas

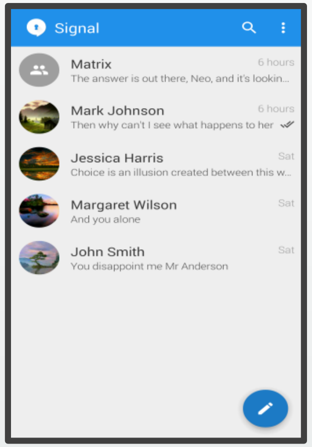
Screen 0

Signal

Enter passphrase

Are The Old Screens Really Gone?

Screen -5



Matrix 6 hours
The answer is out there, Neo, and it's lookin...

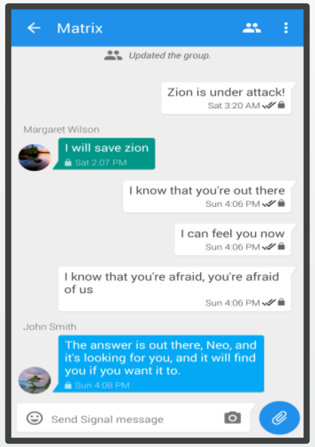
Mark Johnson 6 hours
Then why can't I see what happens to her

Jessica Harris Sat
Choice is an illusion created between this w...

Margaret Wilson Sat
And you alone

John Smith Sat
You disappoint me Mr Anderson

Screen -4



Updated the group.

Zion is under attack!
Sat 3:20 AM

Margaret Wilson
I will save zion
Sat 2:07 PM

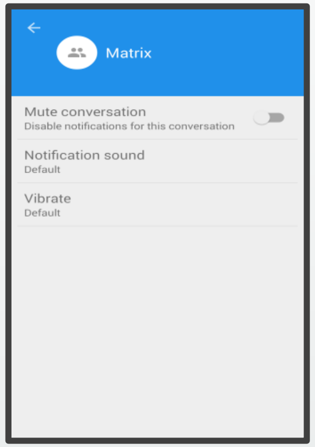
I know that you're out there
Sun 4:06 PM

I can feel you now
Sun 4:06 PM

I know that you're afraid, you're afraid of us
Sun 4:06 PM

John Smith
The answer is out there, Neo, and it's looking for you, and it will find you if you want it to.
Sun 4:08 PM

Screen -3

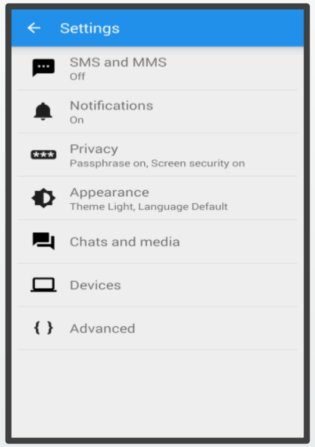


Mute conversation
Disable notifications for this conversation

Notification sound
Default

Vibrate
Default

Screen -2



SMS and MMS
Off

Notifications
On

Privacy
Passphrase on, Screen security on

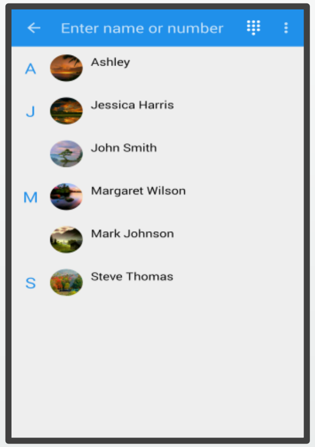
Appearance
Theme Light, Language Default

Chats and media

Devices

{ } Advanced

Screen -1



A Ashley

J Jessica Harris

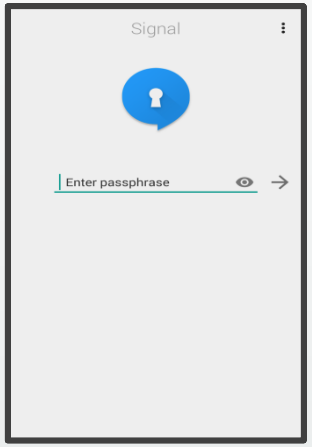
John Smith

M Margaret Wilson

Mark Johnson

S Steve Thomas

Screen 0



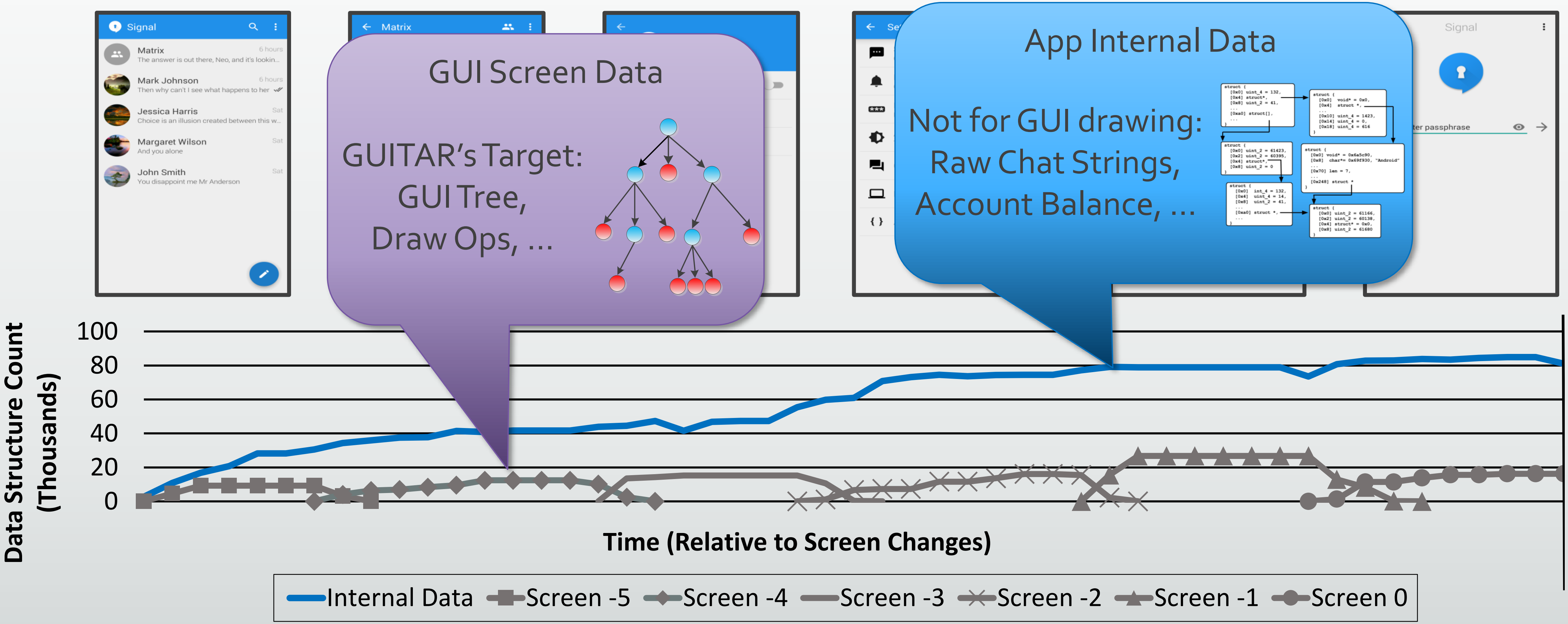
App screen changes are **highly dynamic**

How can every screen be **fully rebuilt** so fast?

Some **data must remain** to bring the screens back

Are The Old Screens Really Gone? … Yes and No

Screen -5 Screen -4 Screen -3 Screen -2 Screen -1 Screen 0



Signal

Matrix 6 hours
The answer is out there, Neo, and it's lookin…

Mark Johnson 6 hours
Then why can't I see what happens to her

Jessica Harris Sat
Choice is an illusion created between this w…

Margaret Wilson Sat
And you alone

John Smith Sat
You disappoint me Mr Anderson

GUI Screen Data

GUITAR's Target:
GUI Tree,
Draw Ops, …

App Internal Data

Not for GUI drawing:
Raw Chat Strings,
Account Balance, …

```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}
```

```
struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}
```

```
struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}
```

```
struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}
```

```
struct {
  [0x0]  int_4 = 132,
  [0x4]  uint_4 = 14,
  [0x8]  uint_2 = 41,
  ...
  [0xa0] struct *,
  ...
}
```

```
struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```

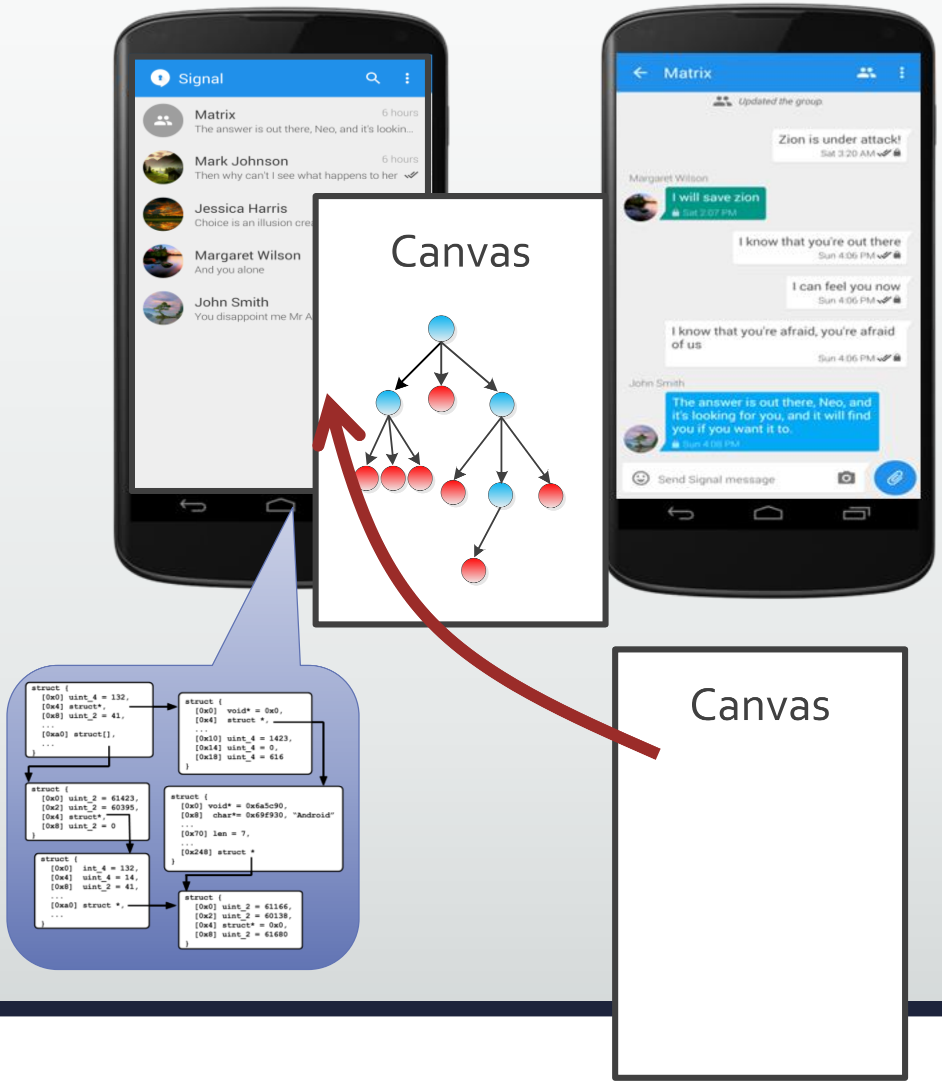
Android Asks The App To Draw A Screen

Android sends a **Redraw Command**

1) A **Canvas** is sent for the app to fill
   - Apps register *draw* routines with Android

2) The app **builds GUI structures** which "package" the internal data
   - Destroying the previous screen!

3) The filled canvas is **rendered** on the device's screen



Signal

Matrix — 6 hours
The answer is out there, Neo, and it's lookin...

Mark Johnson — 6 hours
Then why can't I see what happens to her

Jessica Harris
Choice is an illusion crea

Margaret Wilson
And you alone

John Smith
You disappoint me Mr A

Matrix

Updated the group

Zion is under attack!
Sat 3:20 AM

Margaret Wilson
I will save zion
Sat 2:07 PM

I know that you're out there
Sun 4:06 PM

I can feel you now
Sun 4:06 PM

I know that you're afraid, you're afraid of us
Sun 4:06 PM

John Smith
The answer is out there, Neo, and it's looking for you, and it will find you if you want it to.
Sun 4:08 PM

Send Signal message

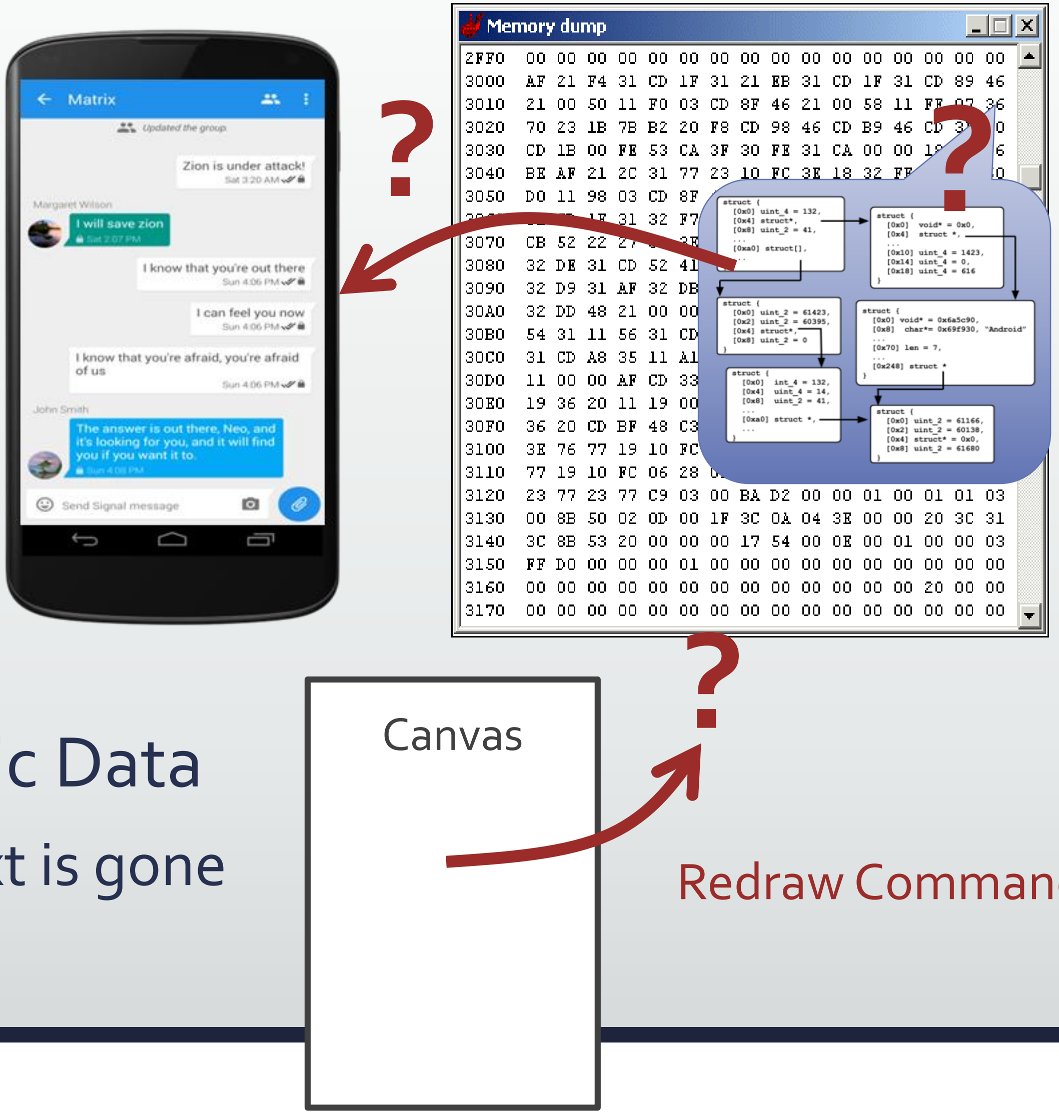
```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}

struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}

struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}

struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}

struct {
  [0x0]  int_4 = 132,
  [0x4]  uint_4 = 14,
  [0x8]  uint_2 = 41,
  ...
  [0xa0] struct *,
  ...
}

struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```

Idea: Ask The Memory Image To Draw A Screen

Challenges:

1) How to inject the Redraw Command?
   - Screen-specific *draw* routines

3) Memory = Static Data
   - Execution context is gone



Matrix

Updated the group

Zion is under attack!
Sat 3:20 AM

Margaret Wilson

I will save zion
Sat 2:07 PM

I know that you're out there
Sun 4:06 PM

I can feel you now
Sun 4:06 PM

I know that you're afraid, you're afraid of us
Sun 4:06 PM

John Smith

The answer is out there, Neo, and it's looking for you, and it will find you if you want it to.
Sun 4:08 PM

Send Signal message

Memory dump

```
2FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000  AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010  21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FE 07 36
3020  70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3     0
3030  CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 1     6
3040  BE AF 21 2C 31 77 23 10 FC 3E 18 32 FF     0
3050  D0 11 98 03 CD 8F
            1F 31 32 F7
3070  CB 52 22 27       3E
3080  32 DE 31 CD 52 41
3090  32 D9 31 AF 32 DB
30A0  32 DD 48 21 00 00
30B0  54 31 11 56 31 CD
30C0  31 CD A8 35 11 A1
30D0  11 00 00 AF CD 33
30E0  19 36 20 11 19 00
30F0  36 20 CD BF 48 C3
3100  3E 76 77 19 10 FC
3110  77 19 10 FC 06 28
3120  23 77 23 77 C9 03 00 BA D2 00 00 01 00 01 01 03
3130  00 8B 50 02 0D 00 1F 3C 0A 04 3E 00 00 20 3C 31
3140  3C 8B 53 20 00 00 00 17 54 00 0E 00 01 00 00 03
3150  FF D0 00 00 00 01 00 00 00 00 00 00 00 00 00 00
3160  00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00
3170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
```

```
struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}
```

```
struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}
```

```
struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}
```

```
struct {
  [0x0]  int_4 = 132,
  [0x4]  uint_4 = 14,
  [0x8]  uint_2 = 41,
  ...
  [0xa0] struct *,
  ...
}
```

```
struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```

Redraw Command

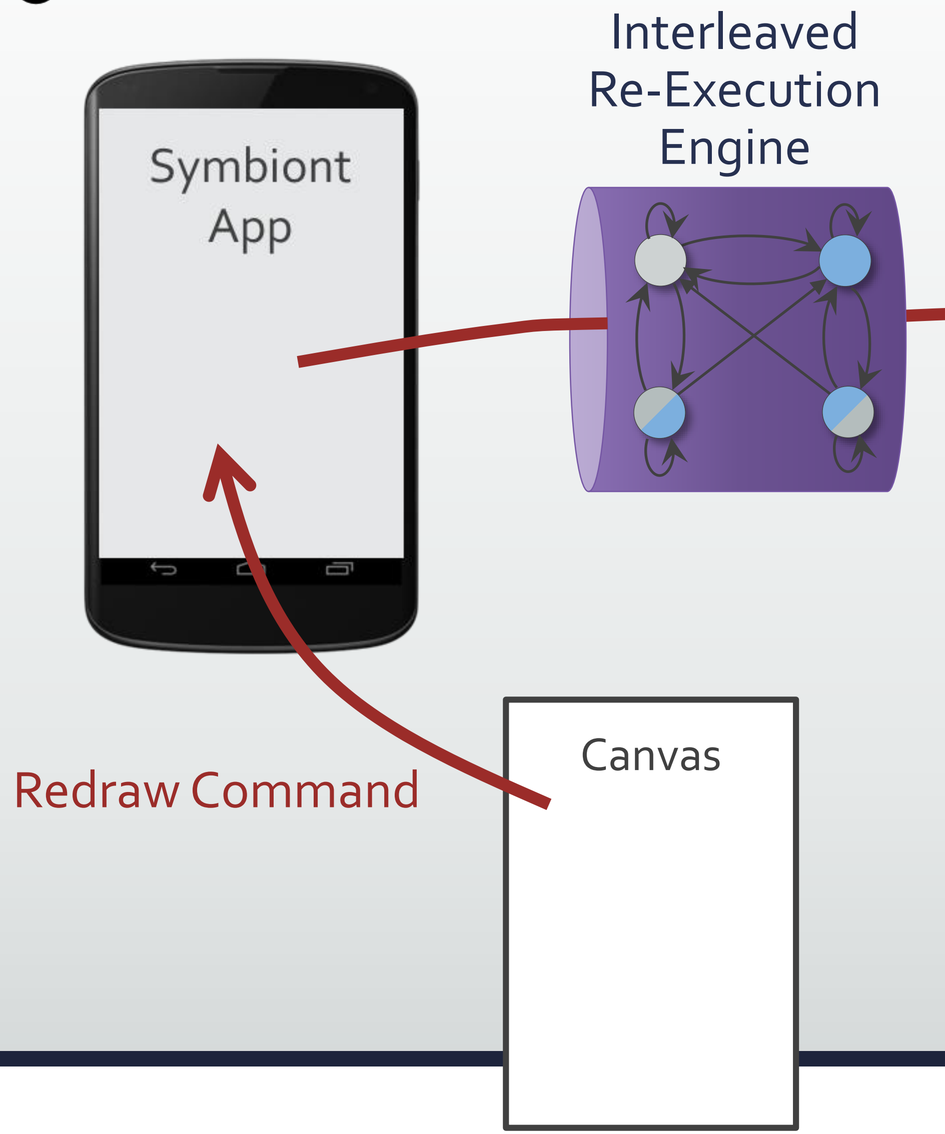
2) Need to understand the app internal data?

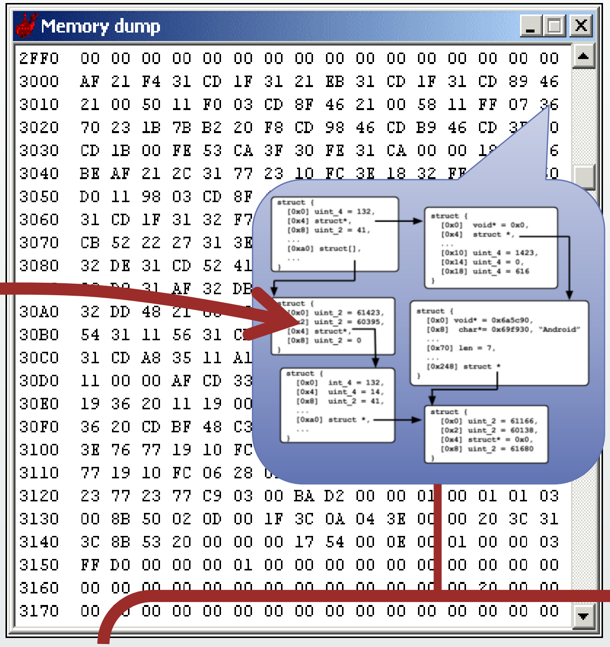
Previous Approaches:

- Data structure signature scanning
- App-specific reverse engineering

Our Goal: "Plug And Play" App-Agnostic Recovery

RetroScope: Spatial-Temporal Display Recreation



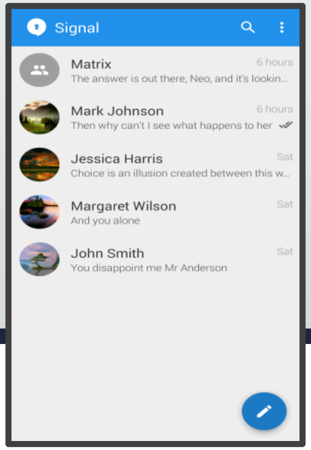


```
2FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000  AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010  21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020  70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3
3030  CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 1
3040  BE AF 21 2C 31 77 23 10 FC 3E 18 32 FF
3050  D0 11 98 03 CD 8F
3060  31 CD 1F 31 32 F7
3070  CB 52 22 27 31 3E
3080  32 DE 31 CD 52 41
         31 AF 32 DB
30A0  32 DD 48 21
30B0  54 31 11 56 31 C
30C0  31 CD A8 35 11 A1
30D0  11 00 00 AF CD 33
30E0  19 36 20 11 19 00
30F0  36 20 CD BF 48 C3
3100  3E 76 77 19 10 FC
3110  77 19 10 FC 06 28
3120  23 77 23 77 C9 03 00 BA D2 00 00 01 00 01 01 03
3130  00 8B 50 02 0D 00 1F 3C 0A 04 3E 00 00 20 3C 31
3140  3C 8B 53 20 00 00 00 17 54 00 0E 00 01 00 00 03
3150  FF D0 00 00 00 01 00 00 00 00 00 00 00 00 00 00
3160  00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00
3170  00    00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}

struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}

struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}

struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}

struct {
  [0x0]  int_4 = 132,
  [0x4]  uint_4 = 14,
  [0x8]  uint_2 = 41,
  ...
  [0xa0] struct *,
  ...
}

struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```

Performs **app-agnostic** screen reconstruction from an app's internal data **within a memory image**

Screen -3



Matrix — 6 hours
The answer is out there, Neo, and it's lookin...

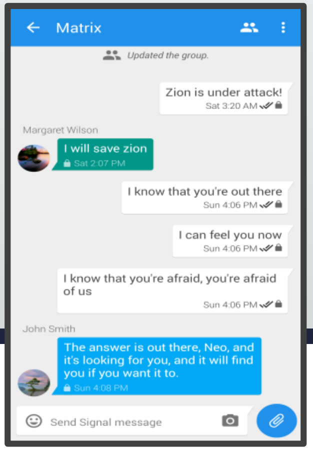
Mark Johnson — 6 hours
Then why can't I see what happens to her

Jessica Harris — Sat
Choice is an illusion created between this w...

Margaret Wilson — Sat
And you alone

John Smith — Sat
You disappoint me Mr Anderson

Screen -2



Updated the group.

