中華大學資訊工程學系

100 學年度專題製作期末報告

網路遊戲外掛製作

組員：B09402213 王永昌

指導老師：黃雅軒 教授

專題編號: PRJ2011-CSIE-10040

執行期間:100 年 07 月至 101 年 06 月

一、摘要

現今網路遊戲林立，相對於以往的單機遊戲，使得遊戲玩家不再是與電腦做競爭，而是與現實存在的遊戲玩家競爭，使遊戲內容也更加的有挑戰性；然而網路遊戲的興起也帶動另類的賺錢方式：販售遊戲幣與遊戲寶物,遊戲幣、寶物通常是借由擊殺NPC所掉落,網路遊戲為了延長遊戲壽命，往往將遊戲幣、寶物掉落率設定調低，遊戲玩家就需要投入更多的時間去遊戲中賺錢和打寶物。

本專題中設計出自動化的程序，依事先設定的環境在網路遊戲中自動找尋NPC攻擊、交易，來達成自動賺錢和打寶物。也因網路遊戲中環境，而設計較為便利的操作介面。

二、簡介

本專題是針對網路遊戲：大航海時代Online，此款遊戲而製作遊戲外掛，遊戲背景位於中世紀，歐洲歷史中的地理大發現，該時期內，歐洲的船隊出現在世界各處的海洋上,尋找著新的貿易路線和貿易夥伴。本專題使用Visual C# .NET針對遊戲特點，開發新的操作介面，與自動化功能。

三、專題進行方式

- 工作分配

組員	工作與職責
王永昌	專題資料收集 專題技術研究 專題程式撰寫 成果發表與報告

- 實作技術簡介

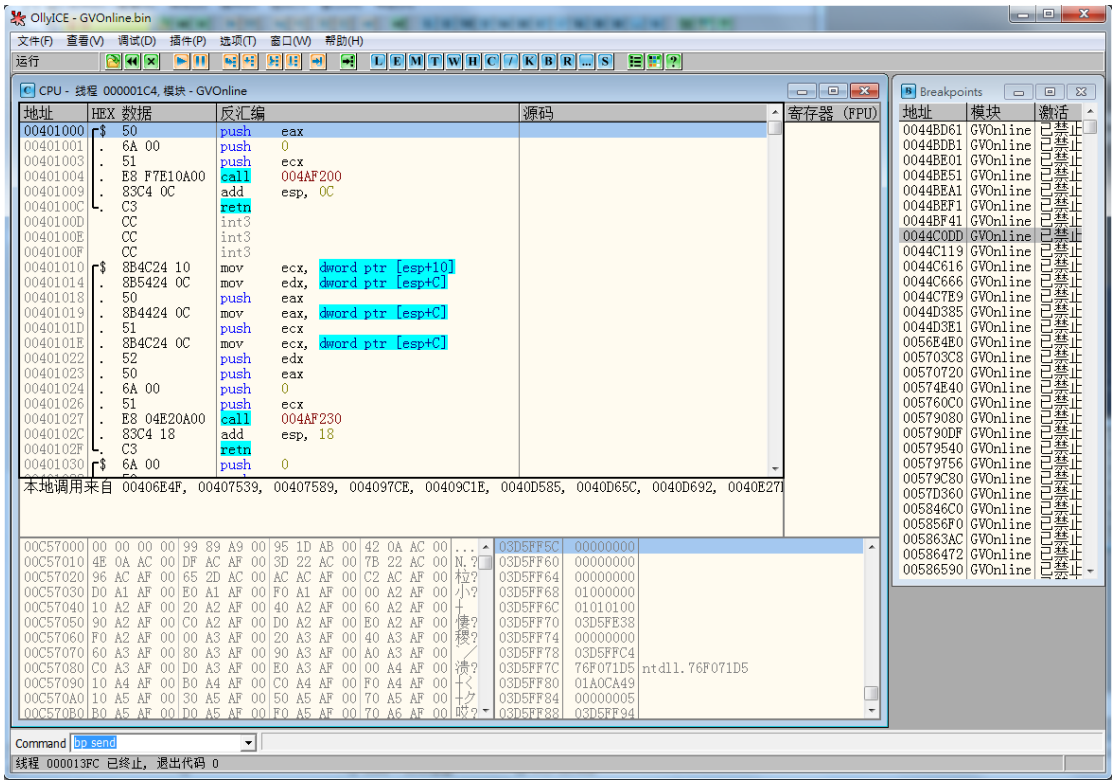
Cheat Engine 是款搜尋遊戲記憶體內容的工具，遊戲中主要的數據資料是由此軟體收集。以下為遊戲中所取得的記憶體內容資料：

