Memory Addresses (SA)

This article may need to be rewritten.
Please help improve this article. The discussion page may contain suggestions.

Note that all offsets thus posted have been confirmed for GTA San Andreas (GTA_SA.EXE) version 1.0. This is *not* for function addresses, for these look into Function Memory Addresses (SA).

Note: None of the memory addresses below will work for GTA: San Andreas v2.0 or 3.0(steam). All addresses in v2.0 and above have been changed or moved. Thus inaccessible.

Contents [hide]

1 Base Memory addresses
- 1.1 No category yet
- 1.2 Stats
- 1.3 HTML Stats File
- 1.4 Cheats
- 1.5 Display Settings
- 1.6 Sound Configuration
- 1.7 Controller Configuration
- 1.8 Other Dynamic Memory Addresses (non-static)
- 1.9 Pedestrians
  - 1.9.1 General
  - 1.9.2 Structures
- 1.10 Cars
- 1.11 Wanted
- 1.12 Camera
- 1.13 Ignored
- 1.14 Pools
- 1.15 Target
- 1.16 Handling
- 1.17 Controls
- 1.18 Rockets
- 1.19 Bullets
- 1.20 Race Checkpoints
- 1.21 Garages and Parking
- 1.22 Interface
- 1.23 Menu
- 1.24 Menu IDs
- 1.25 SCM related
  - 1.25.1 Threads
  - 1.25.2 External Scripts Info
  - 1.25.3 Restart Locations
  - 1.25.4 Misc

Base Memory addresses

No category yet

- 0xA49D54 - [dword] Timer for driving/flying missions (in ms)
- 0xA51974 - [dword] Timer for boat/bike missions (in ms)
- 0xA51A3C - Timer for Bloodring race
- 0xB7CE50 - [dword] Money
- 0xBAA420 - Wanted Level
- 0x8CDEE4 - [dword] Max wanted level
- 0xB79038 - [dword] How many days have passed in game
- 0xB70153 - [byte] Current Hour
- 0xB70152 - [byte] Current Minute
- 0x8D5104 - [byte] Current blur level
- 0xB7014E - [byte] Current Weekday (1 through 7)
- 0x8CB7A5 - [byte] Current Radiostation-ID
- 0xB700F0 - [dword] Current Car ID (from vehicle.ide) - not for bikes
- 0xB7CB49 - [byte] Game freezes like when in menu:
  - 0 = normal
  - 1 = everything stops
- 0xB7CB49 - [byte] Menu show:
  - 0 = leave
  - 1 = show
- 0x863984 - [Int32] Gravity
- 0xB610E0 - [dword] A global timer in ms (read only)
- 0xB7CB84 - [dword] A global timer in ms (while not in menu, read/write)

2 Weather Codes
3 Dependencies
4 External links

- 0xA5153C - [dword] Mission timer from a number to 0 (4 bytes)
- 0xB7CB64 - [float] Game speed in percent
- 0xB70158 - [dword] Timer related to weather and time in ms
- 0xB7015C - [dword] Defines how many ms (1 second... default 1000, set to 1 for a headache, number of ms per sec)
- 0xB7CEE4 - [byte/boolean] Is infinite run
- 0xB7CEE6 - [byte/boolean] Is player fireproof
- 0x96C009 - [byte/boolean] Is paynspray free
- 0xA444A4 - [byte/boolean] Is radar greyed out
- 0x8D2530 - [float] Pedestrian density multiplier
- 0x8A5B20 - [float] Vehicle density multiplier
- 0xB6F065 - [byte/boolean] Widescreen (the view that is displayed during cutscenes, not the display option)
- 0xA4A948 - Lowrider Challenge score
- 0xA4EC20 - Dancing minigame score
- 0xB790B8 - [byte] Photographs taken number (4 bytes)
- 0xA9AD74 - [byte] Tags number (4 bytes)
- 0xB791E4 - [byte] Horseshoes number (4 bytes)
- 0xB791EC - [byte] Oysters number (4 bytes)

Note: For those number above if you change it to maximum amount they appear to pop a message and gives a bonus like weapons in cj savehouses.

- 0x716642 - [float] Change solid clouds
- 0x716655 - [float] Disable solid clouds

Note: Both values default to 200. If you change one of them to 100,000 you get very few clouds, a much nicer effect. If you change both of them to 100,000 you never get the clouds.

- 0xB79078 - [byte] People dropped off in taxi (number used for the stats, 4 bytes)
- 0xA49C30 - [byte] People dropped off in taxi (number used for giving your reward, 4 bytes)
- 0xB79040 - [byte] Safehouse visits number (4 bytes)
- 0xA49EFC - [dword] Denise Progress
- 0xA49F00 - [dword] Michelle Progress
- 0xA49F04 - [dword] Helena Progress
- 0xA49F08 - [dword] Barbara Progress
- 0xA49F0C - [dword] Katie Progress
- 0xA49F10 - [dword] Millie Progress

Note: These above six addresses are within the scm block, and valid only for original scm. setting a value to 100 (ie. 100 pct) gives you all gifts of that GF (ie. car keys, wardrobe etc.).

- 0xB79108 - Number of girls dated
- 0xB79100 - Current number of girlfriends
- 0xB79104 - Number of disastrous dates
- 0xB79110 - Number of successful dates

- 0xB79060 - Unique jumps found number
- 0xB79064 - Unique jumps done number
- 0xBA6774 - Map target:
  - 0 = disabled
  - 1 = enabled
- 0x86329C - List of valid command names
- 0xC17054 - Main game window HWND
- 0xC97C28 - IDirect3DDevice9 pointer
- 0xBA3798 - Beginning of ZoneInfo structure
- 0xBA1DF0 - Beginning of ZonePop structure
- 0xA94B68 - array of pointers to RwTexture, corresponding to opcode 038F

Stats

- 0xB793D4 - [float] Fat stat
- 0xB793D8 - [float] Stamina stat
- 0xB793DC - [float] Muscle stat
- 0xB793E0 - [float] Health stat
- 0xB793E4 - [float] Sex Appeal stat
- 0xB79496 - [float] Pistol stat
- 0xB79498 - [float] Silenced pistol stat
- 0xB7949C - [float] Desert eagle stat
- 0xB794A0 - [float] Shotgun stat
- 0xB794A4 - [float] Sawn-off shotgun stat
- 0xB794A8 - [float] Combat shotgun stat
- 0xB794AC - [float] Machine pistol stat
- 0xB794B0 - [float] SMG stat
- 0xB794B4 - [float] AK47 stat
- 0xB794B8 - [float] M4 stat

HTML Stats File

- 0x8663A0 - File Name (Default : 'stats.html')
- 0x86636C - File Title (Default : '<title>Grand Theft Auto San Andreas Stats</title>')

Cheats

[byte] Can be either on (1) or off (0).