Zion is under attack!
Sat 3:20 AM

Margaret Wilson
I will save zion
Sat 2:07 PM

I know that you're out there
Sun 4:06 PM

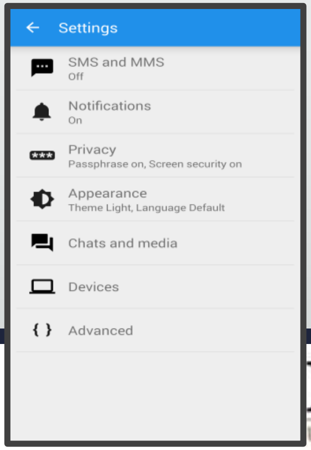
I can feel you now
Sun 4:06 PM

I know that you're afraid, you're afraid of us
Sun 4:06 PM

John Smith
The answer is out there, Neo, and it's looking for you, and it will find you if you want it to.
Sun 4:08 PM

Send Signal message

Screen -1



SMS and MMS
Off

Notifications
On

Privacy
Passphrase on, Screen security on

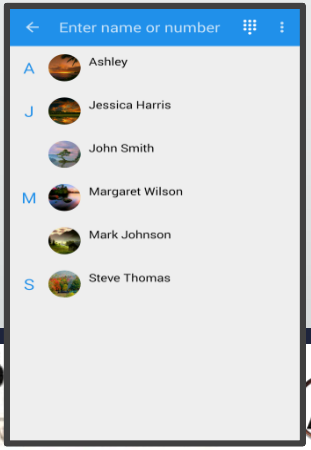
Appearance
Theme Light, Language Default

Chats and media

Devices

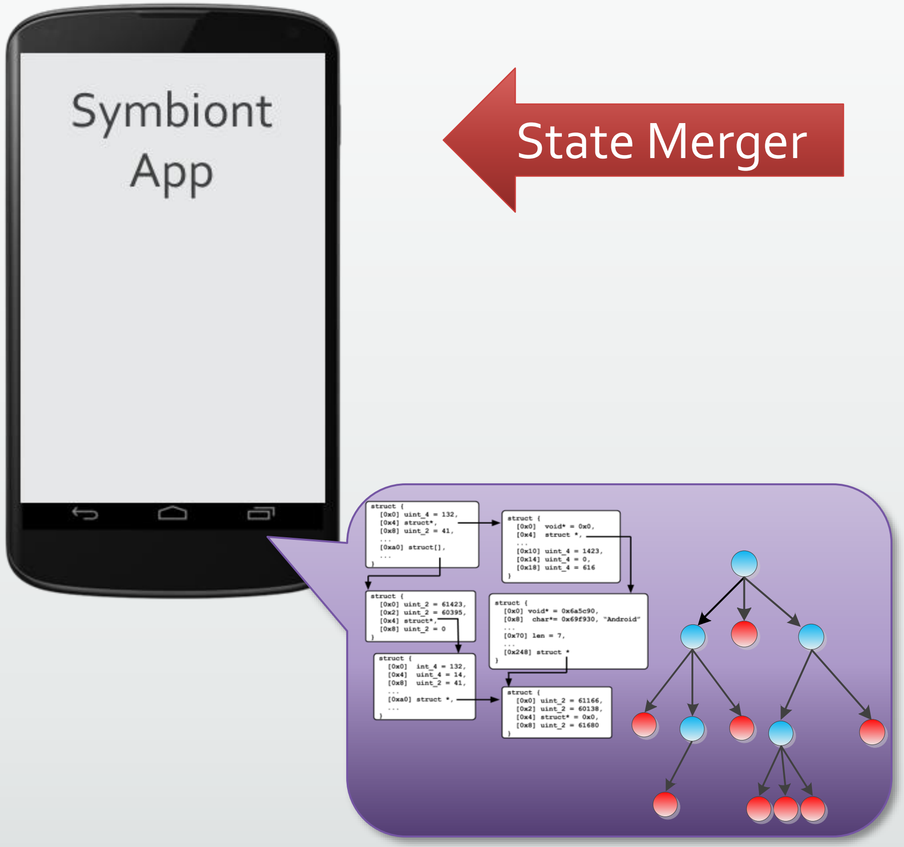
Advanced

Screen 0

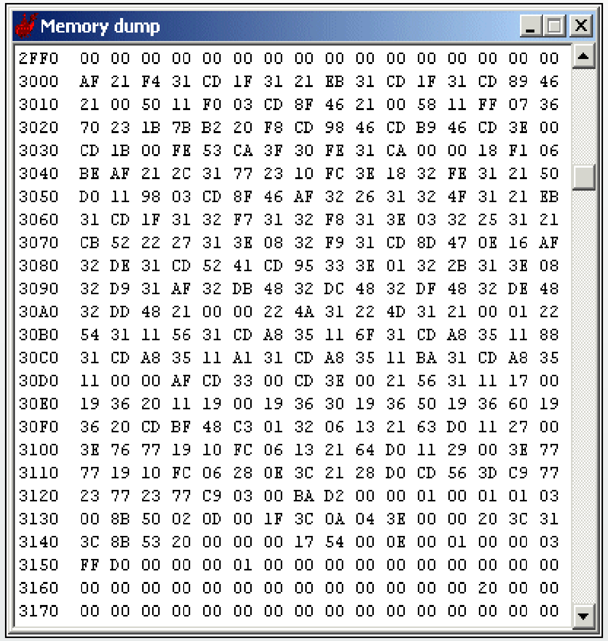


A Ashley
J Jessica Harris
John Smith
M Margaret Wilson
Mark Johnson
S Steve Thomas

Symbiont App: Two Apps In One



```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}

struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}

struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}

struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}

struct {
  [0x0]  int_4 = 132,
  [0x4]  uint_4 = 14,
  [0x8]  uint_2 = 41,
  ...
  [0xa0] struct *,
  ...
}

struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```



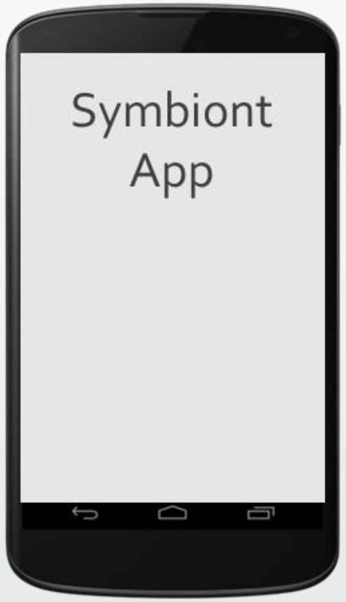
```
2FF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000   AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010   21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020   70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030   CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040   BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050   D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060   31 CD 1F 31 32 F7 31 32 F8 31 3E 03 32 25 31 21
3070   CB 52 22 27 31 3E 08 32 F9 31 CD 8D 47 0E 16 AF
3080   32 DE 31 CD 52 41 CD 95 33 3E 01 32 2B 31 3E 08
3090   32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 32 DE 48
30A0   32 DD 48 21 00 00 22 4A 31 22 4D 31 21 00 01 22
30B0   54 31 11 56 31 CD A8 35 11 6F 31 CD A8 35 11 88
30C0   31 CD A8 35 11 A1 31 CD A8 35 11 BA 31 CD A8 35
30D0   11 00 00 AF CD 33 00 CD 3E 00 21 56 31 11 17 00
30E0   19 36 20 11 19 00 19 36 30 19 36 50 19 36 60 19
30F0   36 20 CD BF 48 C3 01 32 06 13 21 63 D0 11 27 00
3100   3E 76 77 19 10 FC 06 13 21 64 D0 11 29 00 3E 77
3110   77 19 10 FC 06 28 0E 3C 21 28 D0 CD 56 3D C9 77
3120   23 77 23 77 C9 03 00 BA D2 00 00 01 00 01 01 03
3130   00 8B 50 02 0D 00 1F 3C 0A 04 3E 00 00 20 3C 31
3140   3C 8B 53 20 00 00 00 17 54 00 0E 00 01 00 00 03
3150   FF D0 00 00 00 01 00 00 00 00 00 00 00 00 00 00
3160   00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00
3170   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

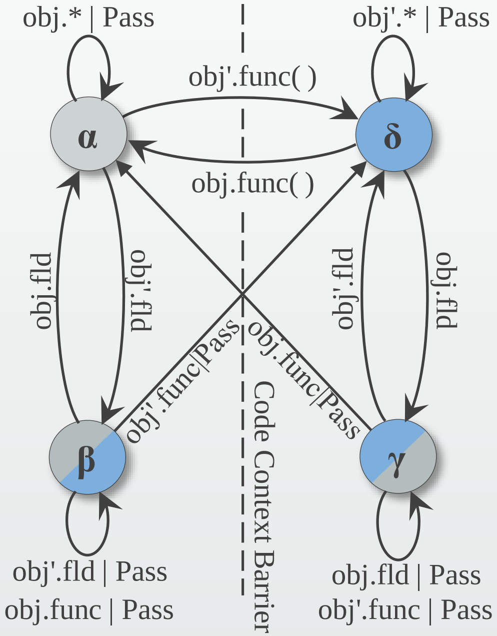
Step 1) Start the **Symbiont App** to host the memory image

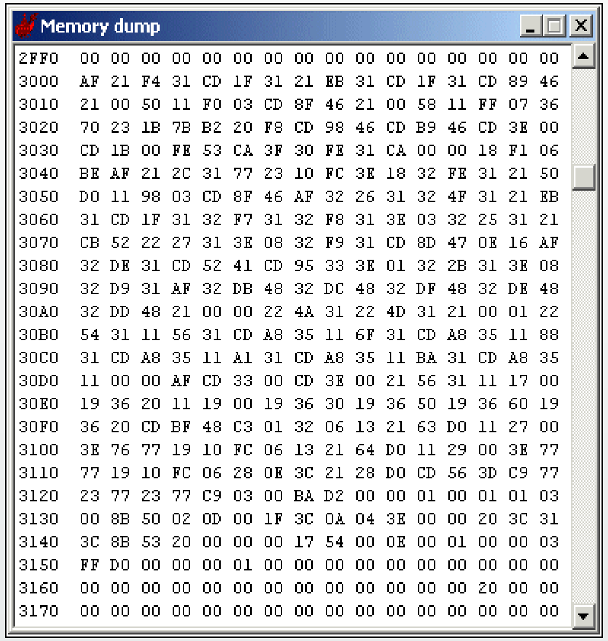
Step 2) **Move** the memory image state into the Symbiont App