Active	Description	Address	Type	Value
☐	==OFFSET 1C0C0	00400000	4 Bytes	9460301
☐	文字訊息	00CCE0AC	4 Bytes	0
☐	忙碌中	00CCE3D8	4 Bytes	0
☐	???	00CCE3E4	4 Bytes	FFFFFFFF
☐	(1-劇情 2-陸戰 4-)	00CCE3E8	4 Bytes	0
☐	海域座標PTR	00CCE3EC	4 Bytes	0626B8B0
☐	海域座標X	P->06273610	4 Bytes	61
☐	海域座標Y	P->06273614	4 Bytes	8
☐	TAB目標type	00CCE404	4 Bytes	2
☐	TAB目標ID	00CCE408	4 Bytes	00000000
☐	TAB目標按鈕數	00CCE458	4 Bytes	0
☐	?	00CCE834	4 Bytes	00AFD874
☐	==OFFSET 1C0C0	00400000	4 Bytes	9460301
☐	場景切換	00CCEEB0	4 Bytes	0
☐	物資-保存的數量	00CD0360	4 Bytes	135
☐	物資-保存的數量	00CD0364	4 Bytes	135
☐	資材-保存的數量	00CD0368	4 Bytes	5
☐	彈藥-保存的數量	00CD036C	4 Bytes	0
☐	==OFFSET 1C0C0	00400000	4 Bytes	9460301
☐	No description	00CD3668	4 Bytes	00000000
☐	連線狀態	00CD374C	4 Bytes	1
☐	伺服器名PTR	00CD37E4	4 Bytes	05A092E0
☐	伺服器名	P->05A092E0	String[10]	戰列艦
☐	選擇角色-角色名PTR	00CD37E8	4 Bytes	05A090E0
☐	選擇角色-角色名	P->05A090E0	String[10]	脫拉庫
☐	玩家ID	00CD37F4	4 Bytes	0004C1FA
☐	?? 身摯?	00CD3800	2 Bytes	768
☐	海上狀況	00CD3804	4 Bytes	0
☐	自動操帆狀態	00CD3809	2 Bytes	0
☐	遊戲中角色名PTR	00CD381C	4 Bytes	05A093A0
☐	遊戲中角色名	P->05A093A0	String[10]	脫拉庫
☐	? ?懽	00CD3822	2 Bytes	4224
☐	戰鬥狀態	00CD3824	Byte	0
☐	國籍	00CD382E	Byte	2
☐	冒exp	00CD3850	4 Bytes	0
☐	商exp	00CD3854	4 Bytes	0
☐	戰exp	00CD3858	4 Bytes	0
☐	==OFFSET 1C0C0	00400000	4 Bytes	9460301
☐	肉搏戰目標ID	00CD3888	4 Bytes	0
☐	行動力	00CD3898	4 Bytes	420
☐	MAX行動力	00CD389C	4 Bytes	755
☐	持有金錢	00CD38A0	4 Bytes	46582432
☐	船員數	00CD38A4	4 Bytes	33
☐	疲勞度/10	00CD38A8	2 Bytes	0
☐	水	00CD38AA	2 Bytes	11
☐	糧食	00CD38AC	2 Bytes	11
☐	彈藥	00CD38AE	2 Bytes	0
☐	資材	00CD38B0	2 Bytes	5
☐	船隻耐久度	00CD38B2	4 Bytes	720
☐	船舵損壞128 船帆破損1~7	00CD38C3	Byte	0
☐	0-正常 1~無法航行	00CD38C4	Byte	0
☐	==OFFSET 1C0C4	00400000	4 Bytes	9460301
☐	座標X	00CD38E0	Float	7081490
☐	座標Z	00CD38E4	Float	0
☐	座標Y	00CD38E8	Float	3708910
☐	COS	00CD38F0	Float	0.173999995
☐	SIN	00CD38F8	Float	0.9850000143
☐	目地座標X	00CD3900	Float	7081490
☐	目地座標Z	00CD3904	Float	0
☐	目地座標Y	00CD3908	Float	3708910
☐	目地COS	00CD3910	Float	0.173999995
☐	目地SIN	00CD3918	Float	0.9850000143
☐	==OFFSET 1C0C4	00400000	4 Bytes	9460301
☐	人物動作	00CD3B70	4 Bytes	FFFFFFFF
☐	MAX耐久度	00CD3C0C	2 Bytes	720
☐	最大船員數	00CD3C0E	2 Bytes	33
☐	必要船員數	00CD3C10	2 Bytes	25
☐	船倉總大小	00CD3C12	2 Bytes	840
☐	==OFFSET 1C0C4	00400000	4 Bytes	9460301
☐	陸地跟隨ID	00CD3C70	4 Bytes	0
☐	船帆狀態 0-停船 1 2 3 4-全帆	00CD3C74	4 Bytes	0
☐	海上跟隨ID	00CD3CE0	4 Bytes	0