- 0x969130 - Weapon Set 1
- 0x969131 - Weapon Set 2
- 0x969132 - Weapon Set 3
- 0x969133 - Health+Armor+250K
- 0x969134 - Increase Wanted Level 2 Stars
- 0x969135 - Clear Wanted Level

- 0x969136 - Sunny Weather
- 0x969137 - Very Sunny Weather
- 0x969138 - Overcast Weather
- 0x969139 - Rainy Weather
- 0x96913A - Foggy Weather
- 0x96913B - Faster Clock
- 0x96913C - Faster Gameplay
- 0x96913D - Slower Gameplay
- 0x96913E - Peds Attack Each other with Golfclub
- 0x96913F - Have Bounty on Head
- 0x969140 - Everyone is Armed
- 0x969141 - *Spawn Rhino (**Not Tested!**)*
- 0x969142 - *Spawn Bloodring Banger (**Not Tested!**)*
- 0x969143 - *Spawn Rancher (**Not Tested!**)*
- 0x969144 - *Spawn Racecar A (**Not Tested!**)*
- 0x969145 - *Spawn Racecar B (**Not Tested!**)*
- 0x969146 - *Spawn Romero (**Not Tested!**)*
- 0x969147 - *Spawn Stretch (**Not Tested!**)*
- 0x96914A - Blow up All Cars
- 0x96914B - Wheels Only (Invisible Cars)
- 0x96914C - Perfect Handling
- 0x96914D - Suicide
- 0x96914E - All Green Lights
- 0x96914F - Aggressive Drivers
- 0x969150 - Pink Traffic
- 0x969151 - Black Traffic
- 0x969152 - Cars can drive on water
- 0x969153 - Boats Can Fly
- 0x969154 - CJ is Fat
- 0x969155 - Max Muscle
- 0x969156 - CJ is Skinny
- 0x969157 - Elvis Everywhere
- 0x969158 - Peds attack with rockets
- 0x969159 - Beach Theme
- 0x96915A - Gang Members everywhere
- 0x96915B - Gangs control the streets
- 0x96915C - Ninja Theme
- 0x96915D - Slut Magnet
- 0x96915E - Traffic is Cheap Cars
- 0x96915F - Traffic is Fast Cars

- 0x969160 - Cars can Fly
- 0x969161 - Huge Bunny Hop
- 0x969162 - *Spawn Hydra (**Not Tested!**)*
- 0x969163 - *Spawn Vortex Hovercraft (**Not Tested!**)*
- 0x969164 - Tank Mode/Smash'n Boom
- 0x969165 - All cars have nitro
- 0x969166 - Cars Float Away when hit
- 0x969167 - Always Midnight
- 0x969168 - Stop Game Clock - Orange Sky
- 0x969169 - Thunderstorm
- 0x96916A - Sandstorm
- 0x96916C - Mega Jump
- 0x96916D - Infinite Health
- 0x96916E - Infinite Oxygen
- 0x96916F - Get Parachute
- 0x969170 - Get Jetpack
- 0x969171 - Never Wanted
- 0x969172 - Six Star Wanted Level
- 0x969173 - Mega Punch
- 0x969174 - Never get Hungry
- 0x969175 - Peds Riot (Chaos Mode)
- 0x969176 - Funhouse Theme
- 0x969177 - Slower Gameplay
- 0x969178 - Infinite Ammo, No Reload
- 0x969179 - Full Weapon Aiming while driving
- 0x96917A - Decreased Traffic
- 0x96917B - Traffic is Country vehicles
- 0x96917C - Recruit Anyone (9mm)
- 0x96917D - Country Theme
- 0x96917E - Recruit Anyone (Rockets)
- 0x96917F - Max Respect
- 0x969180 - Max Sex Appeal
- 0x969181 - Max Stamina
- 0x969183 - Hitman in All Weapons
- 0x969184 - *Spawn Hunter (**Not Tested!**)*
- 0x969185 - *Spawn Quad (**Not Tested!**)*
- 0x969186 - *Spawn Tanker Truck (**Not Tested!**)*
- 0x969187 - *Spawn Dozer (**Not Tested!**)*
- 0x969188 - *Spawn Stunt Plane (**Not Tested!**)*
- 0x969189 - *Spawn Monster (**Not Tested!**)*

[dword]

- 0x96918C - Has ever Cheated or not
- 0xBAA472 - Has now Cheated or not
- 0xB79044 - Cheated Count

[byte]

- 0x96918C - 'Cheated' state:
  - 0 = disabled
  - 1 = enabled

Note: If it's set to 1 you'll get a warning message when saving a game. But this byte doesn't get set if you use a cheat enabler.

Display Settings

- 0xBA6784 - [dword] Brightness
- 0xBA6792 - [byte] Legend
- 0xBA676C - [byte] Radar Mode
  - 0 = maps & blips
  - 1 = blips
  - 2 = off
- 0xBA6769 - [byte] Hud Mode
  - 0 = off
  - 1 = on
- 0xBA678C - [byte] Subtitles
- 0xBA6830 - [byte] Store gallery photos
- 0xBA6788 - [float] Draw Distance
- 0xBA6794 - [byte] Frame limiter
- 0xBA6793 - [byte] Widescreen
- 0xA9AE54 - [byte] Visual FX Quality
- 0xBA680C - [byte] Mip Mapping
- 0xBA6814 - [byte] Antialiasing values:
  - 1 = 0x (off)
  - 2 = 1x
  - 3 = 2x
  - 4 = 3x
- 0xBA6820 - [byte] Resolution values:
  - 11 = 640x480
  - 12 = 800x400
  - 13 = 800x600
  - 15 = 1024x768

  (Depends on the graphic driver/hardware.)

Sound Configuration

- 0xBA6798 - [byte] Radio Volume [0 through 64]
- 0xBA6797 - [byte] SFX Volume [0 through 64]
- 0xBA6799 - [byte] Radio Equalizer
- 0xBA6795 - [byte] Radio Auto-tune
- 0xBA67F8 - [byte] Usertrack/Play mode values:
  - 0 = radio
  - 1 = random
- 0xBA680D - [byte] Usertrack/Automatic Media Scan
- 0xBA679A - [byte] Radio Station ID values:
  - 1 to 12 (see below for station names according to ID)
    - 1 = "Playback FM"
    - 2 = "K Rose"
    - 3 = "K-DST"
    - 4 = "Bounce FM"
    - 5 = "SF-UR"
    - 6 = "Radio Los Santos"
    - 7 = "Radio X"
    - 8 = "CSR 103.9"
    - 9 = "K-JAH West"
    - 10 = "Master Sounds 98.3"
    - 11 = "WCTR Talk Radio"
    - 12 = "User Track Player"
    - 13 = "Radio Off"

AlienX: Seems that the Radio Station ID is just a menu identifier, this does not actually change the radio station while in-game!

Another note... The opcode for switching players radio stations does not work in line with the station ID's, i have yet to figure out what station ID's are for the SCM code - Dont try to use the above ID's for the SCM Operation Code, it just wont work

Thanks to AlienX For the station names and ID's

Controller Configuration

- 0xBA6818 - [byte] Controller Configuration values:
  - 0 = mouse + keys
  - 1 = joypad
- 0xB6EC1C - [float] Mouse sensitivity
- 0xC1CC02 - [byte] Steer with mouse
- 0xC1CC03 - [byte] Fly with mouse
- 0xB6EC2E - REAL aiming mode offset, not menu:
  - 0 = joypad

- 1 = mouse + keys

Other Dynamic Memory Addresses (non-static)

Pedestrians

General

- 0xB6F5F0 - Player pointer (CPed)
- 0xB7CD98 - Player pointer, direct offset to the ped pool start (CPed)
- 0xB74498 - CPeds maximum number (normally 140)
- 0xB74490 - Contains a pointer to a pointer

This pointer:

- +0 = Contains a pointer to the first element in the pool
- +4 = Contains a pointer to a byte map indicating which elements are in use
- +8 = [dword] Is the maximum number of elements in the pool
- +12 = [dword] Is the current number of elements in the pool

Each ped object is 1988 (0x7C4) bytes.

