Ryan Cohen

Nicholas Matthews

CSCSE 451

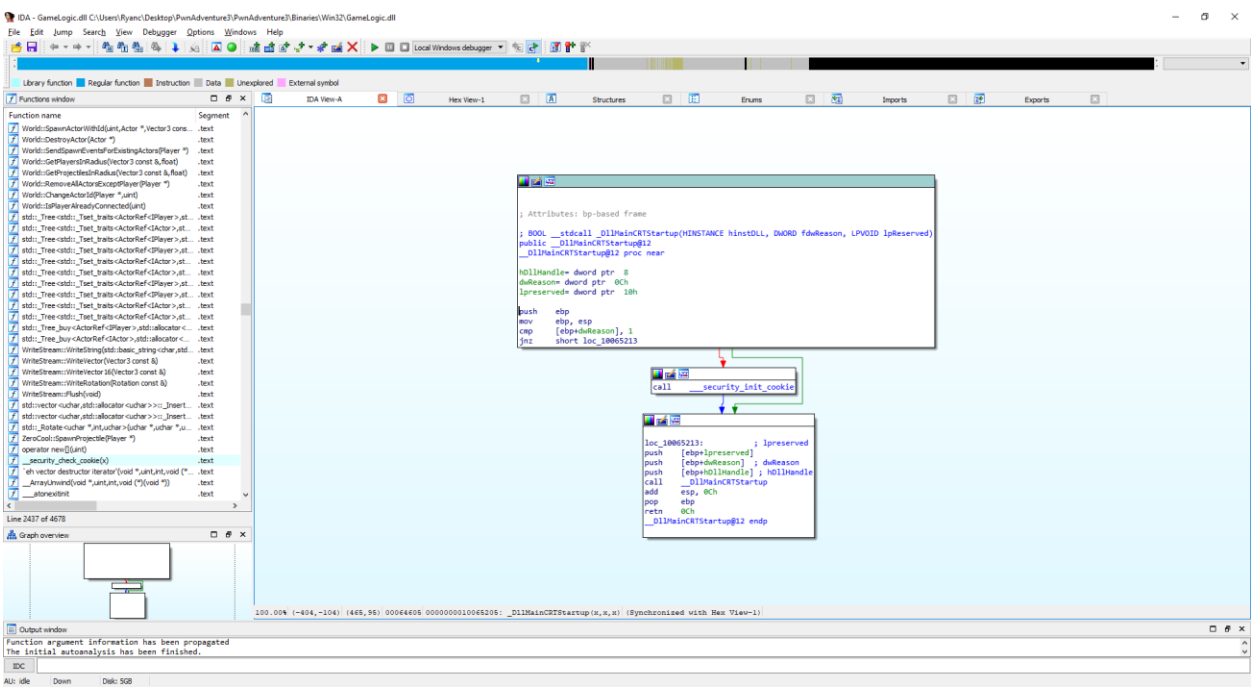
Team hash: 8cc35d5b4568e197443c31da0aec47ac

Team name: cohen_matthews

HW4

The goal of this homework was to play the game PwnAdventure3 and find someway to reverse-engineer the game to receive the flag. We were both playing on Windows and not on Linux, we had to use Windows tools in order to achieve this.

The first tool we used was “IDA” as we could open binaries files in windows with the program. A good spot to start when we searched for tutorials online was to modify the player’s running speed/ jump height. With that in mind, we decided a good place to start would be GameLogic.dll.



This is what we saw when we first opened the logic in IDA.

Digging around in the subclasses we found the player subclass.

640	std::_Tset_traits<ActorRef...	00000001		struct __cppobj {}
662	std::set<ActorRef<IPlayer...	00000008	Auto	struct __cppobj : std::_Tree<std::_Tset_traits<ActorRef<IPlayer>,std::less<ActorRef<IPlayer> >,std::allocator...
681	World	0000002C		struct __cppobj {WorldVtbl *vfptr;std::set<ActorRef<IPlayer>,std::less<ActorRef<IPlayer> >,std::allocator<Ac...
709	Player	000001DC	Auto	struct __cppobj : Actor, IPlayer {unsigned int m_characterId;std::basic_string<char,std::char_traits<char>,std::a...
710	WorldVtbl	00000108		struct {void *(__thiscall *__vecDelDtor)(World *this, unsigned int); _BYTE gap4[32];void (__thiscall *Activate)(Worl...
711	std::_Vector_val<std::_Sim...	0000000C	Auto	struct __cppobj : std::_Container_base0 {IPlayer **_Myfirst;IPlayer **_Mylast;IPlayer **_Myend;}
712	std::_Vector_alloc<0,std::_...	0000000C	Auto	struct __cppobj : std::_Vector_val<std::_Simple_types<IPlayer *> > {}
713	std::vector<IPlayer *,std::...	0000000C	Auto	struct __cppobj : std::_Vector_alloc<0,std::_Vec_base_types<IPlayer *,std::allocator<IPlayer *> > > {}
729	FastTravelDestinationVtbl	00000004		struct {bool (__thiscall *IsAvailable)(FastTravelDestination *this, Player *);}

