

RekordboxReader / Finding Rekordbox Pointers.md



9001 bpm-search clarifications

3 years ago



87 lines (69 loc) · 9.05 KB

Preview

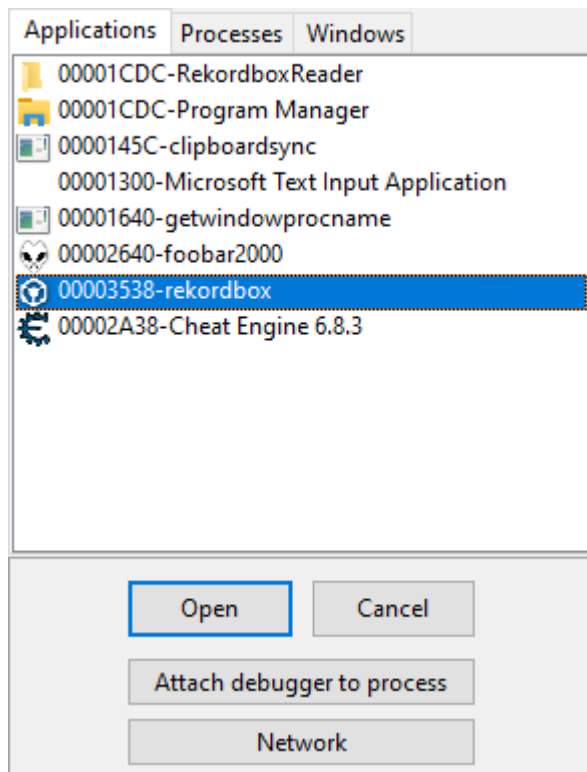
Code

Blame

Raw



- Grab [CheatEngine](#) if you don't already have it.
- In CheatEngine, load the Rekordbox process.