- Map memory segments
- Merge Java runtimes
- Register *draw* functions

Interleaved Re-Execution Engine







```
2FF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000   AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010   21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020   70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030   CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040   BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050   D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060   31 CD 1F 31 32 F7 31 32 F8 31 3E 03 32 25 31 21
3070   CB 52 22 27 31 3E 08 32 F9 31 CD 8D 47 0E 16 AF
3080   32 DE 31 CD 52 41 CD 95 33 3E 01 32 2B 31 3E 08
3090   32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 32 DE 48
30A0   32 DD 48 21 00 00 22 4A 31 22 4D 31 21 00 01 22
30B0   54 31 11 56 31 CD A8 35 11 6F 31 CD A8 35 11 88
30C0   31 CD A8 35 11 A1 31 CD A8 35 11 BA 31 CD A8 35
30D0   11 00 00 AF CD 33 00 CD 3E 00 21 56 31 11 17 00
30E0   19 36 20 11 19 00 19 36 30 19 36 50 19 36 60 19
30F0   36 20 CD BF 48 C3 01 32 06 13 21 63 D0 11 27 00
3100   3E 76 77 19 10 FC 06 13 21 64 D0 11 29 00 3E 77
3110   77 19 10 FC 06 28 0E 3C 21 28 D0 CD 56 3D C9 77
3120   23 77 23 77 C9 03 00 BA D2 00 00 01 00 01 01 03
3130   00 8B 50 02 0D 00 1F 3C 0A 04 3E 00 00 20 3C 31
3140   3C 8B 53 20 00 00 00 17 54 00 0E 00 01 00 00 03
3150   FF D0 00 00 00 01 00 00 00 00 00 00 00 00 00 00
3160   00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00
3170   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

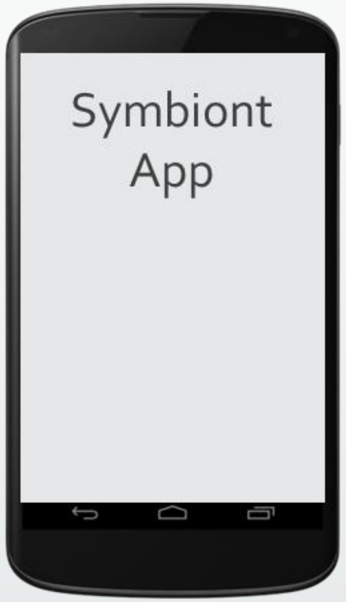
Step 3) Initialize the **Interleaved Re-Execution Engine** (IRE)

Formally modeled the interleaving of states as a finite automata

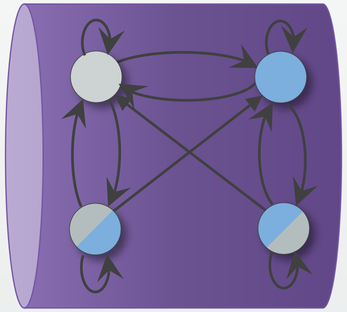
Transition rules guided by executing instruction semantics

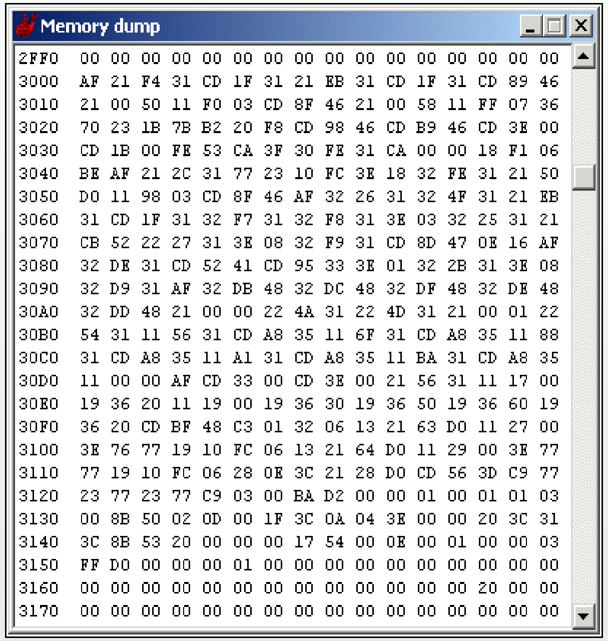
The Overly Simple Explanation:
Live Code outputs to Live Environment &
Old Code reads from Old Environment

Interleaved Re-Execution Engine



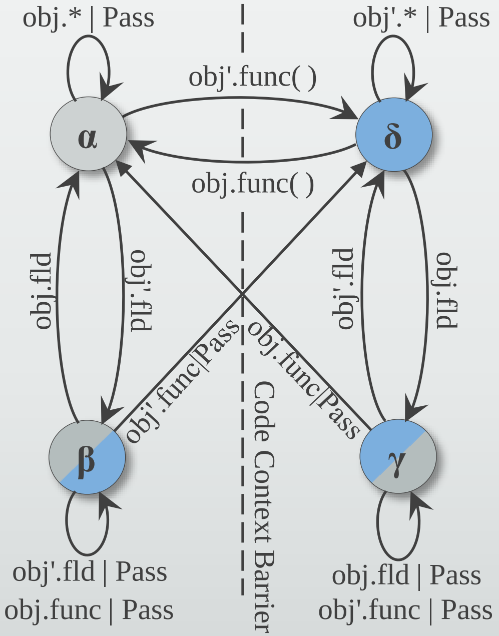
Interleaved Re-Execution Engine



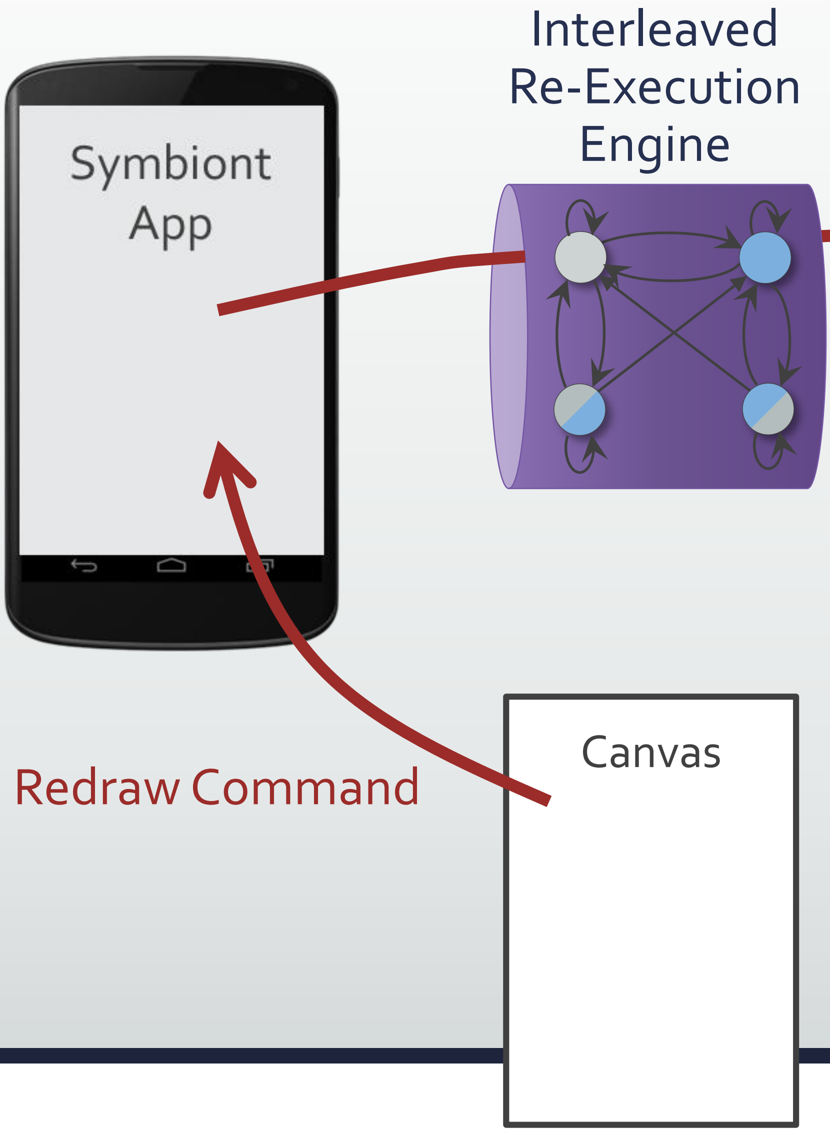


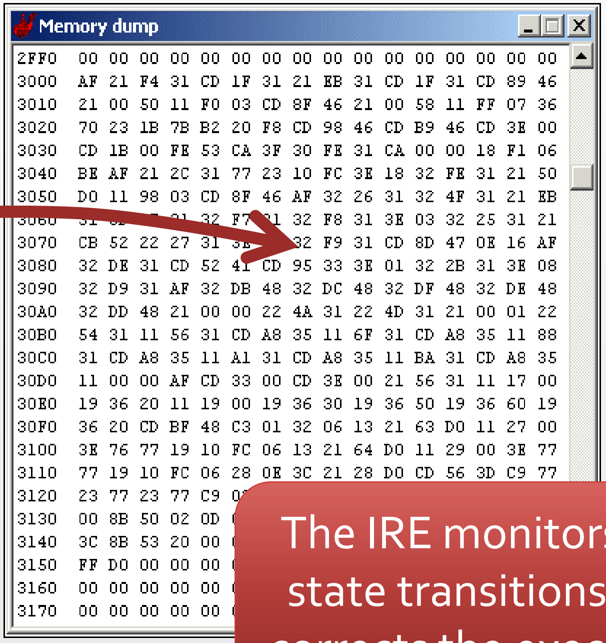
```
2FF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000   AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010   21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020   70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030   CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040   BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050   D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060   31 CD 1F 31 32 F7 31 32 F8 31 3E 03 32 25 31 21
3070   CB 52 22 27 31 3E 08 32 F9 31 CD 8D 47 0E 16 AF
3080   32 DE 31 CD 52 41 CD 95 33 3E 01 32 2B 31 3E 08
3090   32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 32 DE 48
30A0   32 DD 48 21 00 00 22 4A 31 22 4D 31 21 00 01 22
30B0   54 31 11 56 31 CD A8 35 11 6F 31 CD A8 35 11 88
30C0   31 CD A8 35 11 A1 31 CD A8 35 11 BA 31 CD A8 35
30D0   11 00 00 AF CD 33 00 CD 3E 00 21 56 31 11 17 00
30E0   19 36 20 11 19 00 19 36 30 19 36 50 19 36 60 19
30F0   36 20 CD BF 48 C3 01 32 06 13 21 63 D0 11 27 00
3100   3E 76 77 19 10 FC 06 13 21 64 D0 11 29 00 3E 77
3110   77 19 10 FC 06 28 0E 3C 21 28 D0 CD 56 3D C9 77
3120   23 77 23 77 C9 03 00 BA D2 00 00 01 00 01 01 03
3130   00 8B 50 02 0D 00 1F 3C 0A 04 3E 00 00 20 3C 31
3140   3C 8B 53 20 00 00 00 17 54 00 0E 00 01 00 00 03
3150   FF D0 00 00 00 01 00 00 00 00 00 00 00 00 00 00
3160   00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00
3170   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Step 3) Initialize the **Interleaved Re-Execution Engine** (IRE)



Selective Reanimation

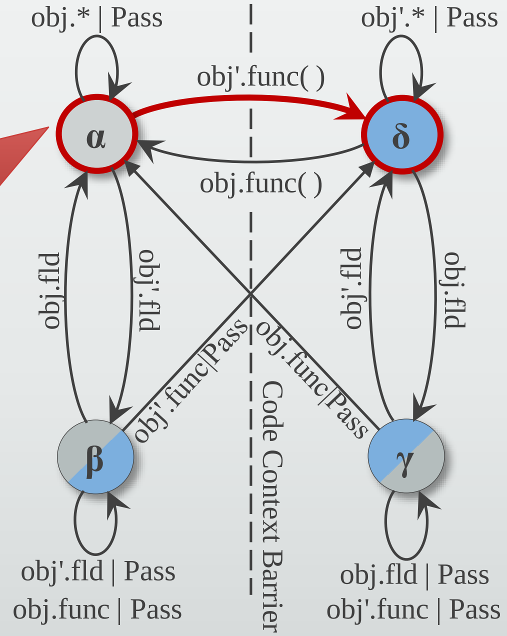




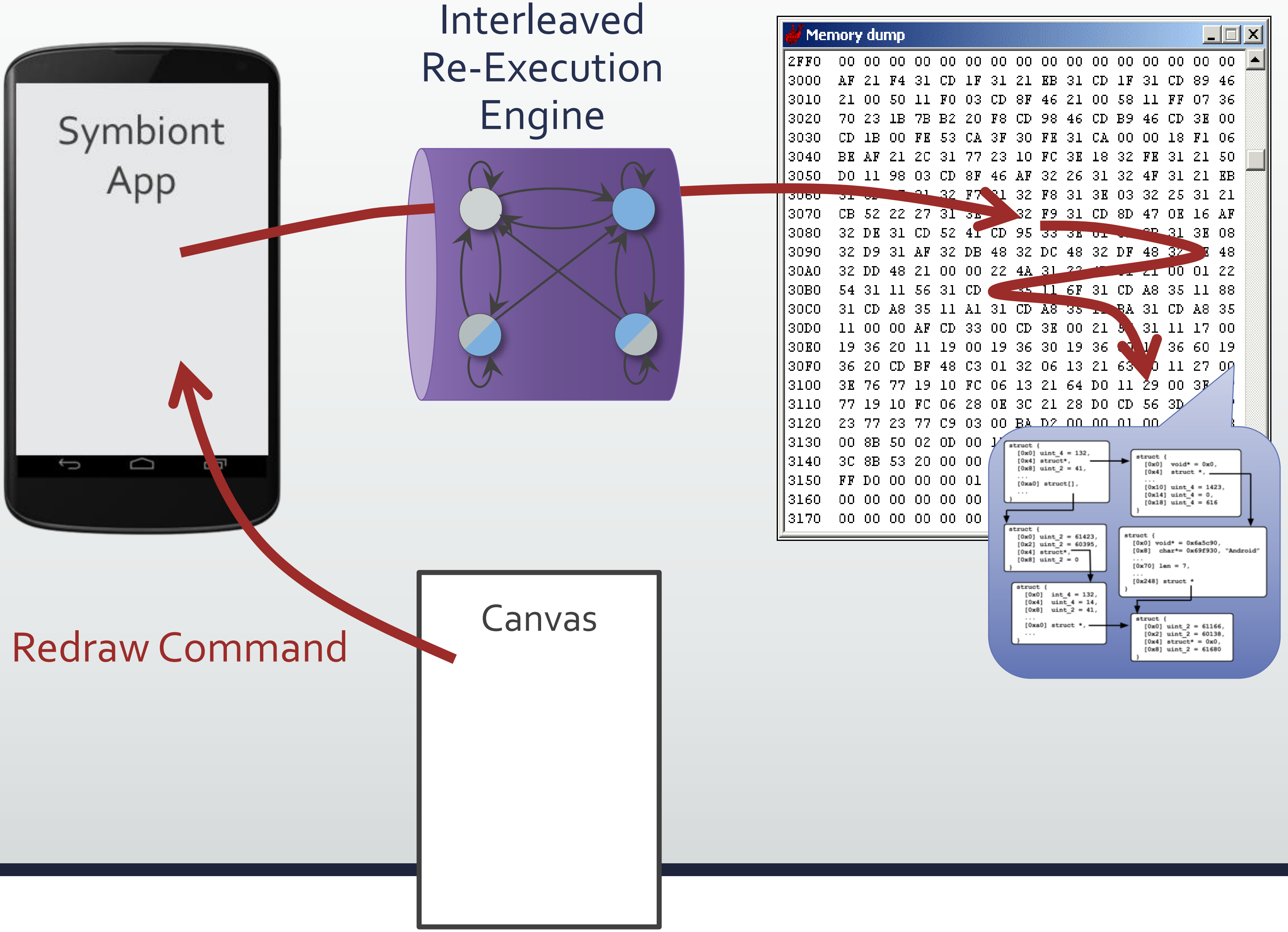
```
2FF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000   AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010   21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020   70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030   CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040   BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050   D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060   31 [illegible] [illegible] [illegible] 32 F7 [illegible] 32 F8 31 3E 03 32 25 31 21
3070   CB 52 22 27 31 3E [illegible] 32 F9 31 CD 8D 47 0E 16 AF
3080   32 DE 31 CD 52 41 CD 95 33 3E 01 32 2B 31 3E 08
3090   32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 32 DE 48
30A0   32 DD 48 21 00 00 22 4A 31 22 4D 31 21 00 01 22
30B0   54 31 11 56 31 CD A8 35 11 6F 31 CD A8 35 11 88
30C0   31 CD A8 35 11 A1 31 CD A8 35 11 BA 31 CD A8 35
30D0   11 00 00 AF CD 33 00 CD 3E 00 21 56 31 11 17 00
30E0   19 36 20 11 19 00 19 36 30 19 36 50 19 36 60 19
30F0   36 20 CD BF 48 C3 01 32 06 13 21 63 D0 11 27 00
3100   3E 76 77 19 10 FC 06 13 21 64 D0 11 29 00 3E 77
3110   77 19 10 FC 06 28 0E 3C 21 28 D0 CD 56 3D C9 77
3120   23 77 23 77 C9
3130   00 8B 50 02 0D
3140   3C 8B 53 20 00
3150   FF D0 00 00 00
3160   00 00 00 00 00
3170   00 00 00 00 00
```