Clicking on it led us to this window.

```
00000000 Player          struc ; (sizeof=0x1DC, align=0x4, copyof_709)
00000000 baseclass_0     Actor ?
00000070 baseclass_70    IPlayer ?
00000074 m_characterId   dd ?
00000078 m_playerName    std::basic_string<char,std::char_traits<char>,std::allocator<char> > ?
00000090 m_teamName      std::basic_string<char,std::char_traits<char>,std::allocator<char> > ?
000000A8 m_avatarIndex   db ?
000000A9                 db ? ; undefined
000000AA                 db ? ; undefined
000000AB                 db ? ; undefined
000000AC m_colors        dd 4 dup(?)
000000BC m_inventory     std::map<IItem *,ItemAndCount,std::less<IItem *>,std::allocator<std::pair<IItem * const,ItemAndCount> > > ?
000000C4 m_pickups       std::set<std::basic_string<char,std::char_traits<char>,std::allocator<char> >,std::less<std::basic_string<char,std::char_traits<char>,std::allocator<char> > >,std::allocator<std::basic_strin
000000CC m_cooldowns     std::map<IItem *,float,std::less<IItem *>,std::allocator<std::pair<IItem * const,float> > > ?
000000D4 m_circuitInputs std::map<std::basic_string<char,std::char_traits<char>,std::allocator<char> >,unsigned int,std::less<std::basic_string<char,std::char_traits<char>,std::allocator<char> > >,std::allocator<std
000000DC m_circuitOutputs std::map<std::basic_string<char,std::char_traits<char>,std::allocator<char> >,std::vector<bool,std::allocator<bool> >,std::less<std::basic_string<char,std::char_traits<char>,std::allocator<
000000E4 m_admin         db ?
000000E5 m_pvpEnabled    db ?
000000E6 m_pvpDesired    db ?
000000E7                 db ? ; undefined
000000E8 m_pvpChangeTimer dd ?
000000EC m_pvpChangeReportedTimer dd ?
000000F0 m_changingServerRegion db ?
000000F1                 db ? ; undefined
000000F2                 db ? ; undefined
000000F3                 db ? ; undefined
000000F4 m_currentRegion std::basic_string<char,std::char_traits<char>,std::allocator<char> > ?
0000010C m_changeRegionDestination std::basic_string<char,std::char_traits<char>,std::allocator<char> > ?
00000124 m_aiZones       std::set<std::basic_string<char,std::char_traits<char>,std::allocator<char> >,std::less<std::basic_string<char,std::char_traits<char>,std::allocator<char> > >,std::allocator<std::basic_strin
0000012C m_mana          dd ?
00000130 m_manaRegenTimer dd ?
00000134 m_healthRegenCooldown dd ?
00000138 m_healthRegenTimer dd ?
0000013C m_countdown     dd ?
00000140 m_remoteLookPosition Vector3 ?
0000014C m_remoteLookRotation Rotation ?
00000158 m_equipped      dd 10 dup(?)            ; offset
00000180 m_currentSlot   dd ?
00000184 m_questStates   std::map<IQuest *,PlayerQuestState,std::less<IQuest *>,std::allocator<std::pair<IQuest * const,PlayerQuestState> > > ?
0000018C m_currentQuest  dd ?                    ; offset
00000190 m_walkingSpeed  dd ?
00000194 m_jumpSpeed     dd ?
00000198 m_jumpHoldTime  dd ?
0000019C m_currentNPC    ActorRef<NPC> ?
000001A0 m_currentNPCState std::basic_string<char,std::char_traits<char>,std::allocator<char> > ?
000001B8 m_localPlayer   dd ?                    ; offset
000001BC m_eventsToSend  dd ?                    ; offset
000001C0 m_itemsUpdated  db ?
```

As seen very closely on that screen we made it to the variable offsets where the modifiers we were looking for were located.