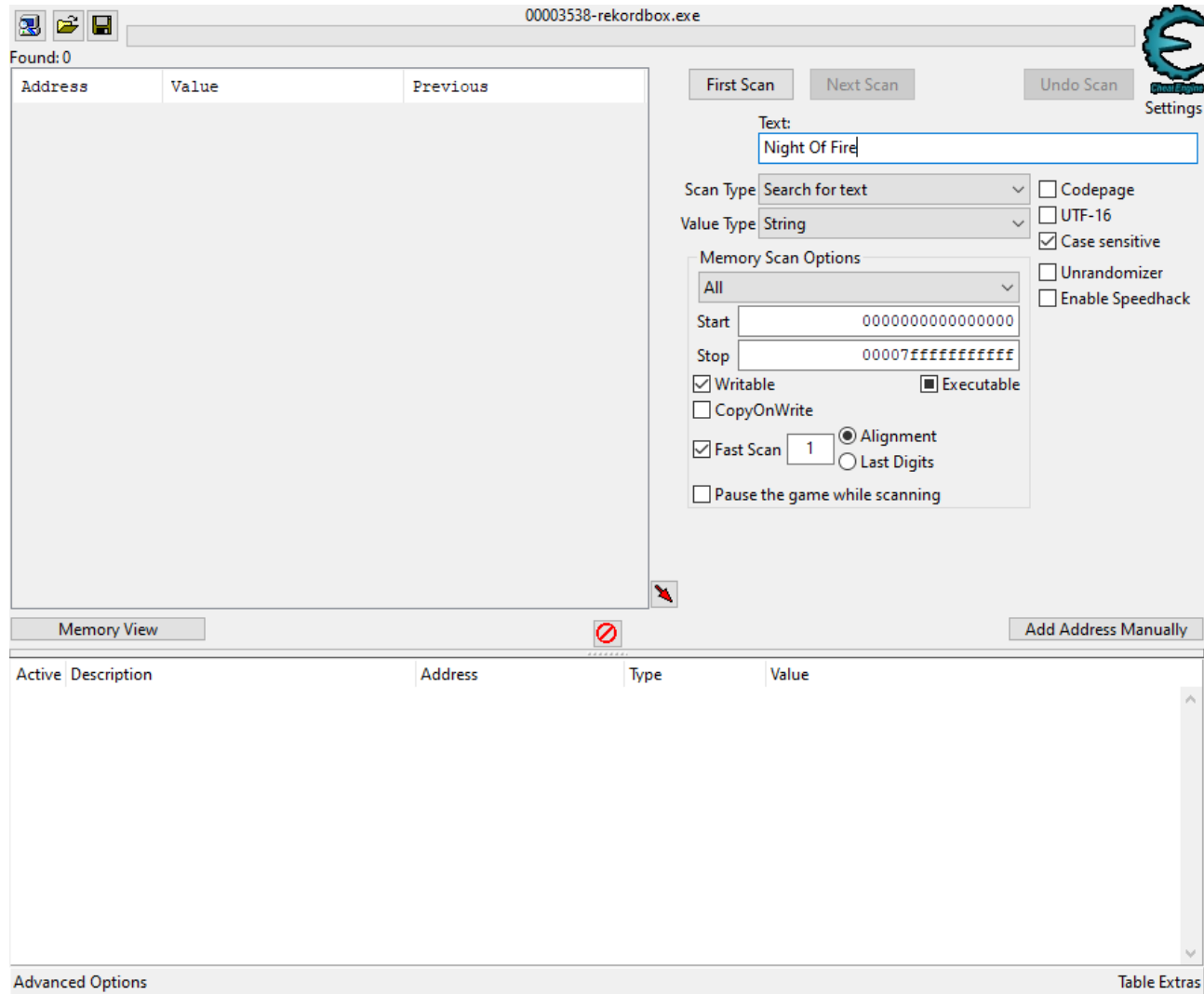


spoiler: you'll want to skip straight to [Finding the Deck Struct via bpm](#) since that JustWorks (it covers artist/title etc)

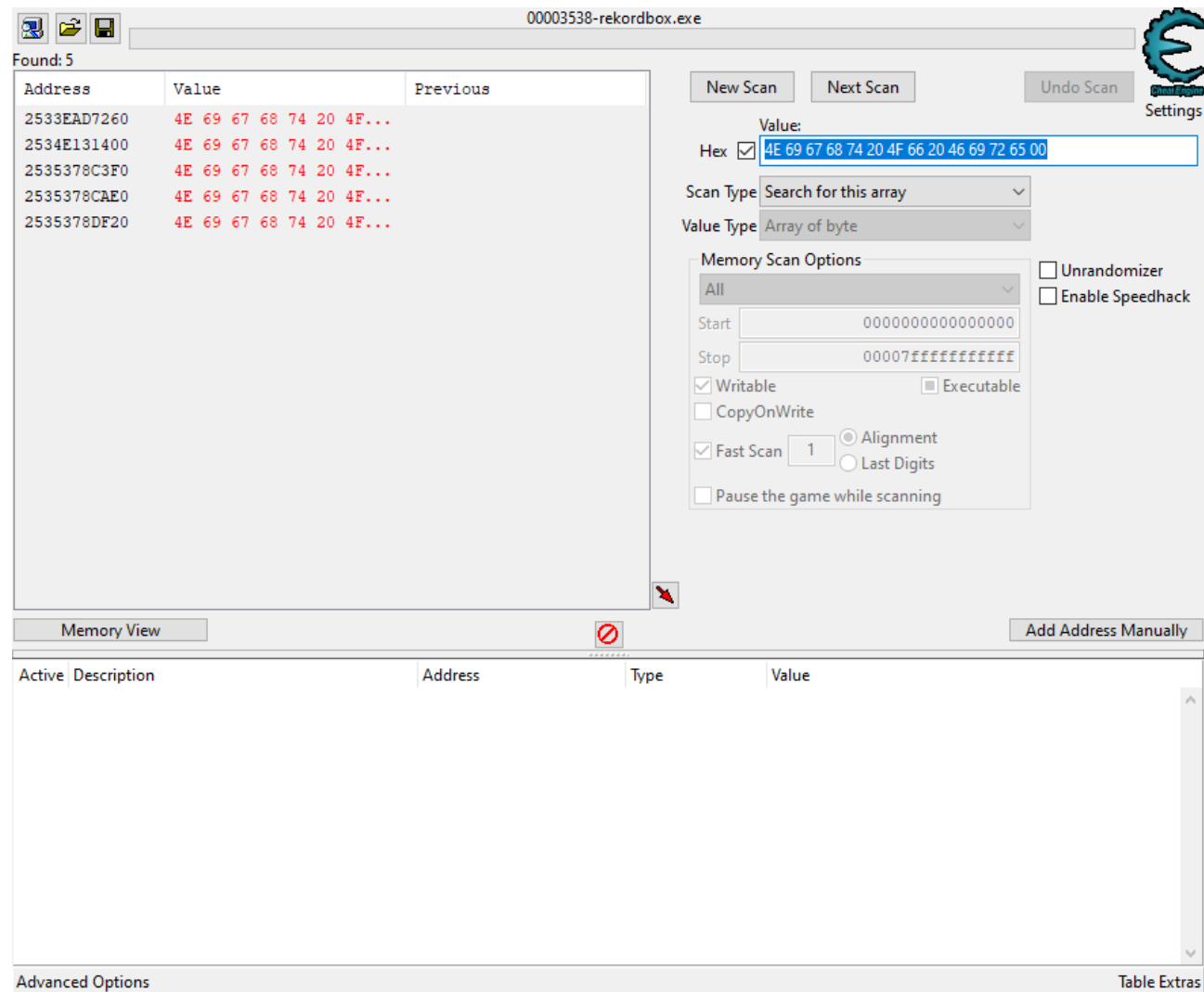
Artist/Title Pointers

- In Rekordbox, load a song into the deck you want to find pointers for.

- On the right half of CheatEngine, set the Value Type to String, and enter the exact song title or artist name loaded into the deck.