The IRE monitors the state transitions and corrects the execution

Step 4) **Redirect** a redraw command to the Target App



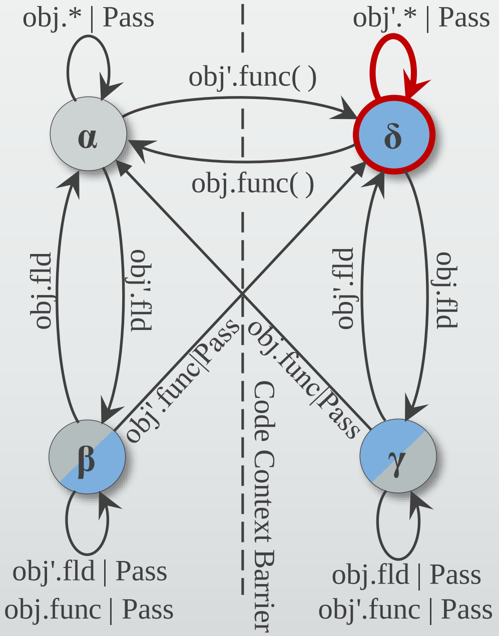
Selective Reanimation



```
2FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000  AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010  21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020  70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030  CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040  BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050  D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060  31 [illegible] [illegible] [illegible] 32 F7 [illegible] 32 F8 31 3E 03 32 25 31 21
3070  CB 52 22 27 31 [illegible] [illegible] 32 F9 31 CD 8D 47 0E 16 AF
3080  32 DE 31 CD 52 41 CD 95 [illegible] [illegible] [illegible] [illegible] [illegible] 31 3E 08
3090  32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 [illegible] [illegible] 48
30A0  32 DD 48 21 00 00 22 4A 31 [illegible] [illegible] [illegible] 21 00 01 22
30B0  54 31 11 56 31 CD [illegible] 11 6F 31 CD A8 35 11 88
30C0  31 CD A8 35 11 A1 31 CD A8 [illegible] [illegible] BA 31 CD A8 35
30D0  11 00 00 AF CD 33 00 CD 3E 00 21 [illegible] 31 11 17 00
30E0  19 36 20 11 19 00 19 36 30 19 36 [illegible] [illegible] 36 60 19
30F0  36 20 CD BF 48 C3 01 32 06 13 21 63 [illegible] 11 27 00
3100  3E 76 77 19 10 FC 06 13 21 64 D0 11 29 00 3E [illegible]
3110  77 19 10 FC 06 28 0E 3C 21 28 D0 CD 56 3D [illegible] [illegible]
3120  23 77 23 77 C9 03 00 BA D2 00 00 01 00 [illegible] [illegible] [illegible]
3130  00 8B 50 02 0D 00 [illegible]
3140  3C 8B 53 20 00 00
3150  FF D0 00 00 00 01
3160  00 00 00 00 00 00
3170  00 00 00 00 00 00
```

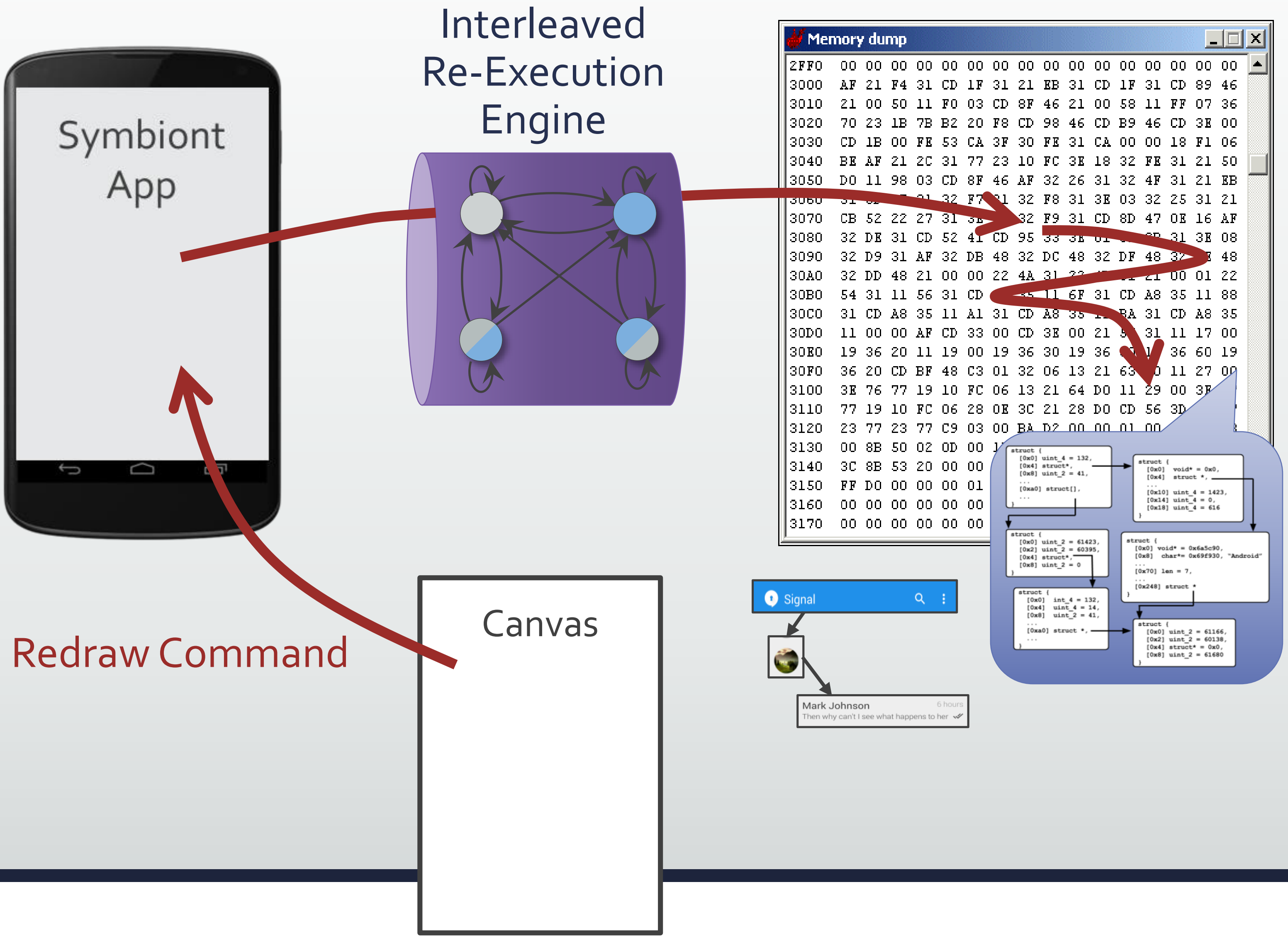
```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}

struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}

struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}

struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}

struct {
  [0x0]  int_4 = 132,
  [0x4]  uint_4 = 14,
  [0x8]  uint_2 = 41,
  ...
  [0xa0] struct *,
  ...
}

struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```

Memory image app's *draw* routines naturally accesses its internal data



PURDUE UNIVERSITY CERIAS

Selective Reanimation



Symbiont App

Interleaved Re-Execution Engine

Redraw Command

Canvas

Memory dump

```
2FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000  AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010  21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020  70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030  CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040  BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050  D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060  31 [illegible] [illegible] [illegible] 32 F7 [illegible] 32 F8 31 3E 03 32 25 31 21
3070  CB 52 22 27 31 [illegible] 32 F9 31 CD 8D 47 0E 16 AF
3080  32 DE 31 CD 52 41 CD 95 [illegible] [illegible] [illegible] [illegible] [illegible] 31 3E 08
3090  32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 [illegible] [illegible] 48
30A0  32 DD 48 21 00 00 22 4A 31 [illegible] [illegible] [illegible] 21 00 01 22
30B0  54 31 11 56 31 CD [illegible] 11 6F 31 CD A8 35 11 88
30C0  31 CD A8 35 11 A1 31 CD A8 35 [illegible] BA 31 CD A8 35
30D0  11 00 00 AF CD 33 00 CD 3E 00 21 [illegible] 31 11 17 00
30E0  19 36 20 11 19 00 19 36 30 19 36 [illegible] [illegible] 36 60 19
30F0  36 20 CD BF 48 C3 01 32 06 13 21 63 [illegible] 11 27 00
3100  3E 76 77 19 10 FC 06 13 21 64 D0 11 29 00 3E
3110  77 19 10 FC 06 28 0E 3C 21 28 D0 CD 56 3D
3120  23 77 23 77 C9 03 00 BA D2 00 00 01 00
3130  00 8B 50 02 0D 00
3140  3C 8B 53 20 00 00
3150  FF D0 00 00 00 01
3160  00 00 00 00 00 00
3170  00 00 00 00 00 00
```

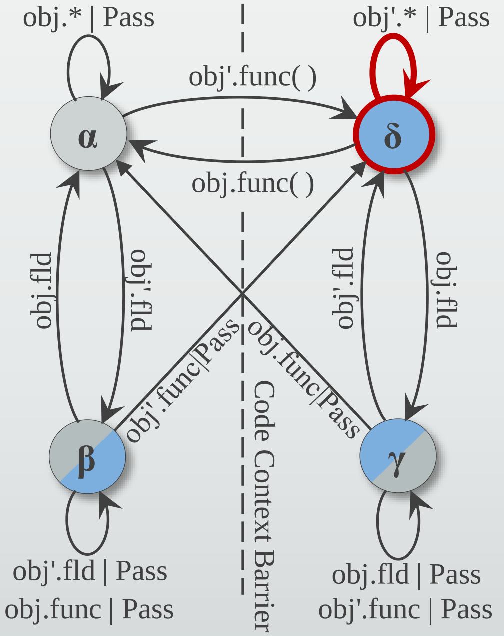
```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}

struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}

struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}

struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}

struct {
  [0x0]  int_4 = 132,
  [0x4]  uint_4 = 14,
  [0x8]  uint_2 = 41,
  ...
  [0xa0] struct *,
  ...
}

struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```

Signal

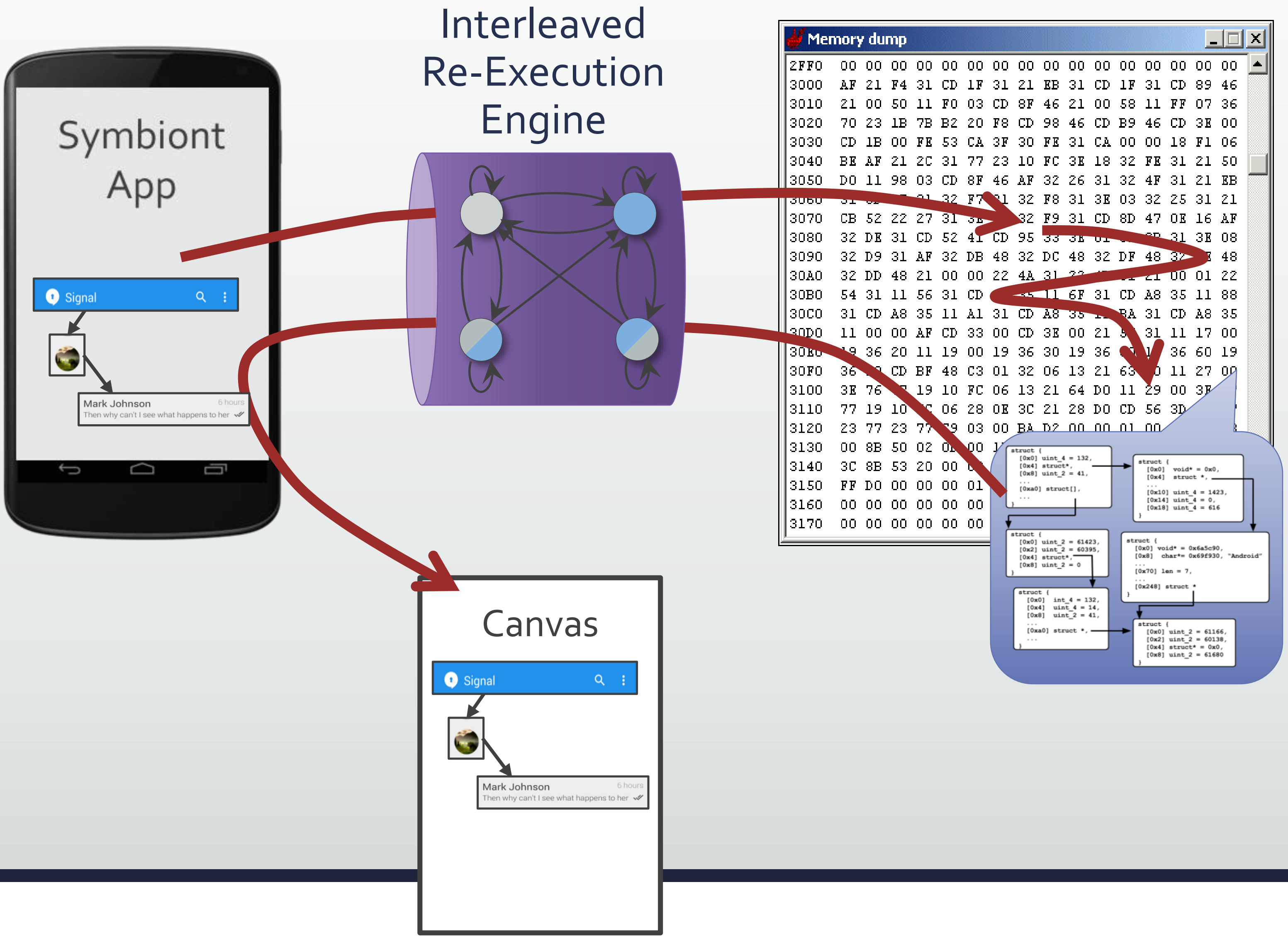
Mark Johnson 6 hours

Then why can't I see what happens to her

Memory image app's *draw* routines naturally accesses its internal data



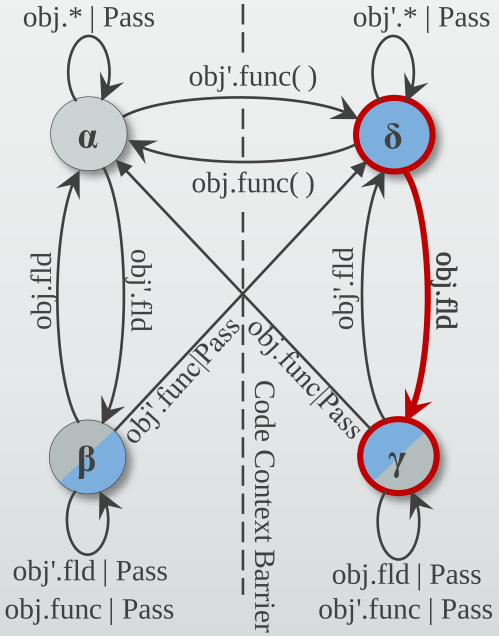
Selective Reanimation



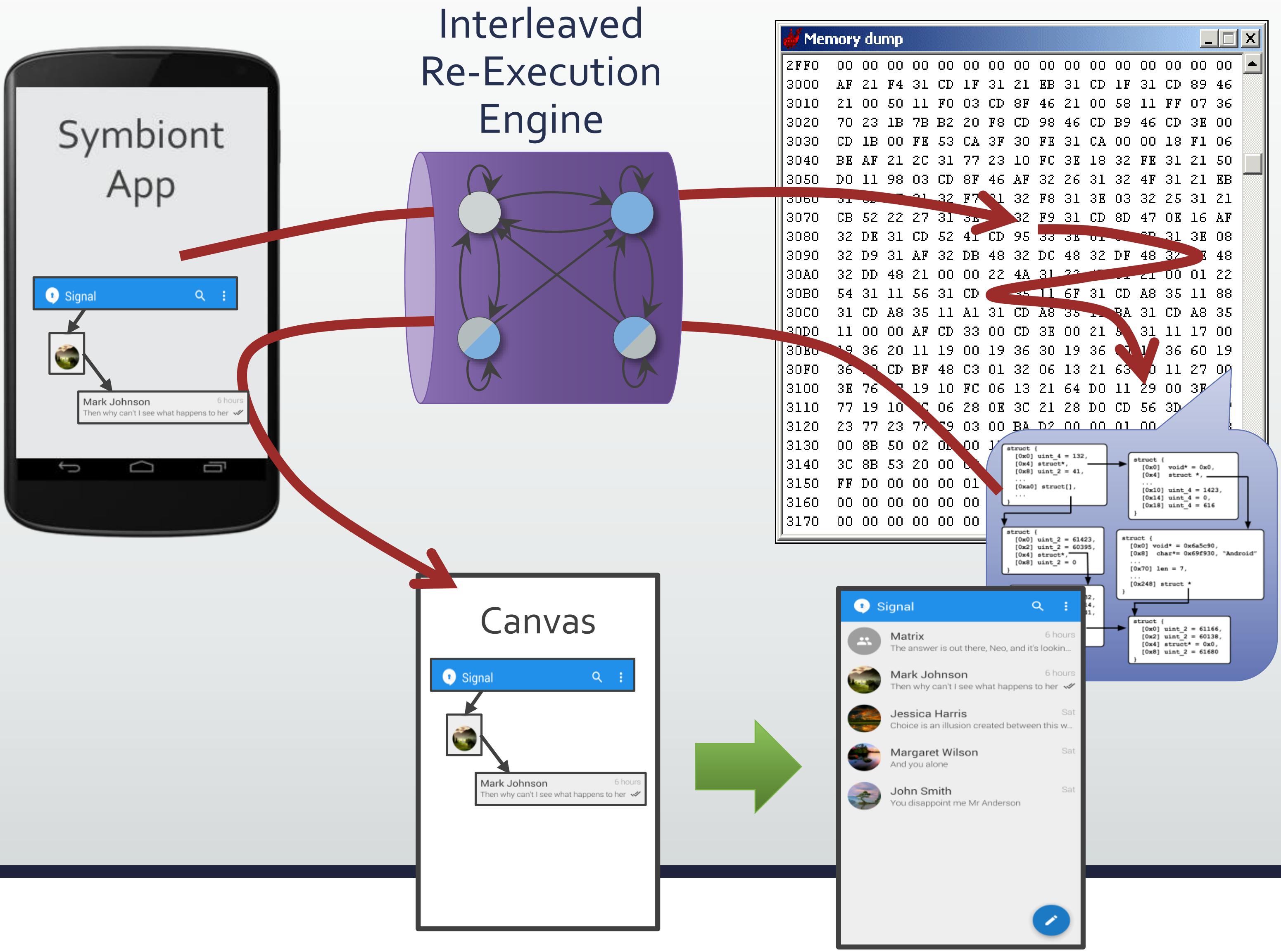
```
2FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000  AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010  21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020  70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030  CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040  BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050  D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060  31 [illegible] [illegible] 31 32 F7 31 32 F8 31 3E 03 32 25 31 21
3070  CB 52 22 27 31 3E [illegible] 32 F9 31 CD 8D 47 0E 16 AF
3080  32 DE 31 CD 52 41 CD 95 33 3E 01 [illegible] [illegible] 31 3E 08
3090  32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 32 [illegible] 48
30A0  32 DD 48 21 00 00 22 4A 31 [illegible] [illegible] [illegible] 21 00 01 22
30B0  54 31 11 56 31 CD [illegible] 35 11 6F 31 CD A8 35 11 88
30C0  31 CD A8 35 11 A1 31 CD A8 35 [illegible] BA 31 CD A8 35
30D0  11 00 00 AF CD 33 00 CD 3E 00 21 [illegible] 31 11 17 00
30E0  19 36 20 11 19 00 19 36 30 19 36 [illegible] [illegible] 36 60 19
30F0  36 [illegible] CD BF 48 C3 01 32 06 13 21 63 [illegible] 11 27 00
3100  3E 76 [illegible] 19 10 FC 06 13 21 64 D0 11 29 00 3E [illegible]
3110  77 19 10 [illegible] 06 28 0E 3C 21 28 D0 CD 56 3D [illegible]
3120  23 77 23 77 [illegible] 03 00 BA D2 00 00 01 00 [illegible]
3130  00 8B 50 02 [illegible] 00 [illegible]
3140  3C 8B 53 20 00 [illegible]
3150  FF D0 00 00 00 01
3160  00 00 00 00 00 00
3170  00 00 00 00 00 00
```

```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}

struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}

struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}

struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}

struct {
  [0x0]  int_4 = 132,
  [0x4]  uint_4 = 14,
  [0x8]  uint_2 = 41,
  ...
  [0xa0] struct *,
  ...
}

struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```

IRE ensures that function calls to the new canvas are directed to the live GUI system



Selective Reanimation



```
2FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000  AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010  21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020  70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030  CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040  BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050  D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060  [illegible] 32 F7 [illegible] 32 F8 31 3E 03 32 25 31 21
3070  CB 52 22 27 31 [illegible] 32 F9 31 CD 8D 47 0E 16 AF
3080  32 DE 31 CD 52 41 CD 95 33 3E 01 [illegible] 31 3E 08
3090  32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 32 [illegible] 48
30A0  32 DD 48 21 00 00 22 4A 31 [illegible] 21 00 01 22
30B0  54 31 11 56 31 CD [illegible] 11 6F 31 CD A8 35 11 88
30C0  31 CD A8 35 11 A1 31 CD A8 35 [illegible] BA 31 CD A8 35
30D0  11 00 00 AF CD 33 00 CD 3E 00 21 [illegible] 31 11 17 00
30E0  19 36 20 11 19 00 19 36 30 19 36 [illegible] 36 60 19
30F0  36 [illegible] CD BF 48 C3 01 32 06 13 21 63 [illegible] 11 27 00
3100  3E 76 [illegible] 19 10 FC 06 13 21 64 D0 11 29 00 3E
3110  77 19 10 [illegible] 06 28 0E 3C 21 28 D0 CD 56 3D
3120  23 77 23 77 [illegible] 03 00 BA D2 00 00 01 00
3130  00 8B 50 02 [illegible] 00
3140  3C 8B 53 20 00
3150  FF D0 00 00 00 01
3160  00 00 00 00 00 00
3170  00 00 00 00 00 00
```

