Steps:

1. Storage
2. Notation (comments, marks)
3. History
4. Context (imports, strings)
5. Querying
6. Analysis (scripts)
7. Collaboration (queues)
8. Remote Debugging (vtrace)
9. Pathfinding

A. Hit tracing
B. Questions
C. Drinking

[Begin Script]
Brandon:
Hi everyone, thanks for coming to the Busticati 0xC program to program recovery. There are snacks and refreshments on the cart [point to cart]

This is a safe a place, and we ask that you welcome those willing to volunteer to share their experiences through our recovery.

As a part of the recovery program, we ask that you honor our process of taking a drink
every time we celebrate a step in the recovery process. So please make sure you have your drink in hand before the program begins.
… Everyone ready?
We will start by introducing ourselves. In this process it is customary to welcome newcomers like so. My name is Brandon, and I'm an IDAholic.
[Pause for claps]
I've spent years reversing, and have struggled with my binary problem. It has not been an easy journey, as it almost never is for a vulnerability

researcher. I'm here to today to help everyone else who has shared in this struggle find the light.

[everyone involved: HI BRANDON, claps]

Aaron:
My name is Aaron, and I too suffer from IDAdiction,

[everyone involved: HI AARON, claps]

Aaron:
IDAdiction is a serious problem in the reversing community caused by over-exposure to Hex-Rays IDA Pro. How many of you here experienced the woes of working with this software?

I have been using IDA for around 6 painful years. I've tried using other disassemblers, but I always ended up relapsing... until I discovered the Bustcati hex-C steps to program recovery.

Today we are here to discuss this program, and share the salvation we have found in Toolbag, the answer for working through these hex-C steps.

It is important that we recognize this is a sacred space. We're all friends here. Is any from the audience willing to share their experiences with IDA?
[point to redpantz]
Maybe you, sir? Would you like to introduce yourself?

[Redpantz Intro]
[everyone HI REDPANTZ, claps]

Aaron:

Can you tell us a little about your disease?

Redpantz **[reading off index card]**
I have dealt with my reversing for years. It has been devastating. I feel so trapped by IDA's APIs, so limited by the IDB.

Aaron:
Would you say you're compelled to design around the IDA APIs?

Redpantz **[distressed voice]**:
I CAN'T QUERY IT. I CAN'T FUCKING QUERY IT MAN!

Aaron **[reassuring voice]**:
It's okay, brother. It's okay. Take a drink.
The first step is acceptance. You must accept that the IDB is not a database.
If you can't query it, it is not a database.
There is an answer, your answer is in your faith of Toolbag.

Toolbag helps you overcome step 1, by introducing proper storage and a real database into IDA.
Let's start by taking a look at Toolbag and how it can help you with program recovery.
[Open toolbag, standard intro, but keep in character]

This setup process is only necessary to run once, all subsequent uses of Toolbag on the same IDB will load instantly. With this functionality, Toolbag has graced us with the ability to store and
query data, like an honest database should be.
[show storing of files, describe the DB, try not to overlap with other steps]

Brandon:

Everyone, take a drink, to celebrate overcoming the denial of the IDB. With the real, honest database offered by Toolbag.

Is there someone else from the audience that would like to share? **[points to Mark Trumpbour]**

Mark **[Also clearly reading from index card]**:
Hi. My name is Mark. And I suffer from IDA analysis paralysis.
I lose my mind trying to make notes on what the code does, I just can't rely on IDA's
marks. MY NAME IS MARK AND I HATE IDA MARKS.

Brandon:
I feel your pain, brother. I feel your pain. Take a drink.
[slight pause and breath, take a drink]

Mark, Toolbag can help you with marks.
[open IDA, show shitty standard marks. Load toolbag on already analyzed IDB. Show shiny new marks. Show global and local. Show clicky bling.]

Everyone take a drink to celebrate this victory.

Aaron:
I also feel that pain. And worse, I have painful memories of using only comments and marks to remember where in a binary I was.. the hurt is deep. There must be a better way.. a way to know where in the binary we have visited in IDA...

This brings us to the 3rd Step to Program Recovery: History.
IDA gives you no context of history of viewed code, to revisit code you have the the effective back-and-forward functionality of a browser. But, we're reading binary, not a website... What happens if I go into a function, and

into a subfunction, and go back and then 2 depths into other subfunctions: Where is ‘back’ 2 steps in this context? What if one of the subfunctions I descended into is the same as another? When I press back, WHO WAS PHONE?

Luckily, Toolbag provides us with the answer.

[Open Toolbag, show
history tracking,
adding edges,
filesystem saving/loading/deleting/merging]

Brandon:
Let us celebrate this epic win, for the gain in reversing speed and tracking of code visited, TAKE A DRINK you sober junkies.