- Set the Value Type to Array of byte, add "00" at the end, and click First Scan. Adding "00" to the end of the array filters a lot of false-positive addresses that might have the file name loaded instead.



- Add all addresses found to the list at the bottom by double-clicking them.

Active	Description	Address	Type	Value
<input type="checkbox"/>	No description	2533EAD7260	Array of byte	4E 69 67 68 74 20 4F 66 20 46 69 72 65 00
<input type="checkbox"/>	No description	2534E131400	Array of byte	4E 69 67 68 74 20 4F 66 20 46 69 72 65 00
<input type="checkbox"/>	No description	2535378C3F0	Array of byte	4E 69 67 68 74 20 4F 66 20 46 69 72 65 00
<input type="checkbox"/>	No description	2535378CAE0	Array of byte	4E 69 67 68 74 20 4F 66 20 46 69 72 65 00
<input type="checkbox"/>	No description	2535378DF20	Array of byte	4E 69 67 68 74 20 4F 66 20 46 69 72 65 00

- For each address, right-click and choose "Browser this memory region" and make sure the value is surrounded by mostly garbage data. The first image below is similar to what you want to see. If it looks like the second image below (surrounded by other similar values or file names), it might find a valid pointer but not of the type we are looking for. Remove any bad addresses from the list.

rekordbox.exe+E836B0																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																
Address	Bytes		Opcode		Comment																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																											
rekordbox.exe+E836B0	48	83 EC 28	sub	rsp,28	40																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																											
rekordbox.exe+E836B4	E8	870C0000	call	rekordbox.exe+E84340																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
rekordbox.exe+E836B9	48	83 C4 28	add	rsp,28	40																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																											
rekordbox.exe+E836BD	E9	7AFEFFFF	jmp	rekordbox.exe+E8353C																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
rekordbox.exe+E836C2	CC		int 3																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
rekordbox.exe+E836C3	CC		int 3																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
rekordbox.exe+E836C4	E9	0BF9FFFF	jmp	rekordbox.exe+E82FD4																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
rekordbox.exe+E836C9	CC		int 3																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
rekordbox.exe+E836CA	CC		int 3																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
rekordbox.exe+E836CB	CC		int 3																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
rekordbox.exe+E836CC	40	53	push	rbx																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
rekordbox.exe+E836CE	48	83 EC 20	sub	rsp,20	32																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																											
subtract																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																
Protect:Read/Write AllocationBase=2535BBC0000 Base=2535C7EA000 Size=10000																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																
address	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F	89	A	B	C	D	E	F	01	2	3	4	5	6	7	8	9	A	B	C	D	E	F																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
2535C7EA048	D7	1B	D5	AE	00	42	00	80	00	00	00	00	00	00	00	00	00	91	7F	1E	53	02	00	00	.	.	B</

EZ MODO

1. Choose one address, right-click and select "Pointer scan for this address" and click OK in the window that pops-up. You will have to select a location to save a file it

generates, this can be chosen anywhere.

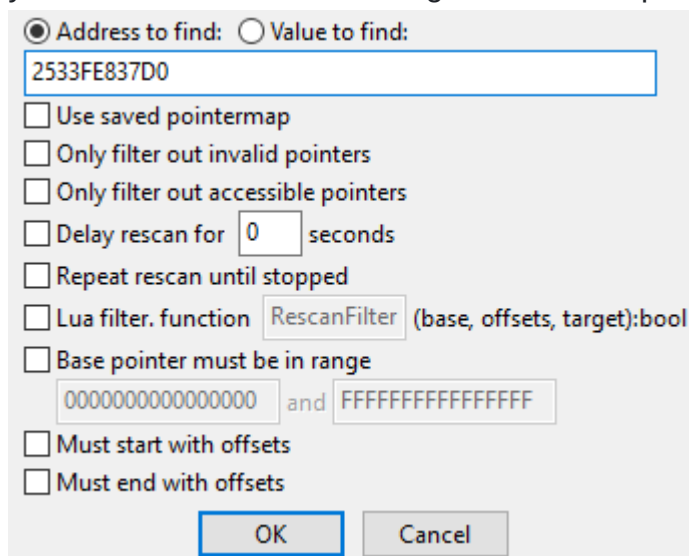
☒ Scan for address ☐ Scan for addresses with value ☐ Generate pointermap
☐ Use saved pointermap
☐ Compare results with other saved pointermap(s) ☐ Show advanced options
☒ Max different offsets per node: 3 ☐ Allow scanners to connect at runtime
☐ Base address must be in specific range Port: 52737 Password:
☐ Pointers must end with specific offsets ☐ Connect to pointerscan node
 Nr of threads scanning: 14 Normal
 Maximum offset value: 2047 Max level 5
 OK Cancel

2. Load a new track into the deck. In the pointer scan window, right-click anywhere in the value list and click Resync modulelist.