移動CALL用	00CD3D34	4 Bytes	05870DF0	
COS	P->05870EE4	Float	5.510185821E-40	
SIN	P->05870EEC	Float	9.183689746E-41	
移動COS	P->05870EF4	Float	0	
移動SIN	P->05870EFC	Float	0	
移動	P->05870F04	4 Bytes	0	
活動對象Base	00CD3D3C	4 Bytes	05D81960	
目前場景的活動對象數	00CD3D44	4 Bytes	201	
固定對象Base	00CD3D5C	4 Bytes	05D819B0	
目前場景的固定對象數	00CD3D64	4 Bytes	3	
==OFFSET 1C0C4	00400000	4 Bytes	9460301	
城市海域PTR	00CD3D7C	4 Bytes	059DB960	
城市海域名	P->00D4A434	String[30]		
地下城名	P->00D4A434	String[30]		
城市海域PTR(上一層)	00CD3D80	4 Bytes	05A31900	
城市海域名(上一層)	P->05D015E0	String[30]	倫敦碼頭	
小地圖城市編號	00CD652A	Byte	0	
地圖編號	00CD3E1C	4 Bytes	041D0000	
城市、海域編號	00CD3E1E	Byte	1D	
場景	00CD3E1F	Byte	04	
艦隊PTR	00CD3E24	4 Bytes	00000000	
隊友1 ID	P->0000000C	4 Bytes	??	
隊友1 NAME	P->????????	String[10]	??	
隊友2 ID	P->????????	4 Bytes	??	
隊友2 NAME	P->????????	String[10]	??	
隊友3 ID	P->????????	4 Bytes	??	
隊友3 NAME	P->????????	String[10]	??	
==OFFSET 1C150	00400000	4 Bytes	9460301	
技能名稱Base	00CD4390	4 Bytes	04D73420	
交易品類型Base2	00CD43AC	4 Bytes	050DC130	
交易品類型Base1	00CD43C8	4 Bytes	050DC220	
場景名稱Base	00CD4470	4 Bytes	051C07E0	
道具、裝備、交易品名稱Base	00CD480C	4 Bytes	0521F890	
(瘛瑟　)?　　鏊箸	00C59E3C	4 Bytes	05000023	
(瘛瑟　)?菜　鏊箸	00C59E58	4 Bytes	000001F9	
==OFFSET 1C150	00400000	4 Bytes	9460301	
技能名稱Base	00CD4390	4 Bytes	04D73420	
交易品類型Base2	00CD43AC	4 Bytes	050DC130	
交易品類型Base1	00CD43C8	4 Bytes	050DC220	
場景名稱Base	00CD4470	4 Bytes	051C07E0	
道具、裝備、交易品名稱Base	00CD480C	4 Bytes	0521F890	
(瘛瑟　)?　　鏊箸	00C59E3C	4 Bytes	05000023	
(瘛瑟　)?菜　鏊箸	00C59E58	4 Bytes	000001F9	
==OFFSET 1C150	00400000	4 Bytes	9460301	
戰鬥標誌	00CD48E4	4 Bytes	00000000	
友方提督ID	00CD4950	4 Bytes	00000000	
敵方提督ID	00CD4954	4 Bytes	00000000	
==OFFSET 1C150	00400000	4 Bytes	9460301	
友方ID1	00CD4964	4 Bytes	0	
血量	00CD4968	4 Bytes	0	
MAX血量	00CD496C	4 Bytes	0	
攻擊力	00CD497C	4 Bytes	0	
防禦力	00CD4980	4 Bytes	0	
戰等	00CD498C	4 Bytes	0	
人物狀態	00CD4990	4 Bytes	0	
狀態小圖案	00CD4994	4 Bytes	0	
使用技巧狀態	00CD4998	4 Bytes	00000000	
人物動作	00CD49A8	4 Bytes	0	
行動力MAX	00CD49B0	4 Bytes	300	
行動力	00CD49B4	4 Bytes	0	
友方ID2	00CD49C8	4 Bytes	0	
友方ID3	00CD4A2C	4 Bytes	0	
友方ID4	00CD4A90	4 Bytes	0	
友方ID5	00CD4AF4	4 Bytes	0	
==OFFSET 1C150	00400000	4 Bytes	9460301	
敵方ID1	00CD4D4C	4 Bytes	0	
敵方血量	00CD4D50	4 Bytes	0	
敵方MAX血量	00CD4D54	4 Bytes	0	
敵方攻擊力	00CD4D64	4 Bytes	0	
敵方防禦力	00CD4D68	4 Bytes	0	
敵方人物狀態	00CD4D78	4 Bytes	0	
敵方狀態小圖案	00CD4D7C	4 Bytes	0	