For each ped in the pool:

In most cases, you can use even the dword of playeraddress as CPed value

- CPed +0x14 = Pointer to XYZ position structure (and rotation)
  - (CPed+0x14) +0x0 to +0x2C = [dword] Is the rotation matrix
  - (CPed+0x14) +0x30 = [dword] XPos
  - (CPed+0x14) +0x34 = [dword] YPos
  - (CPed+0x14) +0x38 = [dword] ZPos
- CPed +0x2F = [byte] Location status:
  - 0 = outside
  - 3 = inside a building
- CPed +0x42 = [float] Is the BP/EP/FP/DP (special flags) status of the player as follows:
  Add these values, and write the sum into +66 (0x42).
  - 1 = makes ped soft (ie. can move through walls and everything) (noclip in other words)
  - 2 = freezes ped (ie. ped cannot walk)
  - 4 = bullet-proof
  - 8 = flame-proof
  - 16 = ?
  - 32 = ?
  - 64 = damage-proof (from collisions etc)
  - 128 = explosion-proof
- CPed +0xC0 = [dword] Pointer to nearest car
- CPed +0x15C = Some anim states:

- 0 = landing from jump
- 61 = punching
- 102 = stopped
- 154 = sprint
- 205 = run

- Cped +0x46C = [byte] Player check:
  - 0 = in air/water
  - 1 = in car
  - 2 = entering interior
  - 3 = on foot
- CPed +0x46D = Jump state:
  - 32 = landed/idle
  - 34 = in air
  - 36 = landing
- CPed +0x46F = Crouch state:
  - 128 = stand
  - 132 = crouched
- CPed +0x47C = Pointer to anim struct
- CPed +0x4DF = Current anim play-state:
  - 0 = nothing
  - 61 = starting/stopping
  - 62 = looping
- CPed +0x504 = [word] Muzzle flash intensity:
  - 0 to 10000 = on
  - 65536 = off
- CPed +0x530 = [dword] State:
  - 0 = leaving a car, falling down from a bike or something like this
  - 1 = normal case
  - 50 = driving
  - 55 = wasted
  - 63 = busted
- CPed +0x534 = Runningstate:
  - 0 = while driving
  - 1 = standing still
  - 4 = start to run
  - 6 = running
  - 7 = running fast (sprinting) by pressing sprint key
- CPed +0x540 = [float] Health
- CPed +0x544 = [float] Max health

- CPed +0x548 = [float] Armor
- CPed +0x558 = [float] Current rotation (Z angle)
- CPed +0x55C = [float] Target rotation (Z angle)
- CPed +0x560 = [float] Rotation speed (Z angle)
- CPed +0x568 = [dword] Current Car you are in contact with
- CPed +0x584 = [dword] Current Entity you are in contact with
- CPed +0x58C = [dword] Last or Current Driven Car (CarPointer)
- CPed +0x598 = [byte] Player lock (set to 1 to lock player controls, can't move)
- CPed +0x5A0 = [byte] Start of weapon data (28 bytes) (See structures: WeaponSlot)
- CPed +0x5D8 = [dword] Pistol weapon type:
  - 22 = 9mm
  - 23 = silenced 9mm
  - 24 = desert eagle
- CPed +0x5DC = [dword] Pistol state
- CPed +0x5E0 = [dword] Pistol ammo in clip
- CPed +0x5E4 = [dword] Pistol total ammo (including clip)
- CPed +0x5F4 = [dword] Shotgun weapon type:
  - 25 = shotgun
  - 26 = sawn-off shotgun
  - 27 = spas-12
- CPed +0x5F8 = [dword] Shotgun state:
  - 1 = firing?
  - 2 = reloading
- CPed +0x5FC = [dword] Shotgun ammo in clip
- CPed +0x600 = [dword] Shotgun total ammo (including clip)
- CPed +0x718 = [byte] Current weapon slot (1 byte)
- CPed +0x740 = Current Weapon ID (from default.dat)
- CPed +0x760 = [dword] Weapon you were damaged with
- CPed +0x764 = [dword] Pointer to the ped that damaged you

Structures

```
WeaponSlot                // Total 28Bytes
 DWORD       type          // + 0
 DWORD       state         // + 4 (0 idle, 1 firing, 2 reloading)
 DWORD       AmmoInClip    // + 8
 DWORD       AmmoRemaining // +12
 FLOAT       unknown       // +16 (increases each time you fire your weapon, 0 when weapon not active,
                              probably used to count bullets fired to know when to reload?)
 UNKNOWN     0..7 Bytes    // +20 (unknown - goggle mode, 0 off and 256 on)...+27
```

```
WeaponSlot.type
   (Slot0: No Weapon)                    (Slot2: Handguns)
   0 - Fist                               22 - Pistol
   1 - Brass Knuckles                     23 - Silenced Pistol
```

```
(Slot1: Melee)                          24 - Desert Eagle
2 - Golf Club                          (Slot3: Shotguns)
3 - Nitestick                           25 - Shotgun
4 - Knife                               26 - Sawn-Off Shotgun
5 - Baseball Bat                        27 - SPAS-12
6 - Shovel                             (Slot4: Sub-Machineguns)
7 - Pool Cue                            28 - Micro Uzi
8 - Katana                              29 - MP5
9 - Chainsaw                            32 - TEC-9
15 - Cane
(Slot5: Machineguns)                    (Slot10: Gifts)
30 - AK47                               14 - Flowers
31 - M4                                 (Slot9:Special1)
(Slot6: Rifles)                         42 - Fire Extinguisher
33 - Country Rifle                      43 - Camera
34 - Sniper Rifle                       (Slot11:Special2)
(Slot7: Heavy Weapons)                  44 - NV Goggles
35 - Rocket Launcher                    45 - IR Goggles
36 - Heat Seaking RPG                   46 - Parachute
37 - Flame Thrower                      (Slot12:Detonators)
38 - Minigun                             40 - Detonator(for remote explosives)
(Slot8: Projectiles)
16 - Grenade
18 - Molotov Cocktail
39 - Remote Explosives
(No slot: Fired from hunter / hydra / missile launcher)
(This type is stored in the rocket pool as rocket type, but is the continuation of this list)
19 - Normal rockets
20 - Heatseeking rockets
58 - Flares
```

Cars

- 0xB6F980 - Is the direct pointer to the pool start (CVehicle)
- 0xBA18FC - Current vehicle pointer:
  - 0 = on-foot
  - >0 = in-car
- 0x969084 - First vehicle you got into

Note: To get the next vehicle, so the second one, you need to add +0x4 as many times you want. They are 0 if you haven't entered a first/second/third/etc car yet.

- 0xB74494 - Contains a pointer

This pointer:

- +0 = Contains a pointer to the first element in the pool
- +4 = Contains a pointer to a byte map indicating which elements are in use
- +8 = [dword] Is the maximum number of elements in the pool
- +12 = [dword] Is the current number of elements in the pool

Each vehicle object is 2584 (0xA18) bytes. It starts at 0xC502AA0.

For each vehicle in the pool:

- +20 = [byte] Contains a pointer to the rotation/position matrix (84 bytes):
  - +0 = [float] X-axis Rotation (Grad)
  - +4 = [float] Y-axis Rotation (Grad)
  - +8 = [float] Z-axis Rotation (Grad)

- +16 = [float] X-axis Rotation (Looking)
- +20 = [float] Y-axis Rotation (Looking)
- +24 = [float] Z-axis Rotation (Looking)
- +48 = [float] X-axis Position
- +52 = [float] Y-axis Position
- +56 = [float] Z-axis Position

- +34 = [word] Vehicle ID from vehicles.ide
- +66 = [byte] Is the BP/EP/DP/DP (Special Flags) status of the car as follows:
  Add these values, and write the sum into +66
  - 1 = n/a
  - 2 = n/a
  - 4 = bullet-proof
  - 8 = fire-proof
  - 16 = damage-proof (from collisions etc)
  - 32 = n/a
  - 64 = n/a
  - 128 = explosion-proof
- +68 = [float] X (East-West) speed
- +72 = [float] Y (North-South) speed
- +76 = [float] Z (Up-Down) speed
- +80 = [float] X (NS) Spin
- +84 = [float] Y (EW) Spin
- +88 = [float] Z (NW) Spin

Note: Do not get confused about the Spin Angles, these are NOT rotations but the angles of how fast your vehicle is turning in the given axis direction...