String		Pointer paths:191				
Base Address	Offset 0	Offset 1	Offset 2	Offset 3	Offset 4	Points to:
"rekordbox.exe"+039C78...	138	0				25328AEF5A0 = Beat Of The Rising Sun
"THREADSTACK0"-00000...	220	90	2D0			2533EAD7260 = Night Of Fire
"THREADSTACK0"-00000...	220	10	0			2533EAD7260 = Night Of Fire
"rekordbox.exe"+039B4840	8	20	1E0			25328AEF880 =
"rekordbox.exe"+039B4840	8	328	330			2533EAD7380 =
"rekordbox.exe"+039B4840	8	18	0			25328AEF5A0 = Beat Of The Rising Sun
"rekordbox.exe"+039B4840	8	320	C0			2533EAD71A0 = 2019-03-24
"rekordbox.exe"+039F5D...	E8	470	1E0			25328AEF880 =
"rekordbox.exe"+039F5D...	E8	770	C0			2533EAD71A0 = 2019-03-24
"rekordbox.exe"+039F5D...	E8	778	330			2533EAD7380 =
"rekordbox.exe"+039F5D...	E8	468	0			25328AEF5A0 = Beat Of The Rising Sun
"rekordbox.exe"+03A578...	220	90	2D0			2533EAD7260 = Night Of Fire
"rekordbox.exe"+03A578...	220	10	0			2533EAD7260 = Night Of Fire
"rekordbox.exe"+03A6E0...	78	138	0			25328AEF5A0 = Beat Of The Rising Sun
"THREADSTACK0"-00000...	140	78	A0	330		-
"THREADSTACK0"-00000...	220	90	28	2B0		-
"rekordbox.exe"+039B4840	8	38	20	1E0		25328AEF880 =
"rekordbox.exe"+039B4840	8	38	328	330		2533EAD7380 =
"rekordbox.exe"+039B4840	8	38	320	C0		2533EAD71A0 = 2019-03-24
"rekordbox.exe"+039B4840	8	38	18	0		25328AEF5A0 = Beat Of The Rising Sun
"rekordbox.exe"+039BA6...	8	138	448	300		2533EAD7260 = Night Of Fire
"rekordbox.exe"+039BA6...	8	138	440	90		2533EAD7260 = Night Of Fire
"rekordbox.exe"+039BA6...	8	A8	448	330		2533EAD7260 = Night Of Fire
"rekordbox.exe"+039BA6...	8	A8	140	1E0		2533EAD7260 = Night Of Fire
"rekordbox.exe"+039BA6...	8	A8	440	C0		2533EAD7260 = Night Of Fire
"rekordbox.exe"+039BA6...	8	A8	138	0		2533EAD7260 = Night Of Fire
"rekordbox.exe"+039C06...	48	0	20	330		2533EAD7260 = Night Of Fire
"rekordbox.exe"+039C06...	48	8	20	330		2533EAD7260 = Night Of Fire

3. Search for the new string you want in the list. You can either confirm if multiple instances point to the same address or not.
4. In the pointer scan window, click "Pointer scanner" at the top and select "Rescan memory." In the window that pops up, enter one of the addresses that has the value

you want, and click OK, saving the file when prompted.

A screenshot of a dialog box for filtering pointers. At the top, there are two radio buttons: "Address to find:" (selected) and "Value to find:". Below this is a text input field containing the hexadecimal address "2533FE837D0". There are several checkboxes: "Use saved pointermap", "Only filter out invalid pointers", "Only filter out accessible pointers", "Delay rescan for" (with a numeric input set to "0" and the unit "seconds"), "Repeat rescan until stopped", "Lua filter. function" (with a dropdown menu showing "RescanFilter" and the signature "(base, offsets, target):bool"), "Base pointer must be in range" (with two text input fields containing "0000000000000000" and "FFFFFFFFFFFFFF" separated by the word "and"), "Must start with offsets", and "Must end with offsets". At the bottom are "OK" and "Cancel" buttons.

5. You should now have a much shorter list of addresses. Repeat step 2. There is a good chance all the pointers will point to the same new address. You can repeat step 2 as many times as you want to be safe.
6. Once you are comfortable with the list of pointers knowing they properly point to the value you want, you have two options.
7. The first option is to choose one of the pointers and use it. This pointer is only guaranteed to work with the deck mode you had Rekordbox running in when finding the pointer.
8. The second option is to change rekordbox's deck mode, Resync the modulelist in the pointer scan window, and repeat step 2 as needed. You will also need to change the deck mode back even if some of the pointers seem to be fine, as they might not actually be fine. This has a high chance of failing in general, and going Hard Mode might be needed to increase your chances of finding a pointer that works regardless of the deck mode being changed.
9. Repeat this step for each deck you want tags for.

HARD MODE

I may have gotten lucky when I went through these steps to write this, and you might not actually find a pointer that works for all decks.

1. Use deck 1 for this, and search for the title, as we can find a pointer that can be used for all decks.
2. Repeat step 1 from ez mode on each address, keeping all pointer scan windows open.
3. Repeat steps 2-4 of ez mode taking but for all pointer scan windows. Do this until you have a decently small list of possible pointers.