☐	敵方使用技巧狀態	00CD4D80	4 Bytes	00000000
☐	敵方ID2	00CD4DB0	4 Bytes	0
☐	敵方ID3	00CD4E14	4 Bytes	0
☐	敵方ID4	00CD4E78	4 Bytes	0
☐	敵方ID5	00CD4EDC	4 Bytes	0
☐	==OFFSET 1C150	00400000	4 Bytes	9460301
☐	陸戰:選定目標	00CD513C	4 Bytes	0
☐	F5	00CD5144	4 Bytes	0
☐	持有數量	00CB8FF8	4 Bytes	3203850443
☐	必要計量	00CB8FFC	4 Bytes	3204030509
☐	使用對象	00CB9000	4 Bytes	1057896922
☐	是否可用	00CB9004	4 Bytes	1057725035
☐	F6	00CD5160	4 Bytes	0
☐	F7	00CD517C	4 Bytes	0
☐	F8	00CD5198	4 Bytes	0
☐	怒氣值	00CD5214	4 Bytes	0
☐	MAX怒氣值	00CD5218	4 Bytes	1000
☐	No description	00CD521C	4 Bytes	00000000
☐	No description	00CD5220	4 Bytes	00000000
☐	陸戰:攻擊目標	00CD5224	4 Bytes	0
☐	==OFFSET 1C150	00400000	4 Bytes	9460301
☐	F1	00CD5228	4 Bytes	0
☐	技巧必要計量	00CD522C	4 Bytes	0
☐	技巧可否使用	00CD5230	4 Bytes	0
☐	F2	00CD5234	4 Bytes	0
☐	F3	00CD5240	4 Bytes	0
☐	==OFFSET 1C150	00400000	4 Bytes	9460301
☐	跳過甲板戰&競技場演出	00CD53B8	4 Bytes	0
☐	剩於演出時間	00CD53D0	Float	0
☐	剩於戰鬥時間	00CD53D4	Float	0
☐	競技場得分	00CD540C	4 Bytes	0
☐	已過戰鬥時間	00CD5418	Float	0
☐	隊友1 PASS	00CD5424	4 Bytes	0
☐	隊友2 PASS	00CD542C	4 Bytes	0
☐	隊友3 PASS	00CD5434	4 Bytes	0
☐	隊友4 PASS	00CD543C	4 Bytes	0
☐	隊友5 PASS	00CD5444	4 Bytes	0
☐	==OFFSET 1C190	00400000	4 Bytes	9460301