(Car addresses continued:)

- +140 = [float] Mass (kg) from handling.cfg
- +144 = [float] Turn Mass from handling.cfg
- +148 = [float] Grip Divider:
  - 1.0 = 1 x gGrip
  - 10.1 = 10 x gGrip
  - 100.0 = g / 100Grip
- +152 = [float] Mass-to-Grip Multiplier. Ie. G Force when flying/during suspension/driving (acceleration towards ground)
- +160 = [float] Normalized Grip Level
- +164 = [float] CoM X
- +168 = [float] CoM Y
- +172 = [float] CoM Z
- +216 = [float] Increases when collision occurs
- +1064 = [byte] Engine State (whether the engine is running or stalled):

    - 0 = stalled
    - 16 = ok
- +1069 = [byte] Siren on/off
- +1076 = [byte] Body Color (as in carcolors.dat, black being the 0)
- +1077 = [byte] Stripe Color (as in carcolors.dat, black being the 0)
- +1078 = [byte] Body Color #2
- +1079 = [byte] Stripe Color #2
- +1080 = [dword] modding data as in garage info (Not working?)
- +1084 = [dword] modding data as in garage info (Not working?)
- +1088 = [dword] modding data as in garage info (Not working?)
- +1092 = [dword] modding data as in garage info (Not working?)
- +1096 = [dword] modding data as in garage info (Not working?)
- +1100 = [dword] modding data as in garage info (Not working?)
- +1104 = [dword] modding data as in garage info (Not working?)
- +1108 = [dword] modding data as in garage info (Not working?)
- +1112 = [float] Car Wheel Size from vehicle.ide
- +1116 = [dword] Time left for car alarm to sound in ms
- +1120 = [dword] Pointer to driver
- +1124 = [dword] Pointer to passenger 1 (Front-right seat)
- +1128 = [dword] Pointer to passenger 2 (Rear-left seat)
- +1132 = [dword] Pointer to passenger 3 (Rear-right seat)
- +1136 = [dword] Pointer to passenger 4 (Used for buses)
- +1140 = [dword] Pointer to passenger 5 (Used for buses)
- +1144 = [dword] Pointer to passenger 6 (Used for buses)
- +1148 = [dword] Pointer to passenger 7 (Used for buses)
- +1152 = [dword] Pointer to passenger 8 (Used for buses)
- +1156 = [dword] Pointer to passenger 9 (Used for buses)
- +1172 = [float] Steer angle 1
- +1176 = [float] Steer angle 2
- +1180 = [float] Gas pedal
- +1184 = [float] Brake pedal
- +1192 = [byte] Places a car-bomb:
    - 0 = no bomb
    - 1 = car has bomb, but not armed
    - 4 = car has bomb, and is armed

Note: You can set the above values to 0 and 1 to give the car a bomb. Some other flags get set when you arm the bomb. So if you set this value to 4, or actually arm the bomb thru normal gameplay, it does not help to change this value back.

- +0x8A4 = [float] Nitro Count
    - 1.0 Nitro Empty

- -1.0 Nitro filled
- +0x48A = [BYTE] Nitro State ?
  - 9 Nos activated
  - 10 Unactivated
  - 0 No nos
- +1200 = [float] Body dirt level:
  - 0.0 = fully clean
  - 15.0 = maximum dirt visible
- +1216 = [float] Health/Car Damage Left:
  - <250.0 = on fire
  - 1000.0 = undamaged
- +1272 = [dword] Car Door Locked State:
  - 1 = open
  - 2 = locked
- +1300 = [dword] Alternate siren (honking):
  - 0 = off
  - 1 = on

Note: Automatically gets reset back to 0. To prevent this just NOP 0x6E0A3B (6 bytes).

- +1412 = [dword] Headlights switch:
  - 0 = off
  - 1 = on

Note: Same case as above, gets automatically reset - NOP 0x6E1EDE (6 bytes).

- +1424 = [byte] Car type:
  - 0 = car/plane
  - 5 = boat
  - 6 = train
  - 9 = bike
- +1444 = [float] Train speed:
  - -0.1 = is forward
  - 0.1 = is reverse
- +1445 = [byte] Car Tire (Left-Front) Status:
  - 0 = ok
  - 1 = flat
  - 2 = Used by planes when landing gear is up
- +1446 = [byte] Car Tire (Left-Rear) Status:
  - 0 = ok
  - 1 = flat
  - 2 = Used by planes when landing gear is up

- +1447 = [byte] Car Tire (Right-Front) Status:
  - 0 = ok
  - 1 = flat
  - 2 = Used by planes when landing gear is up
- +1448 = [byte] Car Tire (Right-Rear) Status:
  - 0 = ok
  - 1 = flat
  - 2 = Used by planes when landing gear is up
- +1628 = [byte] Bike Tire (Front) Status:
  - 0 = ok
  - 1 = flat
- +1629 = [byte] Bike Tire (Rear) Status:
  - 0 = ok
  - 1 = flat
- +1630 = [byte] Bicycle Tire (Front) Status:
  - 0 = ok
  - 1 = shot
- +1631 = [byte] Bicycle Tire (Rear) Status:
  - 0 = ok
  - 1 = shot

Note: You cannot actually shoot the wheels of bmx. If you set the value 1 at above two offsets, it rides as if the wheels were shot. They probably not work.

- +1736 = [byte] Is the bike identifier.

Note: Gets set to 1 if this vehicle is a bike (or bmx).

- +1824 = [float] Front-Left suspension height
- +1828 = [float] Rear-Left suspension height
- +1832 = [float] Front-Rear suspension height
- +1836 = [float] Rear-Rear suspension height

Note: There is also a copy of the suspension values at -0x10, but these are 'smoother'. They range from 0 to 1 (1 = fully extended/airborne, 0 = fully compressed).

- +2020 = [float] Front-Left suspension height
- +2024 = [float] Rear-Left suspension height
- +2028 = [float] Front-Right suspension height
- +2032 = [float] Rear-Right suspension height
- +2156 = [word] Current load of vehicle, works for vehicles such as dumper, packer, dozer, forklift and so on.
- +2160 = [word] Last load value of vehicle. Used to detect whether vehicle should have sound of raising/lowering a load. After detecting it gets value of car struct +2156 below.
- +2276 = [float] Burn Timer (in ms)

Let's say, the Car Position of this given car starts at 0xC5F5DB4:

- +0 = X Level to the ground
- +4 = Y Level to the ground
- +8 = Z Level to the ground
- +16 = X Where am I looking
- +20 = Y Where am I looking
- +24 = Z Where am I looking
- +32 = Dyn flight data
- +36 = Dyn flight data
- +40 = Dyn flight data
- +48 = CarPosX
- +52 = CarPosY
- +56 = CarPosZ

Following offsets are Floats, as positions of doors and other car parts that gets detached by damage. We need to recalculate and set their locations if we warp a car from one location to another. Otherwise the car spins uncontrollably:

- +1828 = Detachables1 Pos X
- +1832 = Detachables1 Pos Y
- +1836 = Detachables1 Pos Z
- +1872 = Detachables2 Pos X
- +1876 = Detachables2 Pos Y
- +1880 = Detachables2 Pos Z
- +1916 = Detachables3 Pos X
- +1920 = Detachables3 Pos Y
- +1924 = Detachables3 Pos Z
- +1960 = Detachables4 Pos X
- +1964 = Detachables4 Pos Y
- +1968 = Detachables4 Pos Z

The locations of the detachable objects are different for cars and bikes. This is merely because bike object is actually smaller than the car object. The car object is used for all vehicles (including heli) but the bikes.

Offsets for Detachables:

- +1532 = BikeDetachPosAdr(0)
- +1632 = BikeDetachPosAdr(1)
- +1676 = BikeDetachPosAdr(2)
- +1720 = BikeDetachPosAdr(3)
- +1764 = BikeDetachPosAdr(4)
- +1828 = CarDetachPosAdr(0)
- +1872 = CarDetachPosAdr(1)
- +1916 = CarDetachPosAdr(2)
- +1960 = CarDetachPosAdr(3)

The trailer of the tanker is handled the same way as the vehicles. Its pointer gets set at offset:

- +1224

To the car object start. When warping vehicles that has trailer, we need to warp this 'vehicle' as well. The same pointer is used also when you are towing other vehicles as well.