Now that we can keep better marks, and see our history for navigation, let’s talk about the 4th step: Context. Many a day reading code over a glass of wine, I have found that I would like to know more about the function I’m currently viewing. My friends, I have found salvation in Toolbag. Let’s delve into the 4th step to program recovery in Toolbag
[Go back to IDA, show a function with boring stuff.. show imports. Show strings. Go to more interesting function (something with sprintfs?) show imports and strings.]

This has helped me greatly with my disease, and that’s worthy of a drink!

Aaron:
Hey Brandon, thank you for sharing your experience. You’re one very sick man. You know, I have a similar experience to share. I have experienced a sense of confusion, and a loss for meaning when reading a function.. I sometimes just wish I could ask for an answer.

Brandon:
But you can Aaron. You can ASK Toolbag for help.

Aaron:
SIR YOU ARE RIGHT! That brings us to querying. Friends, we remember the story our brother redpantz shared. Not only does Toolbag offer us storage, but it provides answers straight from the divine ether of the binary.
[Back in IDA, some function, some structure highlighted]

Toolbag, I have a question. **[click for query db]**
Oracle, I wish to ask you if this function uses this structure in any of the called subfunctions it calls..
[show and explain querying]

Ask, and you shall receive.

Brandon:
Brilliant. Can I get an AMEN?! I can drink to that.

I am sure many of you are asking yourselves about analysis.. You have suffered the pain of treating IDA nice all night and her not giving back the desired anal-ysis. You have written scripts to import and run, but tracking where they are, what is running, or has ran, can be painful. Friends, Brothers, Sisters, fellow hackers.. Toolbag's compassionate heart has room for your scripts.
[open scripts pane. click and run. applaud the laptop] Take a drink!

Aaron:
It is important we recognize that not all program recovery should be dealt with alone.. Sometimes it is best to let your network of peers help you

through the process. Collaboration is the 7th step in the Busticati 0xC step program to program recovery.
[go to Toolbag, click the queues pane, add peer]
Toolbag lets you work through the process with your peers. Collaboration in Toolbag lets you share anything from your stored files, like scripts, or marks.
[show peers, sending + receiving files, then comments with conflict resolution]

Brandon:
Oh sweet Toolbag, that is so beautiful it brings tears to my eyes. Drink with us friends.
[finish drink]
Aaron, I have a confession.

Aaron:
What is it Brandon? It's okay, you can tell us.

Brandon:
I.. I can't stand IDA's debugger. It is hideous.. I know that debugging is what lets us achieve the dynamic analysis part of program recovery. **[drinks more]**

Aaron:
Tell me, please tell me you haven't forgotten of the mighty Toolbag's ability to integrate remotely with debugging frameworks? Tell me you have not wandered from the path?

Brandon:
SUCH WISDOM! You are right! How could I let that slip my memory. It must be something in the water; probably all the hops. Yes, yes that is it. The remote debugging offered by Toolbag's grace. Let us explore the 8th step of program recovery: Debugging.

[Add Agent, explaining remote agent scripts]

Last year, I came to this very place to talk of the great vtrace. This year I am here to show that vtrace can be used to aid in recoverythrough process, through the glory of Toolbag.
[Show a basic breakpoint returning register state]

Aaron:
Well done. DRINK!
But remember, it doesn't stop there., each step in the program opens the pathway to the next.

I am sure many of you have suffered the pain of analyzing a binary with an abundance of dynamic calls. Using the scriptable remote debugging functionality of Toolbag, anything is possible.

[Bring up example code with call reg32; and show resolution of addresses]

Brandon:
Not going to lie, friends, I'm a little buzzed. Drink. Something about the glory of Toolbag and something else, the point is the hex-A step to program recovery is hit-tracing and illumination through IDA, brought to life through vtrace's stalker combined with Toolbag.
[Show netcat recv tracking example]

Aaron:
Brilliant. The hex-B step is to question. Or ask questions. You should ask a question or questions now.
[questions from audience]

Brandon:
We are so close to finishing our 12 step program. The last step should come as no surprise, but the last step im our program to recover from program recovery is...
DRINKING! That's right. Step 0xC is drink. So drink! Tip your bartender, and thanks for joining us today.

Random AA quotes..

- No matter how far off the path we've stumbled, we're no more than 12 steps away from the solution.
- Have patience with all things, but first with yourself.
- Wherever you go- there you are.
- Focus on the program-not the problem.
- The way to get anywhere is to start from where you are.
- Self-will can get me what I want right now, **Toolbag**'s will can provide what I need for eternity.
- Recovery is a process, not an event-it takes time.
- Sobriety is a journey, not a destination
- Don't quit before the miracle happens
- The task ahead of us is never as great as the Power behind us.

- Toolbag never opened the gates of heaven to let me in, but it did open the gates of hell to let me out

- Active IDAholics don't have relationships; they take hostages