☐	技能欄PTR	00CD6308	4 Bytes	00000000
☐	技能欄技能數	P->0000000C	4 Bytes	??
☐	自訂欄PTR	00CD6324	4 Bytes	00000000
☐	自訂欄F1 ID	P->????????	4 Bytes	??
☐	自訂欄F2 ID	P->????????	4 Bytes	??
☐	==OFFSET 1C194	00400000	4 Bytes	9460301
☐	風向COS	00CD65CC	Float	0.5879999995
☐	風向SIN	00CD65D4	Float	-0.8090000153
☐	潮流COS	00CD65DC	Float	0.6949999928
☐	潮流SIN	00CD65E4	Float	0.7189999819
☐	風速	00CD65EC	Byte	14
☐	潮流	00CD65ED	Byte	2
☐	波浪	00CD65EE	Byte	3
☐	天氣	00CD65F1	Byte	80
☐	航行天數	00CD65F4	4 Bytes	21
☐	==OFFSET ??	00400000	4 Bytes	9460301
☐	地下城Code Addr	00CD6814	4 Bytes	05DCF470
☐	地下城Code	P->05DCF498	4 Bytes	00000000
☐	跳出的訊息框(圖)	00CD80D4	4 Bytes	0
☐	跳出的訊息框	00CDD42C	4 Bytes	0
☐	==OFFSET 0x1C5F8	00400000	4 Bytes	9460301
☐	LOG頭PTR	00CD815C	4 Bytes	059DB25C
☐	LOG頭字數	P->059DB270	4 Bytes	17
☐	LOG蝺砌?鎢　TR	P->059DB25C	4 Bytes	059DB280
☐	蝺砌?鎢　???	P->059DB294	4 Bytes	23
☐	LOG蝺砌?鎢　TR	P->059DB280	4 Bytes	059DB2A4
☐	蝺砌?鎢　???	P->059DB2B8	4 Bytes	35
☐	LOG尾PTR	00CD8160	4 Bytes	059DB570
☐	LOG尾字數	P->059DB584	4 Bytes	13
☐	蝮盤OG鎢	00CD8164	4 Bytes	12
☐	??LOG鎢	00CD819C	4 Bytes	8
☐	LOG內容PTR	00CD82D8	4 Bytes	035A6A48
☐	LOG內容	P->035A6A48	String[30]	現於塞維爾，印度文化似乎正成流行。副官
☐	LOG內容?	00CD82DC	4 Bytes	12