Wanted

0xB7CD9C - Wanted pool start (CWanted). Each slot has 668 bytes of data.

- +0x0 = Is the counter for how pissed the cops are:
  - above 50 = 1 star
  - above 180 = 2 stars
  - above 550 = 3 stars
  - above 1200 = 4 stars
  - above 2400 = 5 stars
  - above 4600 = 6 stars
- +0x4 = like above, but 'before parole (timed wanted level decrease?)'
- +0x8 = [dword] time value, the last time the wanted level decreased
- +0xC = [dword] time value, the last time the wanted level changed
- +0x10 = [dword] 'time of parole'
- +0x14 = [float] multiplier of wanted level contribution of crimes (set using 03C7?)
- +0x18 = [byte] Current amount of cops 'in pursuit'
- +0x19 = [byte] Maximum number of foot cops simultaneously shooting at you ('in pursuit')
- +0x1A = [byte] Maximum number of cop cars in pursuit
- +0x1B = [byte] Amount of cops currently 'beating the suspect'
- +0x1C = [word] Chance a road block appears, range unknown (though 127 seems to have a special meaning)
- +0x1E = [bool] Is the player ignored by police? (set by script)
- +0x1F = [bool] Is the player ignored by police? (set by garages)
- +0x20 = [bool] Is the player ignored by everyone?
- +0x21 = [bool] Should the streamer load the SWAT models?
- +0x22 = [bool] Should the streamer load the FBI models?
- +0x23 = [bool] Should the streamer load the army models?
- +0x24 = [dword] Current chase time
- +0x28 = [dword] 'Current chase time counter'
- +0x2C = [bool] 'is time counting'
- +0x2D = [word] Current wanted level (1-6)
- +0x2F = [word] Wanted level before 'parole'
- need to do more

Note: Helicopters will still shoot if you change flag 0x19 to 0.

Camera

- 0xB6F028 - Camera Block Start (CCamera)
- 0x52B730 - Start of camera 'MOVer' subroutine:
  - 0xC3 = lock camera (retn)
- 0xB6F0DC - [dword] Current View:
  - 0 = bumper View
  - 1 = close external view
  - 2 = middle external view
  - 3 = furthest external view
  - 4 = nothing = same as last?
  - 5 = cinematic view
  - 6 to INF = same as 4?
- 0xB6F0E0 - [float] Car View Distance (arm length)
- 0xB6F0E8 - [float] True View Distance (true arm length)

Ignored

0xB7CD9C - Ignored pointer (CIgnored).

- +0x1E = [byte/boolean] Is player ignored by cops
- +0x298 = [byte/boolean] Is player ignored by everyone

Pools

See the Data Pools functions in the Function Memory Addresses (SA) section.

0x550F10 - AllocatePools function.

- 00B74484 - PtrNode Single
- 00B74488 - PtrNode Double
- 00B7448C - EntryInfoNode
- 00B74490 - Peds
- 00B74494 - Vehicles
- 00B74498 - Buildings
- 00B7449C - Objects
- 00B744A0 - Dummys
- 00B744A4 - ColModel
- 00B744A8 - Task
- 00B744AC - Event
- 00B744B0 - PointRoute
- 00B744B4 - PatrolRoute
- 00B744B8 - NodeRoute
- 00B744CC - TaskAllocator
- 00B744C0 - PedIntelligence
- 00B744C4 - PedAttractors

Target

0xB6F3B8 = Pointer to Target.

- +0x79C = Targetted CPed:
  - 0 = no cped targetted
- +0xC0 = Pointer to last object (ped, car, maybe others) you collided with

Handling

0xC2B9DC - Handling Block Start. Each slot has 224 bytes of data.

- +0x0 = [dword] Index/Identifier
- +0x4 = fMass
- +0x8 = 1.0 / fMass
- +0xC = fTurnMass
- +0x10 = fDragMult
- +0x14 = CentreOfMass.x
- +0x18 = CentreOfMass.y
- +0x1C = CentreOfMass.z
- +0x20 = [byte] nPercentSubmerged
- +0x24 = fMass * 8.0000001e-1 / nPercentSubmerged
- +0x28 = fTractionMultiplier
- +0x74 = [byte] TransmissionData.nDriveType
- +0x75 = [byte] TransmissionData.nEngineType
- +0x76 = [byte] TransmissionData.nNumberOfGears
- +0x7C = TransmissionData.fEngineAcceleration (Multiplied by 3.9999999e-4)
- +0x80 = TransmissionData.fEngineInertia
- +0x84 = TransmissionData.fMaxVelocity (Multiplied by 5.5555599e-3)
- +0x94 = fBrakeDeceleration (Multiplied by 3.9999999e-4)
- +0x98 = fBrakeBias
- +0x9C = [byte] bABS
- +0xA0 = fSteeringLock
- +0xA4 = fTractionLoss
- +0xA8 = fTractionBias
- +0xAC = fSuspensionForceLevel
- +0xB0 = fSuspensionDampingLevel
- +0xB4 = fSuspensionHighSpdComDamp
- +0xB8 = Suspension upper limit
- +0xBC= Suspension lower limit
- +0xC0 = Suspension bias between front and rear
- +0xC4 = Suspension anti-dive multiplier
- +0xC8 = fCollisionDamageMultiplier (multiplier not yet found)

- +0xCC = [hex] modelFlags
- +0xD0 = [hex] handlingFlags
- +0xD4 = fSeatOffsetDistance
- +0xD8 = [dword] nMonetaryValue
- +0xDC = [byte] Front lights
- +0xDD = [byte] Rear lights
- +0xDE = [byte] Vehicle anim group

Controls

0xB73458 - Start of controls block.

- +0x20 = [word] Accelerate:
  - 0 = off
  - 255 = on
- +0x22 = [word] Brake

Rockets

The rocket pool contains info on launched rockets (for example, Hydra rockets).

0xC891A8 - Rocket pool start. Each slot has 36 bytes of data. There are 32 elements in the pool.

- +0 = [dword] Rocket type:
  - 16 = none
  - 17 = tear gas
  - 19 = normal
  - 20 = heatseeking
  - 39 = remote explosives
  - 58 = flare
- +4 = [dword] Pointer to launching entity
- +8 = [dword] Pointer to target vehicle (when heatseeking), 0 otherwise
- +16 = [byte] Does rocket exist?
  - 0 = exploded/does not exist
  - 1 = travelling
- +20 = [float] X-axis position
- +24 = [float] Y-axis position
- +28 = [float] Z-axis position

Bullets

0xC88740 - Bullet pool start.

- +12 = [byte] Bullet exists
  - 0 = Does not exist
  - 1 = Exists
- +16 = [float] X-axis position

- +20 = [float] Y-axis position
- +24 = [float] Z-axis position

Note: It works only for Sniper Rifle

Race Checkpoints

The checkpoints block that are used in the "illegal street racing" mini-games.

0xC7F158 - Checkpoint block start. Each block is 38 bytes, but theres always only two at a time.

- +0 = [byte] Type of checkpoint
- +2 = [byte] RGBA color value
- +4 = [float] X-axis Position
- +8 = [float] Y-axis Position
- +12 = [float] Z-axis Position
- +16 to +24 = [float] Rotation Matrix (direction from this checkpoint to the next, all floats)
- +32 = [float] Checkpoint radius

Garages and Parking

Note, that the memory location of garages can vary depending on the scm script you use.