00000190 m_walkingSpeed

00000194 m_jumpSpeed

00000198 m_jumpHoldTime

According to some resources online, we had to include the base offset of the class which could be found here as well.

00000070 baseclass_70

The new values would be:

00000120 m_walkingSpeed

00000124 m_jumpSpeed

00000128 m_jumpHoldTime

Next, we needed to find the pointer to the player class. That can be found in ClientWorld.

```
--------
00000000 ClientWorld     struc ; (sizeof=0x34, align=0x4, copyof_1597)
00000000 baseclass_0     World ?
0000002C m_activePlayer  ActorRef<IPlayer> ?
00000030 m_timeUntilNextNetTick dd ?
00000034 ClientWorld     ends
```

2C would be the offset that we need.

After finding the pointer to the player class we need to find the pointer to the world object.

Name	Address	Public
__unwindfunclet$??0World@@QAE@XZ$0	000000001006E250	
__unwindfunclet$??0World@@QAE@XZ$1	000000001006E25B	
__unwindfunclet$??0World@@QAE@XZ$2	000000001006E266	
__ehhandler$??0World@@QAE@XZ	000000001006E271	
__unwindfunclet$??1World@@UAE@XZ$0	000000001006E290	
__unwindfunclet$??1World@@UAE@XZ$1	000000001006E29B	
__unwindfunclet$??1World@@UAE@XZ$2	000000001006E2A6	
__unwindfunclet$??1World@@UAE@XZ$3	000000001006E2B1	
__ehhandler$??1World@@UAE@XZ	000000001006E2BC	
__unwindfunclet$?GetProjectilesInRadius@World@...	000000001006E2F0	
__ehhandler$?GetProjectilesInRadius@World@@QA...	000000001006E309	
__unwindfunclet$?RemoveAllActorsExceptPlayer@W...	000000001006E330	
__unwindfunclet$?RemoveAllActorsExceptPlayer@W...	000000001006E338	
__ehhandler$?RemoveAllActorsExceptPlayer@World...	000000001006E340	
const ClientWorld::`vftable'	00000000100703D4	
const LocalWorld::`vftable'	0000000010076D60	
const ServerWorld::`vftable'	00000000100787C0	
const World::`vftable'	00000000100789D4	
const ClientWorld::`RTTI Complete Object Locator'	0000000010079DD0	
ClientWorld::`RTTI Base Class Descriptor at (0,-1,0,...	0000000010079DE4	
ClientWorld::`RTTI Base Class Array'	0000000010079E00	
ClientWorld::`RTTI Class Hierarchy Descriptor'	0000000010079E0C	
World::`RTTI Class Hierarchy Descriptor'	0000000010079E1C	
World::`RTTI Base Class Descriptor at (0,-1,0,64)'	0000000010079E2C	
World::`RTTI Base Class Array'	0000000010079E48	
LocalWorld::`RTTI Base Class Descriptor at (0,-1,0,...	000000001007EA98	
LocalWorld::`RTTI Base Class Array'	000000001007EAB4	
const LocalWorld::`RTTI Complete Object Locator'	000000001007EAC0	
LocalWorld::`RTTI Class Hierarchy Descriptor'	000000001007EAD4	
ServerWorld::`RTTI Base Class Descriptor at (0,-1,0...	0000000010080104	
ServerWorld::`RTTI Class Hierarchy Descriptor'	0000000010080120	
const ServerWorld::`RTTI Complete Object Locator'	0000000010080130	
ServerWorld::`RTTI Base Class Array'	0000000010080144	
const World::`RTTI Complete Object Locator'	0000000010080290	
World `RTTI Type Descriptor'	000000001008D9D4	
ClientWorld `RTTI Type Descriptor'	000000001008D9E8	
aAvclientworld	000000001008D9F0	
LocalWorld `RTTI Type Descriptor'	00000000100948D0	
aAvlocalworld	00000000100948D8	
ServerWorld `RTTI Type Descriptor'	00000000100979E8	
aAvserverworld	00000000100979F0	
World * GameWorld	0000000010097D7C	