```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}

struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}

struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}

struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}

struct {
  [0x0] uint_2 = 61166,
  [0x2] uint_2 = 60138,
  [0x4] struct* = 0x0,
  [0x8] uint_2 = 61680
}
```

Signal

Matrix — 6 hours
The answer is out there, Neo, and it's lookin...

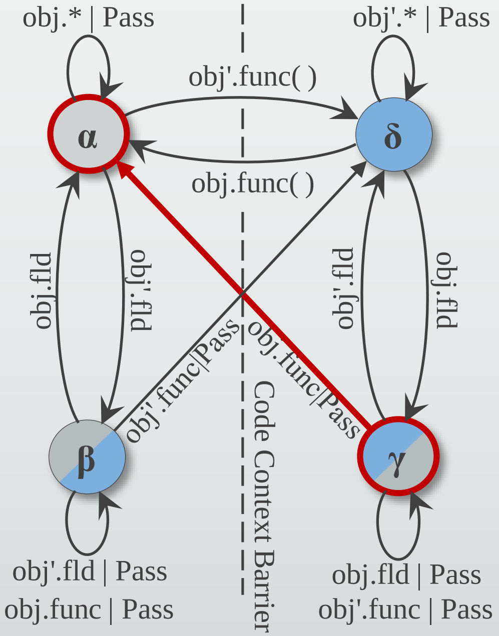
Mark Johnson — 6 hours
Then why can't I see what happens to her

Jessica Harris — Sat
Choice is an illusion created between this w...

Margaret Wilson — Sat
And you alone

John Smith — Sat
You disappoint me Mr Anderson

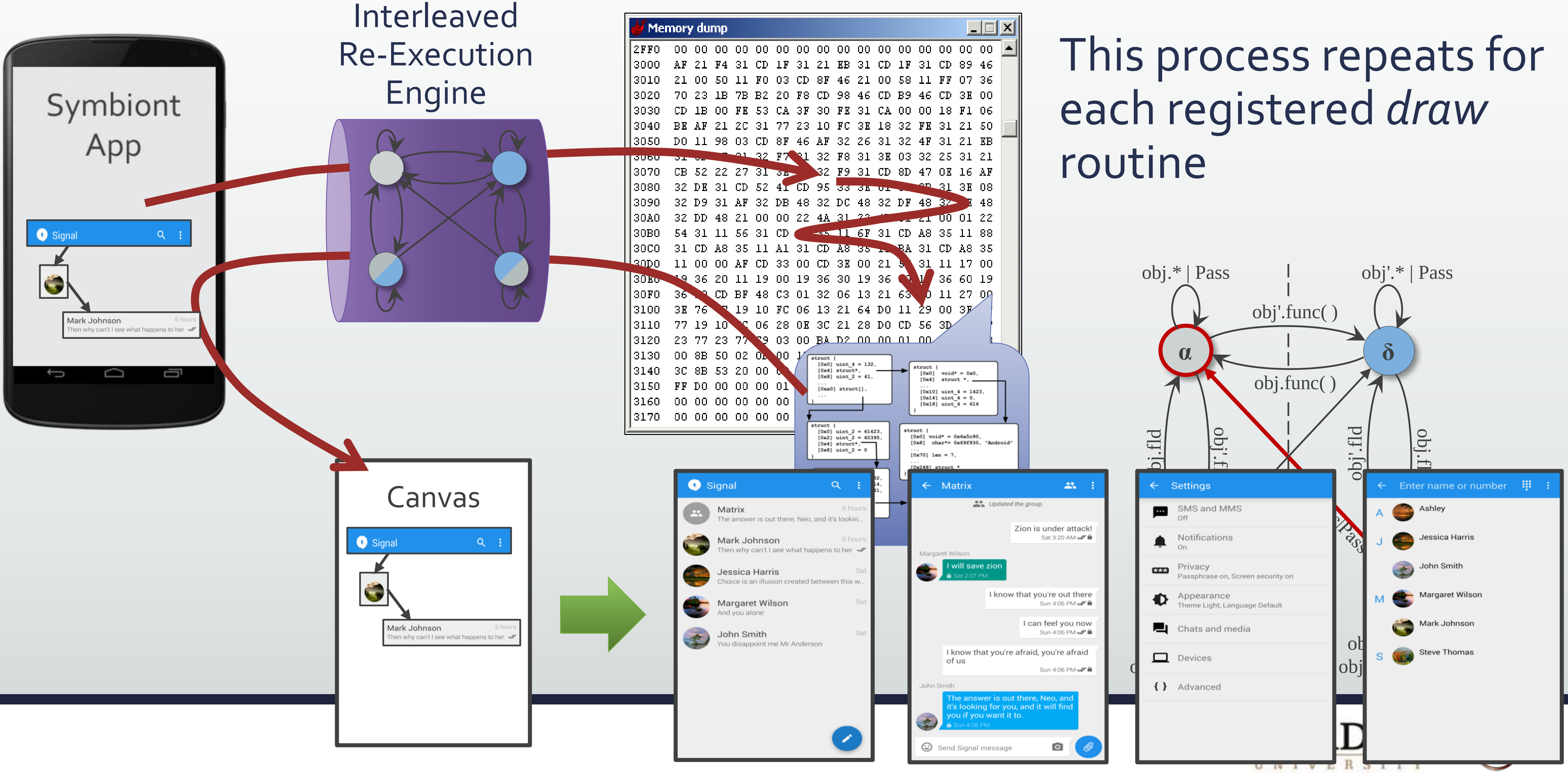
The newly filled Canvas is rendered by the live GUI system and saved



PURDUE UNIVERSITY CERIAS

Selective Reanimation

This process repeats for each registered *draw* routine



Memory dump

```
2FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000  AF 21 F4 31 CD 1F 31 21 EB 31 CD 1F 31 CD 89 46
3010  21 00 50 11 F0 03 CD 8F 46 21 00 58 11 FF 07 36
3020  70 23 1B 7B B2 20 F8 CD 98 46 CD B9 46 CD 3E 00
3030  CD 1B 00 FE 53 CA 3F 30 FE 31 CA 00 00 18 F1 06
3040  BE AF 21 2C 31 77 23 10 FC 3E 18 32 FE 31 21 50
3050  D0 11 98 03 CD 8F 46 AF 32 26 31 32 4F 31 21 EB
3060  31 [illegible] [illegible] 31 32 F7 [illegible] 32 F8 31 3E 03 32 25 31 21
3070  CB 52 22 27 31 3E [illegible] 32 F9 31 CD 8D 47 0E 16 AF
3080  32 DE 31 CD 52 41 CD 95 33 3E 01 [illegible] [illegible] 31 3E 08
3090  32 D9 31 AF 32 DB 48 32 DC 48 32 DF 48 [illegible] [illegible] 48
30A0  32 DD 48 21 00 00 22 4A 31 [illegible] [illegible] [illegible] 21 00 01 22
30B0  54 31 11 56 31 CD [illegible] 35 11 6F 31 CD A8 35 11 88
30C0  31 CD A8 35 11 A1 31 CD A8 35 11 BA 31 CD A8 35
30D0  11 00 00 AF CD 33 00 CD 3E 00 21 [illegible] 31 11 17 00
30E0  19 36 20 11 19 00 19 36 30 19 36 [illegible] [illegible] 36 60 19
30F0  36 [illegible] CD BF 48 C3 01 32 06 13 21 63 [illegible] 11 27 00
3100  3E 76 [illegible] 19 10 FC 06 13 21 64 D0 11 29 00 3E
3110  77 19 10 [illegible] 06 28 0E 3C 21 28 D0 CD 56 3D
3120  23 77 23 77 [illegible] 03 00 BA D2 00 00 01 00
3130  00 8B 50 02 [illegible] 00
3140  3C 8B 53 20 00
3150  FF D0 00 00 00 01
3160  00 00 00 00 00 00
3170  00 00 00 00 00 00
```

```
struct {
  [0x0] uint_4 = 132,
  [0x4] struct*,
  [0x8] uint_2 = 41,
  ...
  [0xa0] struct[],
  ...
}

struct {
  [0x0]  void* = 0x0,
  [0x4]  struct *,
  ...
  [0x10] uint_4 = 1423,
  [0x14] uint_4 = 0,
  [0x18] uint_4 = 616
}

struct {
  [0x0] uint_2 = 61423,
  [0x2] uint_2 = 60395,
  [0x4] struct*,
  [0x8] uint_2 = 0
}

struct {
  [0x0] void* = 0x6a5c90,
  [0x8]  char*= 0x69f930, "Android"
  ...
  [0x70] len = 7,
  ...
  [0x248] struct *
}
```

Signal

Matrix — 6 hours
The answer is out there, Neo, and it's lookin...

Mark Johnson — 6 hours
Then why can't I see what happens to her

Jessica Harris — Sat
Choice is an illusion created between this w...

Margaret Wilson — Sat
And you alone

John Smith — Sat
You disappoint me Mr Anderson

Matrix

Updated the group.

Zion is under attack!
Sat 3:20 AM

Margaret Wilson
I will save zion
Sat 2:07 PM

I know that you're out there
Sun 4:06 PM

I can feel you now
Sun 4:06 PM

I know that you're afraid, you're afraid of us
Sun 4:06 PM

John Smith
The answer is out there, Neo, and it's looking for you, and it will find you if you want it to.
Sun 4:08 PM

Send Signal message

Settings

SMS and MMS
Off

Notifications
On

Privacy
Passphrase on, Screen security on

Appearance
Theme Light, Language Default

Chats and media

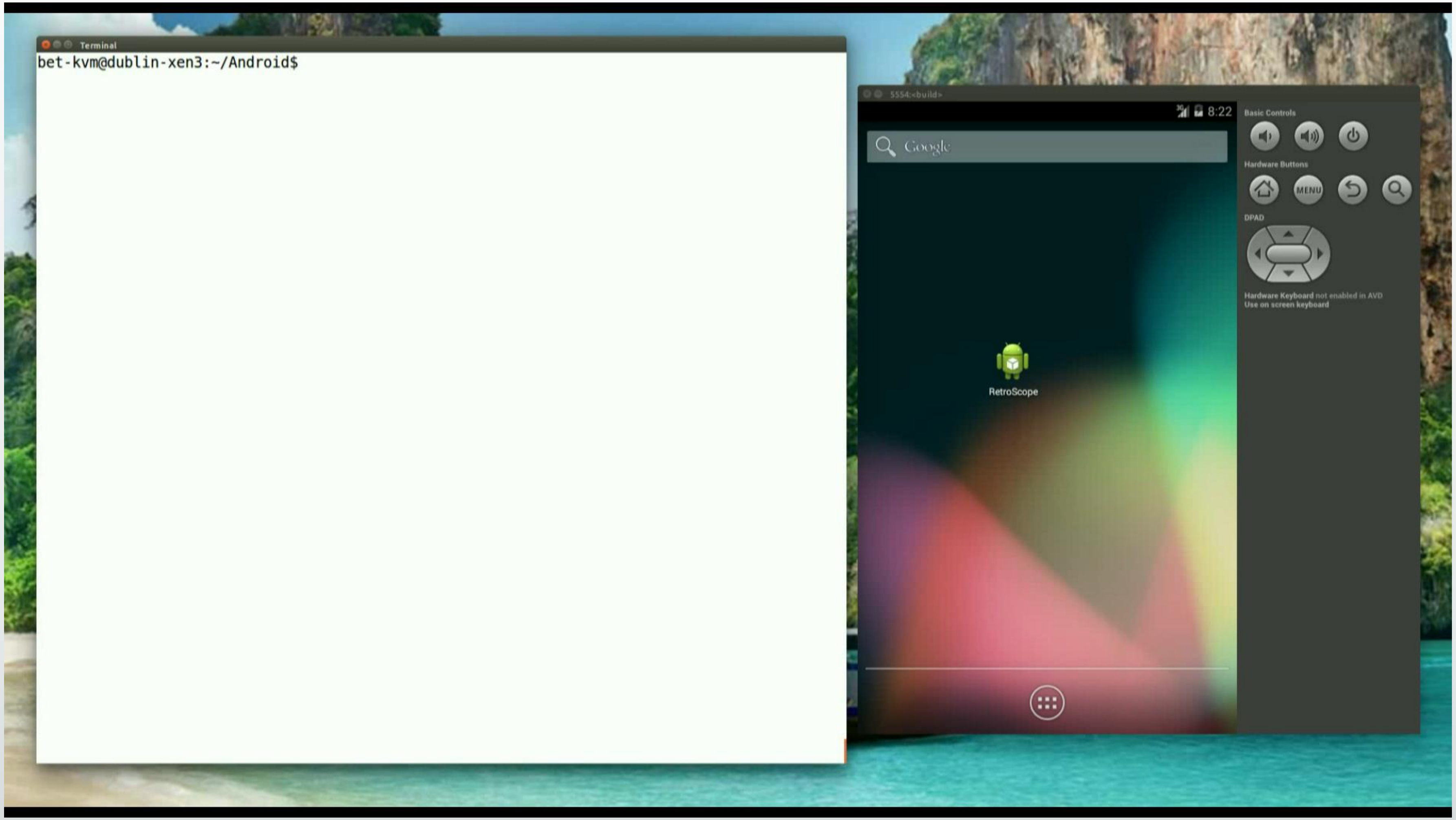
Devices

Advanced

Enter name or number

A Ashley
J Jessica Harris
John Smith
M Margaret Wilson
Mark Johnson
S Steve Thomas

Breaking The Case Wide Open!