4. Load songs into all 4 decks.
5. Switch between 2-deck and 4-deck mode, refreshing the pointer scan windows after each switch. Do this two or three times. You should be left with only a couple potentially valid pointers.
6. On the main CheatEngine window, click "Add Address Manually." In the window that pops up, check the "Pointer" box, set the Type to Text, and add as many offsets as is needed for whatever pointer you are checking.

Address: = ???

Description:

Type:

Length: ☐ Unicode ☐ Codepage

☒ Pointer

< > ?????????+0 = ????????

< > [????????+0] -> ????????

-> ????????

7. Add the base address and offsets, verify the value is what you expect.

Address: = 恋する☆宇宙戦争っ!!

Description:

Type:

Length: ☐ Unicode ☐ Codepage

☒ Pointer

< > 1A06CFD3350+0 = 1A06CFD3350

< > [1A042EDFD50+130] -> 1A06CFD3350

-> 1A042EDFD50

8. Increase the last non-0 offset by 0x8. Verify it shows the artist.

Address: 1A0740A61D0 =Prim

Description: No description

Type: Text

Length: 30 ☐ Unicode ☐ Codepage

☒ Pointer

< 0 > 1A0740A61D0+0 = 1A0740A61D0

< 138 > [1A042EDFD50+138] -> 1A0740A61D0

rekordbox.exe+03a578f0 -> 1A042EDFD50

Add Offset Remove Offset

OK Cancel

9. Increase the offset by 0x30 from its initial value, and verify the song title in deck 2 appears. If it does not, discard the pointer and try the next one starting at step 7.
10. Repeat step 9 cycling through all 4 decks, so the deck 4 title offset value will be 0x90 above the initial offset value.

Address: 1A0766B0280 =Mermaid girl-秋葉工房 MIX-

Description: No description

Type: Text

Length: 30 ☐ Unicode ☐ Codepage

☒ Pointer

< 0 > 1A0766B0280+0 = 1A0766B0280

< 1c0 > [1A042EDFD50+1C0] -> 1A0766B0280

rekordbox.exe+03a578f0 -> 1A042EDFD50

Add Offset Remove Offset

OK Cancel

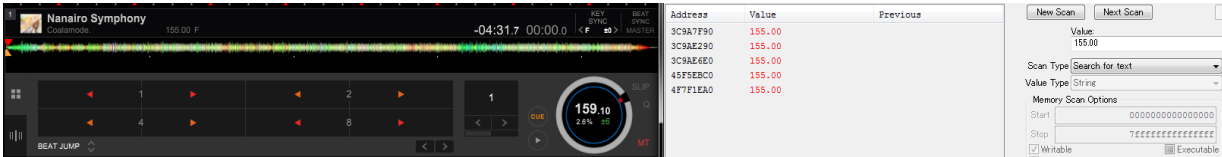
11. Congratulations, you have a pointer that should work for all deck modes. Maybe.

Finding the Deck Struct via bpm

What we are looking for is an array of Deck structs. The Deck struct looks something along the lines of {Title, Artist, Album, ?, BPM, Key} Same with the HARD MODE above.

1. Start rekordbox in 2-deck mode. Switch over to 4-deck.

2. Load songs in all 4 decks. Preferably something you'd like to listen to while scanning for pointers.
3. Change the tempo of deck 1, then do a text/string search for the track's original BPM (so 155.00 in the pic below, not 159.10) You should get a couple results like