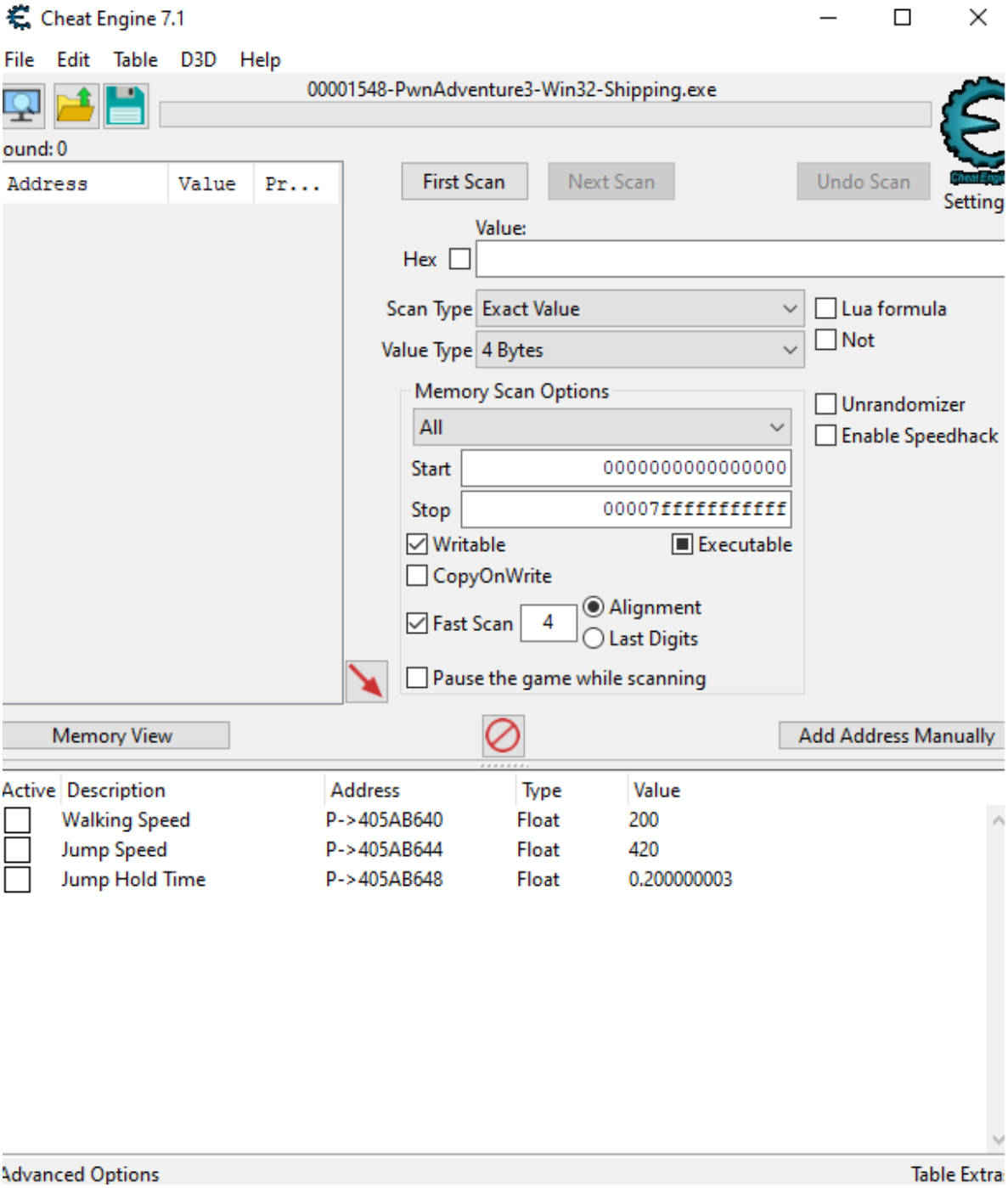
This would be found in a different section than the rest. This section is the “Names” section in IDA and shows the different variables/functions.

```
.data:10097D7C ; World *GameWorld
.data:10097D7C ?GameWorld@@3PAVWorld@@A dd ?
```

We would now need to get the offset from the base address. The base address is 1000000 so it is not just 97D7C.

*We know the base address is that number through the IDA at the top when it mentions that “Imagebase : 10000000”. Imagebase is the address in virtual memory where the executable should be loaded at to avoid any adjustment of jump instructions in the code.