There are 50 garages in the game. Each garage has:-

- Position
- Details
- Usage information
- Location in game
- Location of door
- Width
- Depth
- Height
- Direction it looks
- Coordinates of lower left corner
- Coordinates of upper right corner,
- Usable by the player
- Which property (safe house) it belongs
- Number of vehicles which can be parked inside
- The door state (closed, opening, open and closing)

These are found in the garage object of 212 bytes. The memory locations where the garages start are:

- 0x96C048 (start of first garage)
- +0xD4 (offset for second garage - offset this much again for third garage, again for fourth, etc.)
- 0x96C120 (start of final garage)

(Tested using non-patched original v1.0 German EXE with English language option selected, and original SCM file.)

(UZI-I Tested Player Garage and Pay'n'Spray using Hoodlum Crack EXE with an Blank SCM)

Here is the known garage offsets:

- +0 = [float] X Coord of the Garage Lower Left corner
- +4 = [float] Y Coord of the Garage Lower Left corner
- +8 = [float] Z Coord of the Garage Lower Left corner
- +12 = [float] X Value of direction vector 1
- +16 = [float] Y Value of direction vector 1
- +20 = [float] X Value of direction vector 2
- +24 = [float] Y Value of direction vector 2
- +28 = [float] Top Z Coord. of the garage
- +32 = [float] Normalized Width of the garage
- +36 = [float] Normalized Depth of the garage
- +40 = [float] Left Border (X) corrdinate
- +44 = [float] Right Border (X) corrdinate
- +48 = [float] Front Border (Y) corrdinate
- +52 = [float] Back Border (Y) corrdinate
- +56 = [float] Garage Door Position
- +60 = [dword] unknown (Timer)
- +64 = [dword] unknown (not saved)
- +68 = [chars] Garage Name (7 bytes + nul)
- +76 = [byte] Garage Type
- +77 = [byte] Garage Door State values:
  - 0 = closed
  - 1 = open
  - 2 = closing
  - 3 = opening
- +78 = [byte] Door Flags
  - 0x01 = used mod shop (?)
  - 0x02 = inactive door
  - 0x04 = used Pay'n'Spray (?)
  - 0x08 = small door (reflective?)
  - 0x10 = up and in door
  - 0x20 = camera follows player
  - 0x40 = door is closed flag
  - 0x80 = girlfriend PnS
- +79 = [byte] Original Type

The direction vector 3 is completely left out, I think because the garages are always even to the ground. I think that is also why the Z values of the direction vectors are also left-out.

Note: Direction Vectors marked above may be Quaternions.

Here are the static Addresses of the Garage Blocks, and to which garage they belong:

- 0x96C048 - Commerce Region, Loading Bay Garage (Life's a Beach)
- 0x96C120 - LSPD Police Impound Garage
- 0x96C1F8 - Mission Garage near El Corona (Los Desperados)
- 0x96C2D0 - Eight Ball Autos near El Corona
- 0x96C3A8 - Mission Garage near El Corona (Cesar Vialpando)
- 0x96C480 - Player Garage: El Corona
- 0x96C558 - LS Burglary Garage near Playe del Seville
- 0x96C630 - LowRider Tuning Garage in Willowfield
- 0x96C708 - Pay 'n' Spray in Idlewood
- 0x96C7E0 - Player Garage: Johnson House
- 0x96C8B8 - Pay 'n' Spray in Temple
- 0x96C990 - Transfender in Temple
- 0x96CA68 - Pay 'n' Spray in Santa Maria Beach
- 0x96CB40 - Player Garage: Santa Maria Beach
- 0x96CC18 - Player Garage: Mulholland
- 0x96CCF0 - Wheel Archangels in Ocean Flats
- 0x96CDC8 - Mission Garage in Ocean Flats (T-Bone Mendez)
- 0x96CEA0 - Player Garage: Hashbury
- 0x96CF78 - Transfender near Wang Cars in Doherty
- 0x96D050 - Pay 'n' Spray near Wang Cars in Doherty
- 0x96D128 - SF Burglary Garage, Loading Bay near Doherty
- 0x96D200 - Player Garage: Doherty
- 0x96D2D8 - Mission Garage in Doherty Garage
- 0x96D3B0 - Woozie's Mission Garage in Chinatown (Ran Fa Li)
- 0x96D488 - Michelle's Pay 'n' Spray in Downtown
- 0x96D560 - Player Garage: Calton Heights
- 0x96D638 - SFPD Police Impound Garage
- 0x96D710 - Pay 'n' Spray in Juniper Hollow
- 0x96D7E8 - Player Garage: Paradiso
- 0x96D8C0 - LVPD Police Impound Garage
- 0x96D998 - Airport Plane Garage in Las Venturas
- 0x96DA70 - LV Burglary Garage near Camel's Toe
- 0x96DB48 - Pay 'n' Spray near Royal Casino
- 0x96DC20 - Transfender in come-a-lot
- 0x96DCF8 - Player Garage: Rockshore West
- 0x96DDD0 - Welding Wedding Bomb-workshop in Emerald Isle
- 0x96DEA8 - Pay 'n' Spray in Redsands East
- 0x96DF80 - Player Garage: Redsands West
- 0x96E058 - Player Garage: Prickle Pine

- 0x96E130 - Player Garage: Whitewood Estates
- 0x96E208 - Pay 'n' Spray in El Quebrados
- 0x96E2E0 - Pay 'n' Spray in Fort Carson
- 0x96E3B8 - Player Garage: Fort Carson
- 0x96E490 - Player Garage: Verdant Meadows
- 0x96E568 - Mission Garage in El Castillo del Diablo (Interdiction)
- 0x96E640 - Airport Garage in Verdant Meadows
- 0x96E718 - Mission Garage in Angel Pine (Puncture Wounds)
- 0x96E7F0 - Pay 'n' Spray in Dillimore
- 0x96E8C8 - Player Garage: Palomino Creek
- 0x96E9A0 - Player Garage: Dillimore

Static Mem. Locations for garages:

- 0x96ABD8 - Johnson House Car 1
- 0x96AC18 - Johnson House Car 2
- 0x96AC58 - Johnson House Car 3
- 0x96AC98 - Johnson House Car 4
- 0x96ACD8 - Santa Maria Beach Car 1
- 0x96AD18 - Santa Maria Beach Car 2
- 0x96AD58 - Santa Maria Beach Car 3
- 0x96AD98 - Santa Maria Beach Car 4
- 0x96ADD8 - Rockshore West Car 1
- 0x96AE18 - Rockshore West Car 2
- 0x96AE58 - Rockshore West Car 3
- 0x96AE98 - Rockshore West Car 4
- 0x96AED8 - Fort Carson Car 1
- 0x96AF18 - Fort Carson Car 2
- 0x96AF58 - Fort Carson Car 3
- 0x96AF98 - Fort Carson Car 4
- 0x96AFD8 - Verdant Meadows Car 1
- 0x96B018 - Verdant Meadows Car 2
- 0x96B058 - Verdant Meadows Car 3
- 0x96B098 - Verdant Meadows Car 4
- 0x96B0D8 - Dillimore Car 1
- 0x96B118 - Dillimore Car 2
- 0x96B158 - Dillimore Car 3
- 0x96B198 - Dillimore Car 4
- 0x96B1D8 - Prickle Pine Car 1
- 0x96B218 - Prickle Pine Car 2
- 0x96B258 - Prickle Pine Car 3