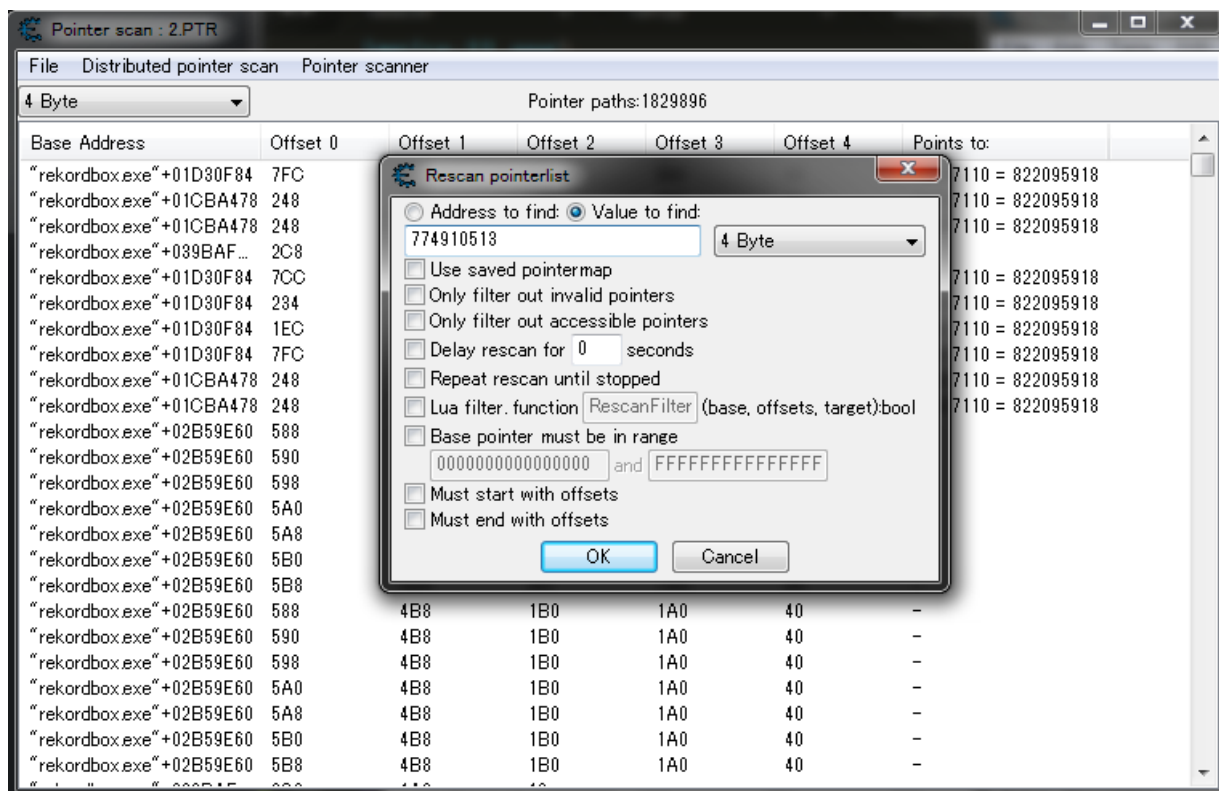
4. Grab all those addresses into the bottom window and right click, perform a Pointer scan for that address. Make sure to keep organized. I'd like to name the scan files as their respective row. ie. the 3rd row will just be named 3. And the rescans in the upcoming steps will be named 3-1. It's important to keep the previous scans in the case you do an error and need to recover.
5. After all the scans are done, and you have all of the scan windows open. Change the song of Deck 1 to a different song.
6. After changing the song, you should see that some of the addresses have changed. Those are the pointers you want.

Active	Description	Address	Type	Value
<input type="checkbox"/>	No description	3C9A7F90	String[6]	128.00
<input type="checkbox"/>	No description	3C9AE290	String[6]	
<input type="checkbox"/>	No description	3C9AE6E0	String[6]	-3.3d
<input type="checkbox"/>	No description	45F5EBC0	String[6]	155.00
<input type="checkbox"/>	No description	4F7F1EA0	String[6]	155.00

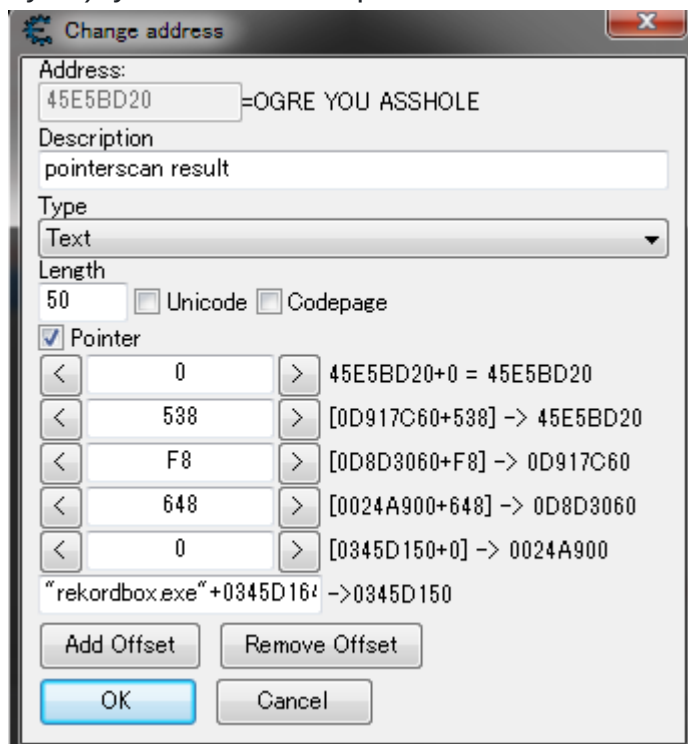
In the above case, I'll be taking a look at the 2nd and 3rd address.

7. There will be exactly one pointer which is correct (at least in rekobo v5.8.5) so switch deck 1 to a new track. Do a search for the new track's BPM, add it to the codelist (doubleclick the result), rightclick » change record » type: 4 bytes , rightclick » disable "Show as hexadecimal" and that integer value is what we want in the pointerscan results. So in the ptrscan window click on Pointer Scanner -> Rescan Memory, Hit value to find. I switched mine to to a 120.00 bpm song so my 4 byte value

is 774910513.