OllyICE是由對岸人士將Ollydbg改進的一款逆向工程軟體針對軟體進行反編譯，用來分析網路遊戲主程式和追蹤指令：

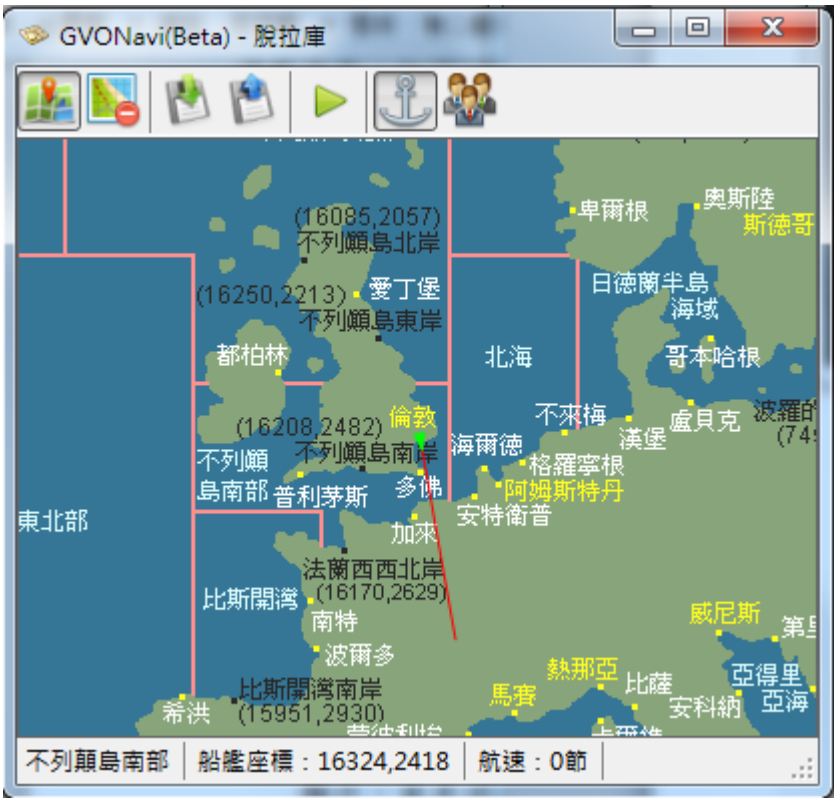


Visual C# .NET 有Windows Form編寫介面，對於專案不大的程式而言很便利。借由Windows API來存取記憶體，取得遊戲中的資料。

四、主要成果

主介面:破解nProtesct GameGuard(保護遊戲主程式，防止外部程式讀取、修改遊戲記憶體)，使多個遊戲角色操作簡便化，並提供各角色遊戲中的資料，角色介面中可額外設定自動功能來使遊戲過程簡化

導航系統：使用GDI(圖形裝置介面)編寫。遊戲玩家可自由設定海上航行地點，來達到自動航行效果，並且根據遊戲中所截取的資料顯示於介面上



交易介面：航海貿易中最主要的一環，可記錄商品的購買、販售價格，並記錄數量

陸戰介面：自動進入地下城與NPC戰鬥，可將NPC所掉落的商品販售，並將持有金錢儲存；收集NPC和玩家角色資料於單一介面上顯示，並可手動操作角色進行攻擊

五、評估與展望

逆向工程只是個程式檢測的過程，但有版權的遊戲軟體往往都有使用防修改技術，而製作遊戲外掛過程中可能已促成軟體重構，違反版權。

六、結論

因個人的好奇心驅使和懶惰心態，不想花太多時間在遊戲中做一些重覆的動作，所以才有製作網路遊戲外掛的念頭，但玩遊戲畢竟不能當作正業，而是當作打發時間用途。對學生而言，從遊戲中學習程式分析、編寫和資料結構是個不錯的體驗。

七、參考文獻

- 廣海社區 http://www.ghoffice.com/bbs/
- 看雪學院 http://pediy.com/
- MSDN http://msdn.microsoft.com/