- 0x96B298 - Prickle Pine Car 3
- 0x96B2D8 - Whitewood Estates Car 1
- 0x96B318 - Whitewood Estates Car 2
- 0x96B358 - Whitewood Estates Car 3
- 0x96B398 - Whitewood Estates Car 4
- 0x96B3D8 - Palomino Creek Car 1
- 0x96B418 - Palomino Creek Car 2
- 0x96B458 - Palomino Creek Car 3
- 0x96B498 - Palomino Creek Car 4
- 0x96B4D8 - Redlands West Car 1
- 0x96B518 - Redlands West Car 2
- 0x96B558 - Redlands West Car 3
- 0x96B598 - Redlands West Car 4
- 0x96B5D8 - El Corona Car 1
- 0x96B618 - El Corona Car 2
- 0x96B658 - El Corona Car 3
- 0x96B698 - El Corona Car 4
- 0x96B6D8 - MulHolland Car 1
- 0x96B718 - MulHolland Car 2
- 0x96B758 - MulHolland Car 3
- 0x96B798 - MulHolland Car 4
- 0x96B7D8 - LSPD Impound Car 1
- 0x96B818 - LSPD Impound Car 2
- 0x96B858 - LSPD Impound Car 3
- 0x96B898 - LSPD Impound unused
- 0x96B8D8 - SFPD Impound Car 1
- 0x96B918 - SFPD Impound Car 2
- 0x96B958 - SFPD Impound Car 3
- 0x96B998 - SFPD Impound unused
- 0x96B9D8 - LVPD Impound Car 1
- 0x96BA18 - LVPD Impound Car 2
- 0x96BA58 - LVPD Impound Car 3
- 0x96BA98 - LVPD Impound usued
- 0x96BAD8 - Calton Heights Car 1
- 0x96BB18 - Calton Heights Car 2
- 0x96BB58 - Calton Heights Car 3
- 0x96BB98 - Calton Heights Car 4
- 0x96BBD8 - Paradiso Car 1
- 0x96BC18 - Paradiso Car 2
- 0x96BC58 - Paradiso Car 3

- 0x96BC98 - Paradiso Car 4
- 0x96BCD8 - Doherty Car 1
- 0x96BD18 - Doherty Car 2
- 0x96BD58 - Doherty Car 3
- 0x96BD98 - Doherty Car 4
- 0x96BDD8 - Hashbury Car 1
- 0x96BE18 - Hashbury Car 2
- 0x96BE58 - Hashbury Car 3
- 0x96BE98 - Hashbury Car 4
- 0x96BED8 - Verdant Meadows Airport Car 1
- 0x96BF18 - Verdant Meadows Airport Car 2
- 0x96BF58 - Verdant Meadows Airport Car 3
- 0x96BF98 - Verdant Meadows Airport Car 4

Offsets:

- +0 = [float] X Coord
- +4 = [float] Y Coord
- +8 = [float] Z Coord
- +14 = [word] BPDPEPFP coding
- +16 = [word] Car ID
- +47 = [byte] Body Color ordinal
- +48 = [byte] Stripe Color ordinal
- +60 = [float] Car Angle

Interface

- 0xBAB22C - [byte] Health bar/red text/enemy marker/anything red color (RGBA, 4 bytes)
- 0xBAB230 - [byte] Money font color/vehicle entry name/green text/anything green color (RGBA, 4 bytes)
- 0xBAB238 - [byte] White text color (RGBA, 4 bytes)
- 0xBAB240 - [byte] Main menu title border (RGBA, 4 bytes)
- 0xBAB244 - [byte] Wanted level color (RGBA, 4 bytes)
- 0xBAB24C - [byte] Radio station text color (RGBA, 4 bytes)
- 0xBAB258 - [byte] Yellow blip/text color (RGBA, 4 bytes)

Menu

The following addresses have been found:

0xBA6748 - Base address.

- +0x15D = [byte] Current Menu ID
- +0x78D = [byte] Show menu item hover
- +0x54 = [dword] Selected menu item
- +0xE9 = [byte] Main menu switch (startup menu/menu when playing)
- +0x84 = [dword] Language

- +0x15F = [byte] Selected savegame
- +0x24 = [dword] Radar mode
- +0x64 = [float] Map zoom
- +0x68 = [float] Map x position
- +0x6C = [float] Map y position
- +0x5C = [byte] Player in menu?

Menu IDs

Known Menu IDs (get ID at 0xBA68A5):

- 0 = Stats
- 1 = Start game
- 2 = Brief
- 3 = Audio options
- 4 = Display settings
- 5 = Map
- 6 = Question start new game
- 7 = Game selection
- 8 = Question load mission pack
- 9 = Load game
- 10 = Delete game
- 11 = Question load save game
- 12 = Question delete game
- 13 = Loads first savegame? *crash
- 14 = Delete successful
- 15 = Delete successful
- 16 = Save game
- 17 = Question save
- 18 = Save successful
- 19 = Save successful
- 20 = Save game ok
- 21 = Load game ok
- 22 = Game affected, do not save
- 23 = Display default settings
- 24 = Audio default settings
- 25 = Controller default settings
- 26 = User track options
- 28 = Language
- 29 = Save game ok
- 30 = Save unsuccessful
- 31 = Load game (save unsuccessful)

- 32 = Load unsuccessful, file corrupted
- 33 = Options
- 34 = Main menu
- 35 = Quit game
- 36 = Controller setup
- 37 = Redefine controls
- 38 = Foot/vehicle controls
- 39 = Mouse settings
- 40 = Joypad settings
- 41 = Game running main menu
- 42 = Quit game
- 43 = Empty

SCM related

- 0xA49960 - Start of the SCM block (0xA49960 + (4 * varnumber) is that particular variable)
- 0xA7A6A0 - Start of the mission block (69000 bytes)
- 0x464080 - GetOpcodeParameters()
- 0xA447F4 - Command count
- 00469F00 - CRunningScript_ProcessOneCommand
- 0x464080 - CRunningScript_CollectParameters
- 0x4859D0 - CRunningScript_UpdateCompareFlag
- 0x469390 - Game_Script_Thread struct
- 0xA43C78 - Where the routine above stores opcode parameters values. Max 16 paramters for an opcode it seems
- 0x8A6168 - "Master" jumptable, each dword points to one of 27 different functions, each one handling approx 100 opcodes
- 0x466C50 - Opcodes 0000 - 0063. Array of dword, each pointing to the function for that opcode
- 0x468364 - Opcodes 0064 - 00C4. Array of dword, each pointing to the function for that opcode
- 0x469E4C - Opcodes 00D6 - 0129. Array of byte, each byte is an index for the array of dword at 0x469DD4, which points to the opcode function
- 0x47D1B4 - Opcodes 0137 - 018F. Array of byte, each byte is an index for the array of dword at 0x47D0F4, which points to the opcode function
- 0x47DFE0 - Opcodes 0190 - 01F3. Array of byte, each byte is an index for the array of dword at 0x47DF58, which points to the opcode function
- 0x47F304 - Opcodes 01F4 - 0256. Array of byte, each byte is an index for the array of dword at 0x47F24C, which points to the opcode function
- 0x47FA04 - Opcodes 0292 - 02B8. Array of byte, each byte is an index for the array of dword at 0x47F9BC, which points to the opcode function
- 0x480FD8 - Opcodes 02BE - 031D. Array of byte, each byte is an index for the array of dword at 0x480F10, which points to the opcode function
- 0x4836B8 - Opcodes 0320 - 0382. Array of byte, each byte is an index for the array of dword at 0x483600, which points to the opcode function

(No time to finish now, will finish later)

Threads

0xA8B430 - Start of the threads pool. There are two queues: the active threads and inactive ones.
0xA8B42C - Pointer to the first active SCM thread.
0xA8B428 - Pointer to the first inactive SCM thread.

Each thread has size of 224 (0xE0) bytes.