- After getting the pointer you want to test onto the main window by double clicking, double click on address, and change the second to last pointer (538 in the pic below) by hitting the left and right arrows or by adding/subtracting 8 bytes. When moving by 8 bytes, you'll be traversing the struct mentioned above. If you hit it 4 times (jumping 32 bytes), you should end up in the title for deck 1.



- If you have confirmed that the pointer you found was a deck struct and is working, here comes the fun part. If you keep adding 8 bytes to the second to last offset, you

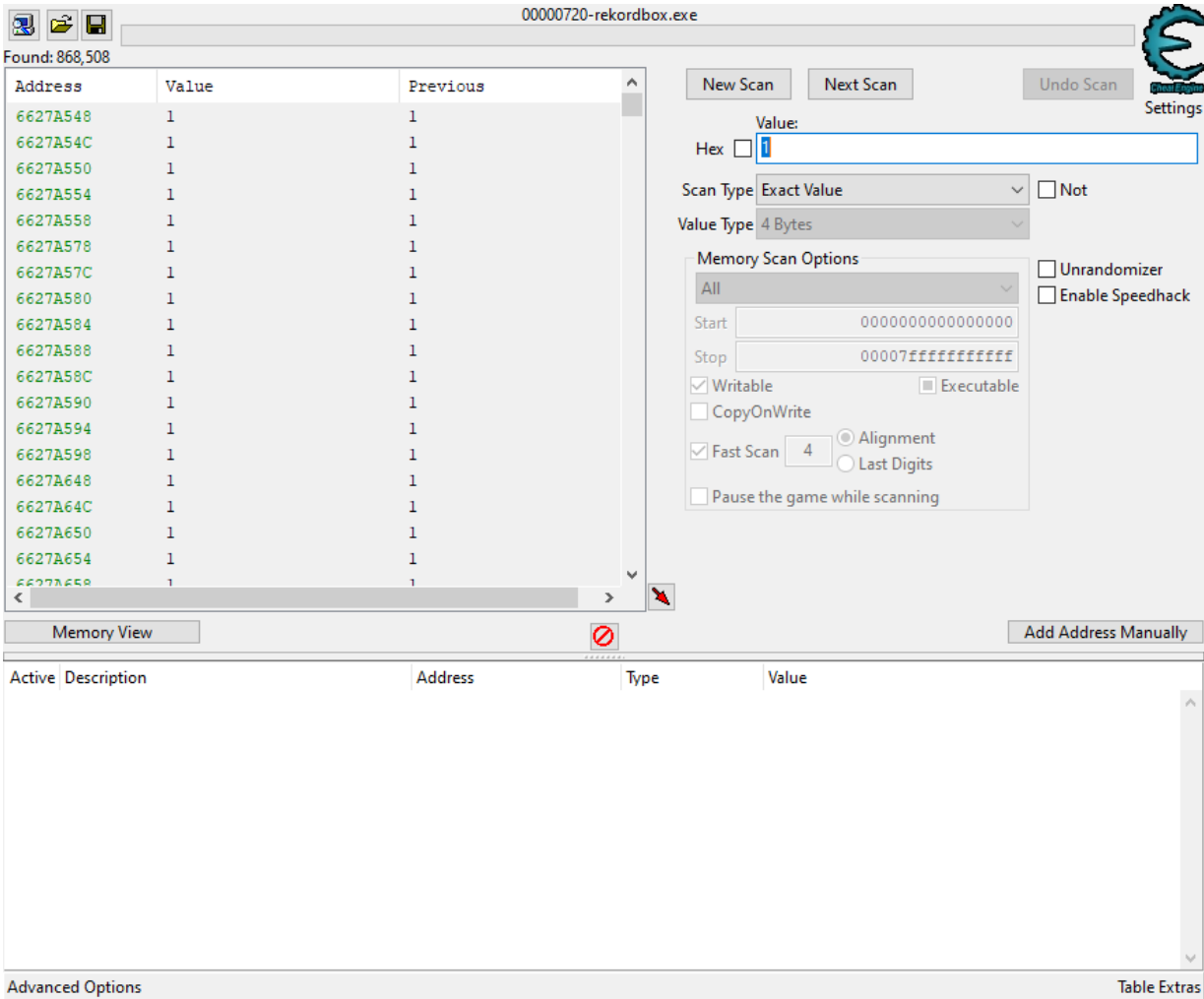
should end up in deck 2. And if you continue adding, you'll end up in deck 3, and then deck 4. Note that the pointer should also work if there's nothing loaded into deck 1, so eject the first track and see if you can still traverse to the other decks. If the pointer you found does not lead to the other decks, Head back to step 7 and grab yourself another one, or you can repeat the same procedure for other decks and find different pointers for each (not recommended tho).

10. If you have found a pointer that can be used to get all the other decks too, it's time to test it. It should be able to withstand: Closing and reopening rekordbox, switching modes to export/performance/lighting. What it should not be able to withstand: Updating rekordbox.
11. See step 11 of HARD MODE.