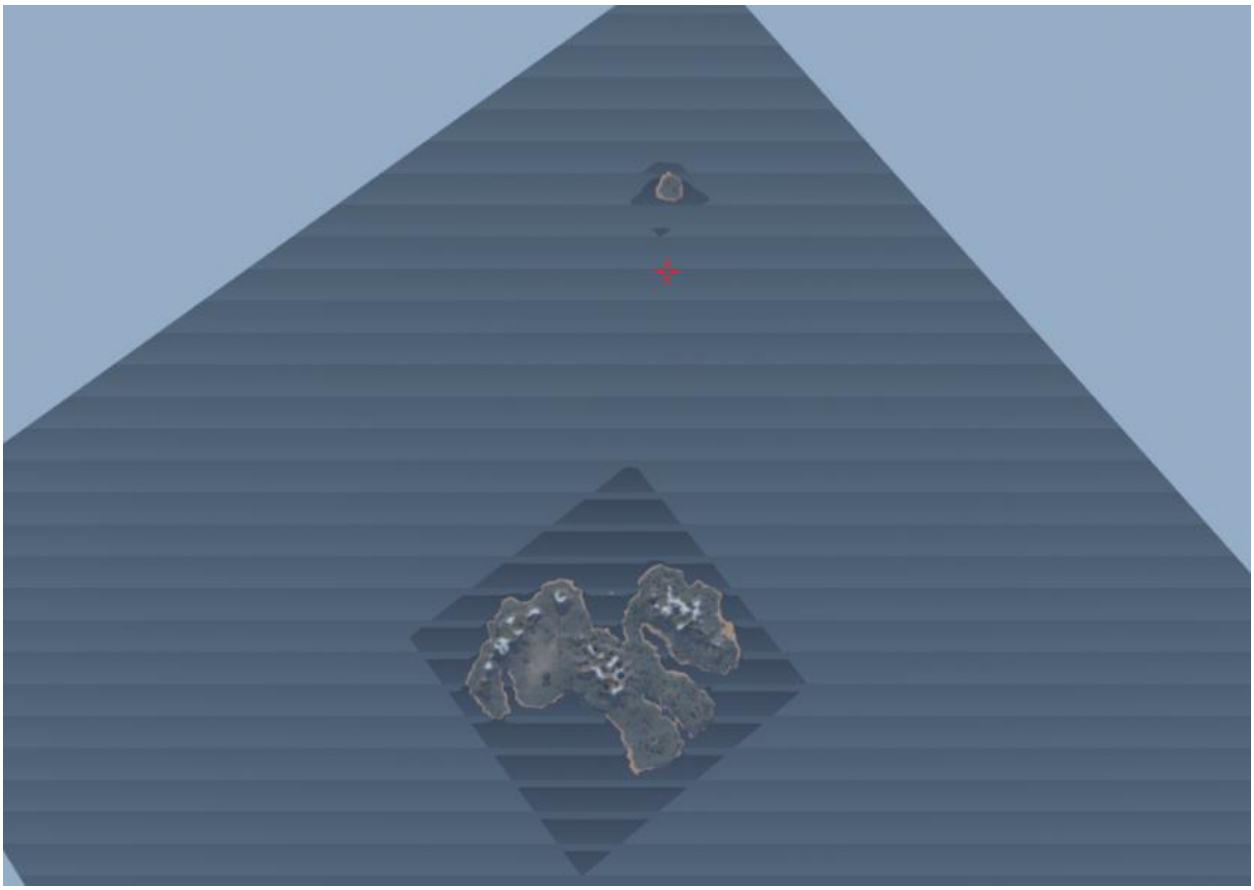
Now in a tool called CheatEngine, we can log into the game and load everything that we found out so far in the Addresses section.



From here we can modify any of our values at will.

Now onto the game. The lowest point value of a flag in the game is the “Until the Cows Come Home” flag so we decided to go try that one.

With that hint, and some other hints on the internet, we learned that the cows were off the main island and teleported to an island in the ocean.



We eventually made it over to the island with our high jump and our fast walking speed.

By talking to a guy on the island and killing the cow, we were able to get the flag.


Unbeearable Revenge
Find the bear's treasure
Inventory
43
38
10
10,797 Pwncoins
Close
HEALTH
100
MANA
100


Unbeearable Revenge
Find the bear's treasure
Inventory
43
38
10
Flag of the Cow
1337 Flag
Bound (no trade or sale)
The key is:
I shouldve used dynamic link
Submit this flag to the scoreboard to get points!
10,797 Pwncoins
Close
HEALTH
100
MANA
100