- +0 = [void*] Pointer to the next thread in a queue
- +4 = [void*] Pointer to the previous thread in a queue
- +8 = [char] Thread name given by the opcode 03A4, char 8
- +16 = [dword] Thread base IP (used in the missions and external scripts to calculate a global address of a local jump offset)
- +20 = [dword] Current IP
- +24 = [dword] Return stack (stores the current IP when a gosub executed, dword 8)
- +56 = [word] Last item index of the return stack
- +60 = [dword] Local variables array, dword 32
- +188 = [dword] Automatically incrementing timers, dword 2
- +196 = [boolean] Thread active flag
- +197 = [boolean] IF result
- +198 = [boolean] Mission flag
- +199 = [boolean] External script flag
- +200 = [boolean] Unknown flag (in menu?). Used in 03E5
- +201 = [boolean] Unknown flag (ID of an assigned script?)
- +204 = [dword] Wakeup time (set by 0001)
- +208 = [word] IF number (set by 00D6)
- +210 = [boolean] Not flag (if a condition to check is negative â€“ any opcodes higher than 0x7FFF)
- +211 = [boolean] Wasted or busted check enabled flag (set by 0111); **only for missions**
- +212 = [boolean] Player is wasted or busted flag; **only for missions**
- +216 = [dword] Skip scene IP (used by opcodes 0707, 0701)
- +220 = [boolean] Mission flag

External Scripts Info

0xA47B60 - Start of the external scripts info pool. There are 82 elements with 32 bytes of size each

- +0 = [dword] Script IP
- +4 = [word] Status (can be obtained by 0926)
- +6 = [word] Index in SCM (a number as defined in the scm header)
- +8 = [char] Name, char 20
- +28 = [dword] Size

0xA485A0 - [dword] Size of the largest external script
0xA485A4 - [dword] Total scripts count

Restart Locations

Also see: opcodes 016C and 016D / save file block 8

An unmodded game has 7 restart locations for "busted" and 8 for "wasted". The memory structure suggests a limit of 10 for both of these.

- 0xa43268: dword -- number of busted structures
- 0xa4326c: dword -- number of wasted structures
- 0xa43270: float[10] -- town numbers for busted structures (1 LS / 2 Country+SF / 3 Desert+LV)
- 0xa43298: float[10] -- angles for busted structures
- 0xa432c0: float[10] -- town numbers for wasted structures (1 LS / 2 Country+SF / 3 Desert+LV)
- 0xa432e8: float[10] -- angles for wasted structures
- 0xa43310: byte[8] -- unknown -- seems to be always the same: 0A D7 A3 39 00 00 00 00
- 0xa43318: float[3][10] -- x,y,z - respawn coords for wasted structures
- 0xa43390: float[3][10] -- x,y,z - respawn coords for busted structures
- 0xa43408: byte[12] -- unknown; matching 12 unknown bytes of save block 8, 0x01 after Busted structures
- 0xa43414: byte[12] -- unknown; matching 12 unknown bytes of save block 8, 0x0F after Busted structures
- 0xa43420: [end]

Notes:

- Town nos. and angles have the busted structures first but coords have the wasted structures first.
- I'm not sure about the end of this structure, but I couldn't recognize anything from the according save block 8 after 0xa43420.

Misc

0xA4892C - Start of the pool stored the flipped vehicles handles. There are 6 elements in there, with each of them:

- +0 = [dword] Vehicle handle to check if it flipped. Stored by opcode 0190.
- +4 = [dword] Time in ms passed from the moment a vehicle flipped. Used by opcode 018F

00A90850 - Start of the mission cleanup list. This list keeps the handles of any entities created during a mission. When the opcode 00D8 executed (normally it happens at the end of any mission), the game reads this list and destroys everything being stored there. Maximum items on the list is 75. Each item has the following structure:

- +0 = [byte] Entity type:
  - 1 - vehicle
  - 2 - actor
  - 3 - object
  - 4 - particle
  - 5 - group (062F)
  - 7 - AS_origin (061D)
  - 8 - action_sequence
  - 9 - decision maker
  - 11 - searchlight
  - 13 - txd_dictionary
- +4 = [dword] entity handle (an index in the proper pool)

Weather Codes

0xC81318 - [word] Weather lock (by AlienX).
0xC8131C - [word] Upcoming weather.
0xC81320 - [word] Current weather.

The following values tie up with the sections in data/timecycp.dat. There are several different kinds of weathers (including underwater), and the current weather affects viewing distance, sky colour, fog intensity, and other things like that. The appearance of each weather is time-dependent too.

Weather Values:

- 0 = EXTRASUNNY_LA
- 1 = SUNNY_LA
- 2 = EXTRASUNNY_SMOG_LA
- 3 = SUNNY_SMOG_LA
- 4 = CLOUDY_LA
- 5 = SUNNY_SF
- 6 = EXTRASUNNY_SF
- 7 = CLOUDY_SF
- 8 = RAINY_SF
- 9 = FOGGY_SF
- 10 = SUNNY_VEGAS
- 11 = EXTRASUNNY_VEGAS (heat waves)
- 12 = CLOUDY_VEGAS
- 13 = EXTRASUNNY_COUNTRYSIDE
- 14 = SUNNY_COUNTRYSIDE
- 15 = CLOUDY_COUNTRYSIDE
- 16 = RAINY_COUNTRYSIDE
- 17 = EXTRASUNNY_DESERT
- 18 = SUNNY_DESERT
- 19 = SANDSTORM_DESERT
- 20 = UNDERWATER (greenish, foggy)
- 21 = EXTRACOLOURS_1 (very dark, gradiented skyline, purple) Used for interiors?
- 22 = EXTRACOLOURS_2 (very dark, gradiented skyline, green) Used for interiors?

The following are not mentioned in that file, but can be used anyway:

- 23 to 26 = variations of pale orange
- 27 to 29 = variations of fresh blue
- 30 to 32 = variations of dark, cloudy, teal
- 33 = dark, cloudy, brown
- 34 = blue/purple, regular

- 35 = dull brown
- 36 to 38 = bright, foggy, orange
- 39 = extremely bright
- 40 to 42 = blue/purple cloudy
- 43 = dark toxic clouds
- 44 = black/white sky
- 45 = black/purple sky

Warning: Setting these values to anything higher will result in things like black screen, flickering, really red, etc.

Dependencies

- Car ptr = player ptr when on foot.

Note: This depends on which address for the pointer is being used, if the car pointer appears to be the same as the player pointer on foot, then you may be using a camera-related target pointer.

- CPed block size = 0x7C4 bytes.
- CVehicle block size = 0x0A18 bytes.

External links

- GTAForums: GTASA Memory Addresses

v • d • e	Grand Theft Auto: San Andreas [hide]
File Formats	.col • .cfg • .cut • .dff • .dat • .fxp • .gxt • .ide • .ifp • .img • .ipl • nodes*.dat • .rep • .rrr • .scm • .txd
Documentation	Audio • Cutscenes • Handling.cfg • Map Listing • Mission Packs • Opcodes • Paths • Replays • Saves
Tools	CLEO • Collision File Editor II • ENBSeries • G-Tools • IMG Tool • Limit Adjuster • Map Editor • PathViewer • San Andreas Audio Toolkit • Sanny Builder • TXD Workshop
Tutorials	San Andreas v2.0 Modding • How to create a mission • How to create a thread • How to use Map Editor
Modifications	Design Your Own Mission • Gostown Paradise • GTA: United • Myriad Islands
Multiplayer	gtaTournament • Multi Theft Auto • San Andreas Multiplayer • (more...)
Useful links	Community portal • Discussion forums • Mods on GTAGarage.com • Opcodes database

Categories: Articles needing rewrite | GTA SA | Memory Addresses

navigation

- Main Page
- Tutorials and guides
- Documentation
- Recent changes
- Random page
- Help

games

- Grand Theft Auto IV
- GTA Vice City Stories
- GTA Liberty City Stories
- GTA San Andreas
- GTA Vice City
- Grand Theft Auto III
- Grand Theft Auto 2
- Grand Theft Auto

search

Go Search

toolbox

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link

network

- GTA Network
- GTA Forums
- GTA IV
- GTA San Andreas
- GTA Vice City
- GTA III
- GTA Garage