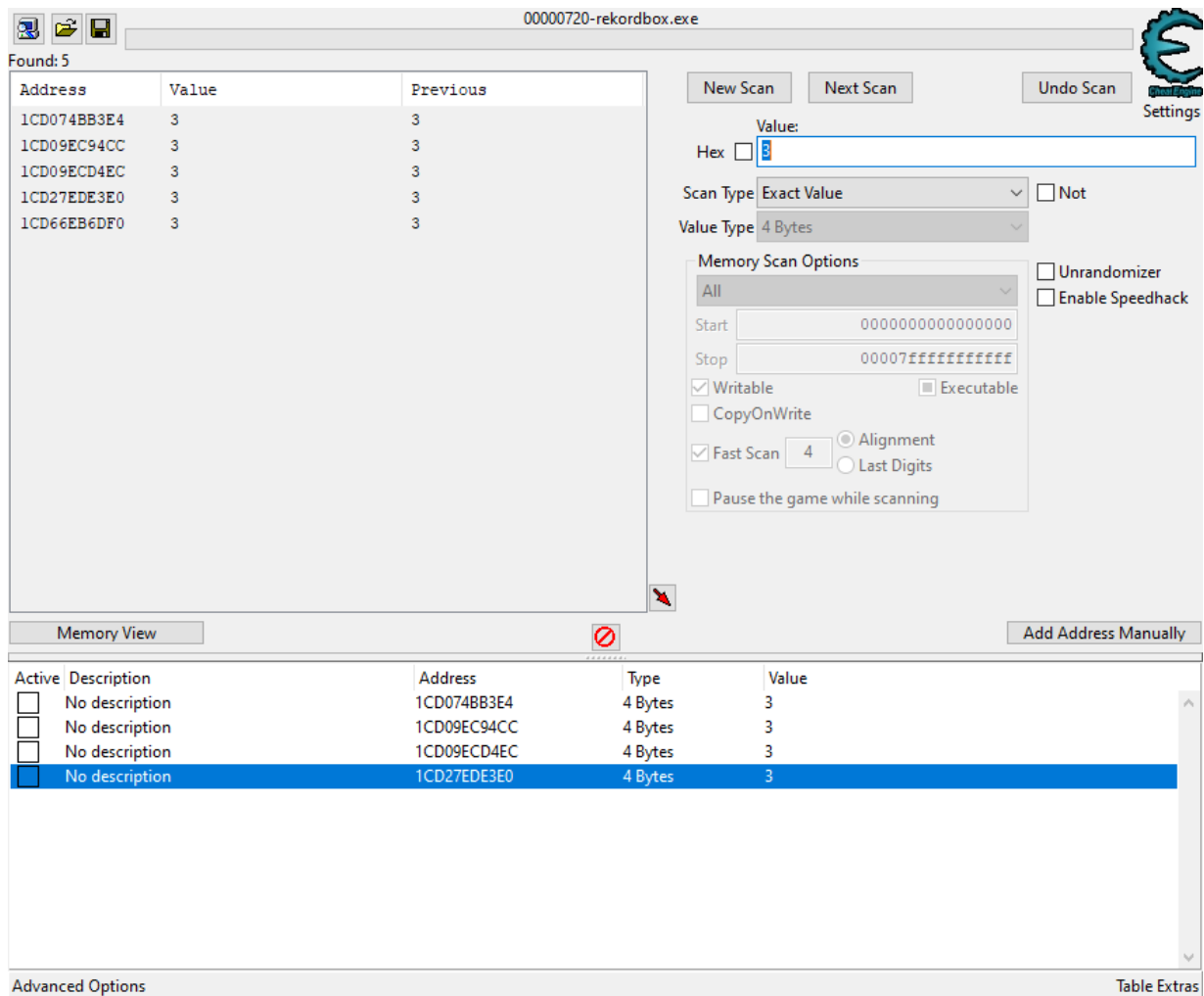
Master Deck

Finding a master deck pointer is easy as there are usually plenty of valid pointers for it. The master deck value is an integer with the deck indexes being 0-based. So deck 1 is set as master, the pointer will show 0, with deck 2 set it would show 1, etc.

1. You can change deck modes and the pointer found should still work, so to make things easier set Rekordbox to 4-deck mode
2. Set one of the decks in Rekordbox as Master.
3. In CheatEngine, set the Value Type to 4 bytes, enter the expected deck number in the search box, and click First Scan



4. Change the master deck in Rekordbox, set the search value to the expected one, and click Next Scan



- Repeat step 4 until you have narrowed the list of address found to a manageable amount.
- Change the master deck and check the addresses after each change. They should all show the correct value. Choose one and scan for a pointer per Step 1 of ez mode artist/title instructions.
- Choose any pointer you want that uses "rekordbox.exe" as part of the base address. You can sort the offset columns to find the pointer with the fewest offsets.