```
bet-kvm@dublin-xen3:~/Android$
```

Evaluation

15 Apps on 3 “Suspect” Devices: HTC One, LG G3, Samsung Galaxy S4

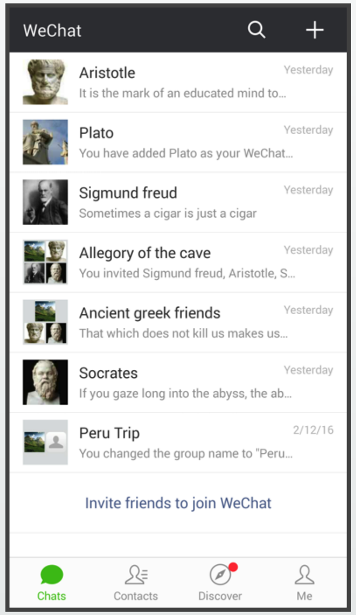
HTC One
(More In Paper)

App	Screens Recovered	Ground Truth (lower bound)	Byte Code Inst. Re-Executed	New Java Objects	New C/C++ Structures
Calendar	6	6	197316	732	102642
Chas			584587	2091	266965
Cont			190847	723	71578
Face			382522	1451	95516
Gma			235973	929	129804
Instagram	3	3	86829	433	42037
Messaging	4	4	93971	287	45085
TextSecure	7	8	231891	924	98571
WhatsApp	6	6	321229	1571	104216

Average of:
41,078 Byte-Code Instructions,
158 New Java Objects, and
13,535 New C/C++ Structures
Per Screen

Case 1: WeChat (And Others) Deleted Messages

Screen -4


WeChat

Aristotle — Yesterday
It is the mark of an educated mind to...

Plato — Yesterday
You have added Plato as your WeChat...

Sigmund freud — Yesterday
Sometimes a cigar is just a cigar

Allegory of the cave — Yesterday
You invited Sigmund freud, Aristotle, S...

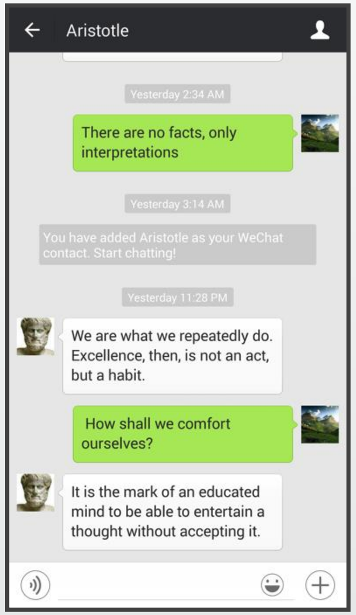
Ancient greek friends — Yesterday
That which does not kill us makes us...

Socrates — Yesterday
If you gaze long into the abyss, the ab...

Peru Trip — 2/12/16
You changed the group name to "Peru...

Invite friends to join WeChat

Screen -3


Aristotle

Yesterday 2:34 AM

There are no facts, only interpretations

Yesterday 3:14 AM

You have added Aristotle as your WeChat contact. Start chatting!

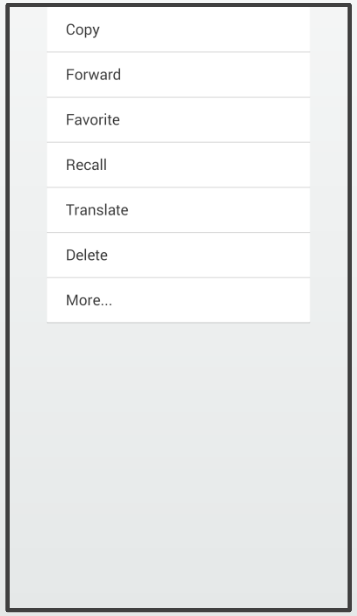
Yesterday 11:28 PM

We are what we repeatedly do. Excellence, then, is not an act, but a habit.

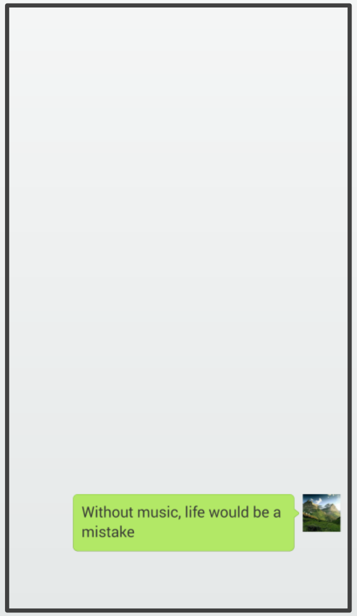
How shall we comfort ourselves?

It is the mark of an educated mind to be able to entertain a thought without accepting it.

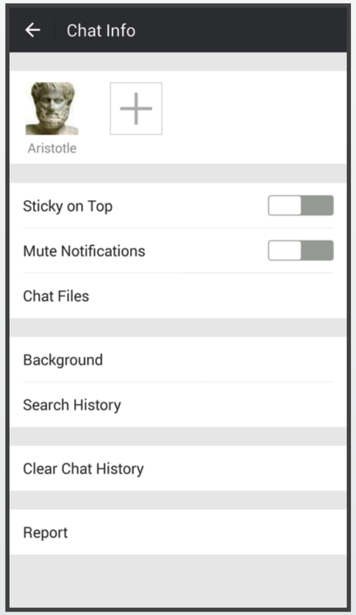
Screen -2



Screen -1


Without music, life would be a mistake

Screen 0

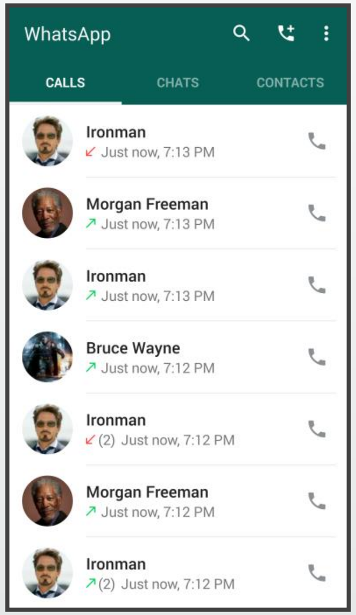

Chat Info

Aristotle

From LG G3 Device

Case 2: WhatsApp Background Update

Screen -5



WhatsApp

CALLS | CHATS | CONTACTS

Ironman
↙ Just now, 7:13 PM

Morgan Freeman
↗ Just now, 7:13 PM

Ironman
↗ Just now, 7:13 PM

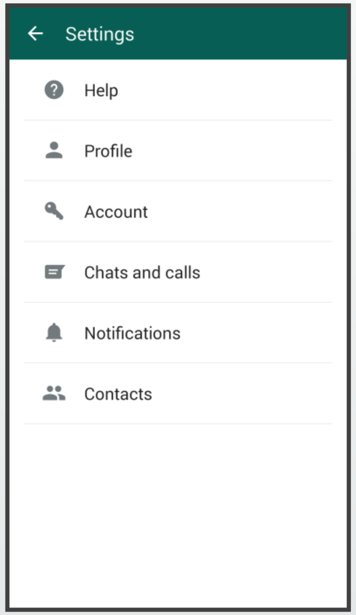
Bruce Wayne
↗ Just now, 7:12 PM

Ironman
↙ (2) Just now, 7:12 PM

Morgan Freeman
↗ Just now, 7:12 PM

Ironman
↗ (2) Just now, 7:12 PM

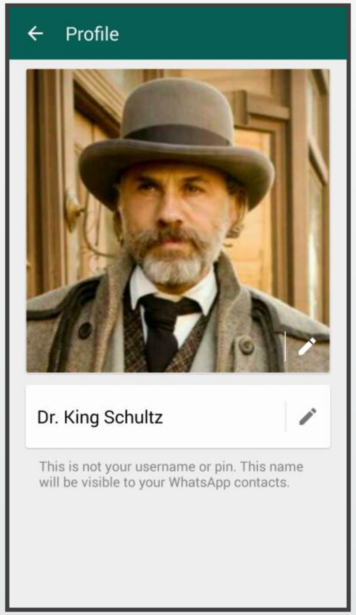
Screen -4



← Settings

- Help
- Profile
- Account
- Chats and calls
- Notifications
- Contacts

Screen -3

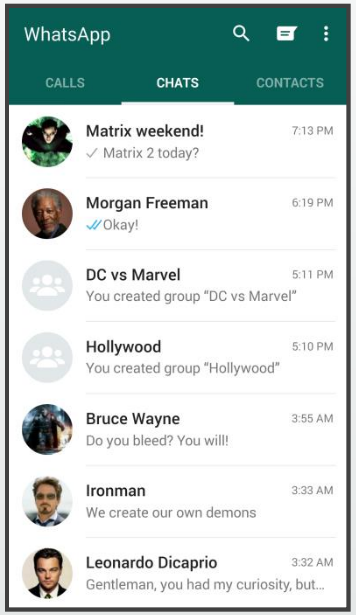


← Profile

Dr. King Schultz

This is not your username or pin. This name will be visible to your WhatsApp contacts.

Screen -2



WhatsApp

CALLS | CHATS | CONTACTS

Matrix weekend! 7:13 PM
✓ Matrix 2 today?

Morgan Freeman 6:19 PM
✓✓ Okay!

DC vs Marvel 5:11 PM
You created group "DC vs Marvel"

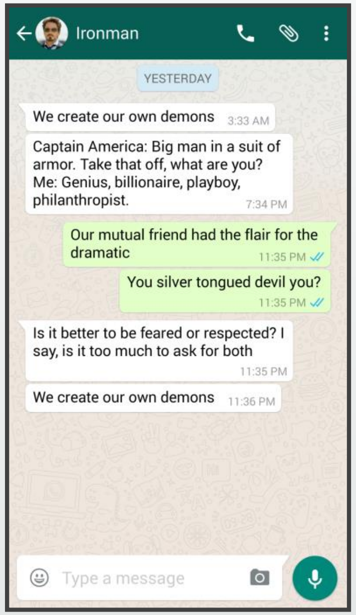
Hollywood 5:10 PM
You created group "Hollywood"

Bruce Wayne 3:55 AM
Do you bleed? You will!

Ironman 3:33 AM
We create our own demons

Leonardo Dicaprio 3:32 AM
Gentleman, you had my curiosity, but...

Screen -1



← Ironman

YESTERDAY

We create our own demons 3:33 AM

Captain America: Big man in a suit of armor. Take that off, what are you?
Me: Genius, billionaire, playboy, philanthropist. 7:34 PM

Our mutual friend had the flair for the dramatic 11:35 PM ✓✓

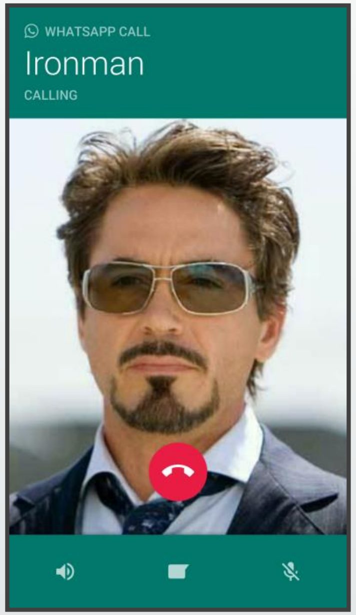
You silver tongued devil you? 11:35 PM ✓✓

Is it better to be feared or respected? I say, is it too much to ask for both 11:35 PM

We create our own demons 11:36 PM

Type a message

Screen 0

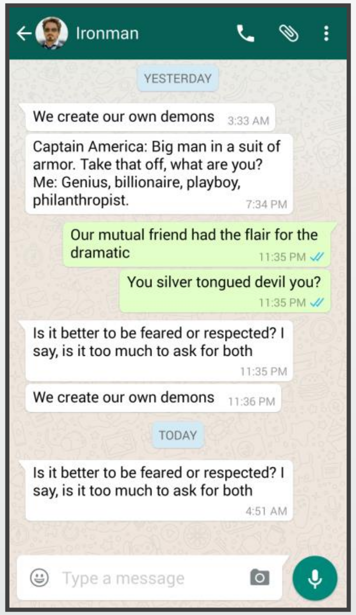


WHATSAPP CALL

Ironman

CALLING

Screen +1



← Ironman

YESTERDAY

We create our own demons 3:33 AM

Captain America: Big man in a suit of armor. Take that off, what are you?
Me: Genius, billionaire, playboy, philanthropist. 7:34 PM

Our mutual friend had the flair for the dramatic 11:35 PM ✓✓

You silver tongued devil you? 11:35 PM ✓✓

Is it better to be feared or respected? I say, is it too much to ask for both 11:35 PM

We create our own demons 11:36 PM

TODAY

Is it better to be feared or respected? I say, is it too much to ask for both 4:51 AM

Type a message

From Samsung Galaxy S4 Device

Related Works

B. Saltaformaggio, Z. Gu, X. Zhang, and D. Xu. DSCRETE: Automatic Rendering of Forensic Information from Memory Images via Application Logic Reuse. In Proc. USENIX Security, 2014. Best Student Paper.

M. Carbone, W. Cui, L. Lu, W. Lee, M. Peinado, and X. Jiang. Mapping kernel objects to enable systematic integrity checking. In Proc. CCS, 2009.

B. Dolan-Gavitt, A. Srivastava, P. Traynor, and J. Giffin. Robust signatures for kernel data structures. In Proc. CCS, 2009.

J. Lee, T. Avgerinos, and D. Brumley. TIE: Principled reverse engineering of types in binary programs. In Proc. NDSS, 2011.

A. Slowinska, T. Stancescu, and H. Bos. Howard: A dynamic excavator for reverse engineering data structures. In Proc. NDSS, 2011.

R. Walls, B. N. Levine, and E. G. Learned-Miller. Forensic triage for mobile phones with DECoDE. In Proc. USENIX Security, 2011.

Conclusion

RetroScope represents a new paradigm of **spatial-temporal** memory forensics for app GUI screens

RetroScope's novel IRE selectively reanimates an app's screen redrawing functionality **without** any app-specific knowledge

Recovers visually accurate, temporally ordered screens (ranging from 3 to 11 screens) for a wide variety of **privacy-sensitive apps**

Thank you!
Questions?

Brendan Saltaformaggio
bsaltafo@cs.purdue.edu

Privacy Implications of RetroScope?

The privacy-sensitive apps are not broken, per se

- Unlike disk or network, memory is assumed private
- Little incentive to "protect" memory
- E.g., Malware in your app's memory = all bets are off

RetroScope is just emulating the standard behavior of Android

- To disrupt RetroScope would also hinder an app's ability to draw screens
- Encrypting memory doesn't work because RetroScope would reanimate the decryption logic
- Privacy vs. Usability
  - E.g., Zeroing data would require getting it back in order to redraw (slowing down the UI)

Citizens' privacy is protected by strict legal protocols and regulations (see [9,21])

- Search warrants & strict chain of custody documentation prior to performing "invasive" forensics