Runtime Scriptcalling; The gateway to gen IV Arbitrary Code Execution

Before reading this article; some very basic information.
Pal Park mode is enabled when entering map xFB or 251, and gives us two methods to call scripts through runtime.

The first uses the Pal Park menu, which has the RETIRE function. Unless the Great Marsh flag 0x967 is set, this runs 4th script in runtime.
The second uses the fact that encountertables are ignored now, and you can capture 6 migrated Pokémon. When all 6 are caught, it runs 3rd script in runtime.

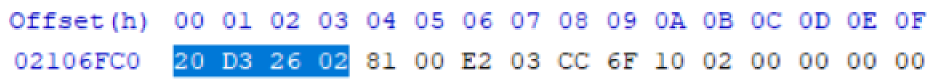
By finally knowing where scripts through runtime are stored in RAM, and as extension knowing where RETIRE or Alt-RETIRE run scripts from when there are less than 4 or 3 scripts in runtime respectively, we now have a fairly viable Arbitrary Script Executing method in the works.

The moment a script is called through runtime, all scripts through runtime of a map are copied to ram. The location is based on a couple of variables, which are the following:

[base]
The base value is used to determine the Address Space Layout Randomisation, which 'shifts' portions of ram by a randomized value. The base address is located at:

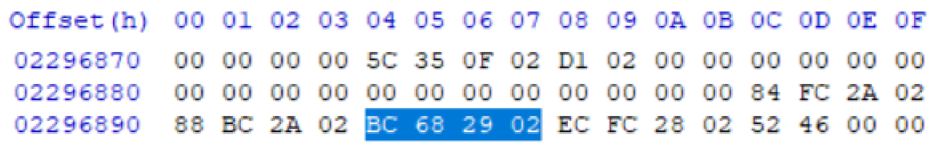
EN	0x02106FC0
DE	0x02107100
FR	0x02107140
IT	0x021070A0
JP	0x02108818
KS	0x021045C0
ES	0x02107160

Example value: 0x0226D320

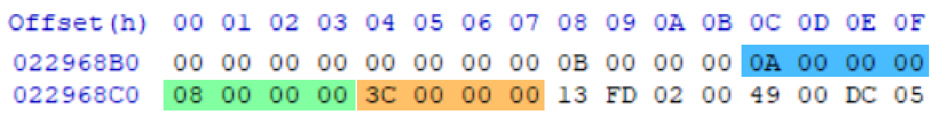

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
02106FC0  20 D3 26 02 81 00 E2 03 CC 6F 10 02 00 00 00 00
```

Runtime_ptr = [base] + 0x29574
Here we find a 4-byte value which when read as word, is the address for the first script in runtime.

Example: 0x0226D320 + 0x29574 = 0x0229 6894
4-byte value: 0x022968BC

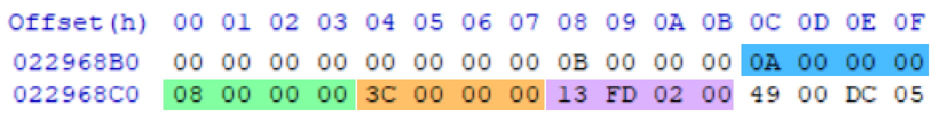

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
02296870  00 00 00 00 5C 35 0F 02 D1 02 00 00 00 00 00 00
02296880  00 00 00 00 00 00 00 00 00 00 00 00 84 FC 2A 02
02296890  88 BC 2A 02 BC 68 29 02 EC FC 28 02 52 46 00 00
```

Script_ptr
And once we go to 0x022968BC we land at the address of the first script in runtime
Every script in runtime is a 4-byte value, which is used as a jump. I am using map 376, a map with 3 scripts. The blue section is the jump when the first script in runtime is ran, the green if the second In runtime is ran, orange if the third is ran.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
022968B0  00 00 00 00 00 00 00 00 0B 00 00 00 0A 00 00 00
022968C0  08 00 00 00 3C 00 00 00 13 FD 02 00 49 00 DC 05
```

Following this logic, even though there are only 3 scripts, when we press RETIRE, the purple section, 0x0002FD13, is used as a jump. FD13 sections off runtime and the scripts themselves, 0002 is actually a part of a script. The jump starts at the first byte after the script_ptr. So we add 4 bytes.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
022968B0  00 00 00 00 00 00 00 00 0B 00 00 00 0A 00 00 00
022968C0  08 00 00 00 3C 00 00 00 13 FD 02 00 49 00 DC 05
```

If we put this as a calculation, the script_ptr is located at [Runtime_ptr] + 4*(Scriptamount-1)
Example: 0x022968BC + 4*3 = 0x022968C8

The jump will occur by adding (script_ptr +C) to Runtime_ptr

Example: 0x022968BC + 0x0002FD13 +6 +4 = 0x022C65D9

From this point the game reads values as script instructions

There is a minor adjustment that has to be performed when doing this process in a battletower void. The runtime_ptr is located at [base] + 0x31678 instead, due to a ramshift.

Researchers: Flederkiari, Martmist, MAP, RETIRE
Opcodes/Instructions and Paramaters

Op name	Opcode	Parameters										
Nop	0000	00	00									
Nop1	0001	01	00									
End	0002	02	00									
Return2	0003											
Nop4	0004	04	00									
	0005											

	0006												
	0007												
	0008												
	0009												
	000A												
	000B												
	000C												
	000D												
	000E												
	000F												
	0010												
If	0011		11	00	var	var	val	val					
If2	0012												
	0013												
CallStandard	0014		14	00	xx	yy							
KillScript	0015												
Jump	0016		16	00	js	js	js	js					
	0017												
	0018												
	0019												
Call	001A												
Return	001B												
CompareLastResultJump	001C		1C	00	val	js	js	js	js				
	001D												
ClearFlag	001E		1E	00	fid	fid							
SetFlag	001F		1F	00	fid	fid							
CheckFlag	0020												
	0021												
	0022												
SetValue	0023		23	00	??	??	??	??					

	0024												
	0025												
CompareVarstoByte	0026												
	0027												
SetVar	0028		28	00	var	var	val	val					
CopyVar	0029												
	002A												
	002B												
Message	002C		2C	00	mes								
Message2	002D		2D	00	mes								
	002E												
Message3	002F		2F	00	mes								
	0030												
WaitButton	0031		31	00									
	0032												
	0033												
CloseMessageOnKeyPress	0034		34	00									
FreezeMessageBox	0035												
CallMessageBox	0036												
ColorMessageBox	0037												
TypeMessageBox	0038												
NoMapMessageBox	0039												
CallMessageBoxText	003A												
	003B												
Menu	003C		3C	00									
	003D												
YesNoBox	003E		3E	00	0C	80							
WaitFor	003F												
Multi	0040												

Multi2	0041												
TextScriptMulti	0042												
CloseMulti	0043												
Multi3	0044												
	0045												
TextMessageScriptMulti	0046												
	0047												
MultiRow	0048												
PlayFanfare	0049		49	00	sid	sid							
PlayFanfare2	004A												
WaitFanfare	004B												
PlayCry	004C		4C	00	sp	sp							
WaitCry	004D		4D	00									
PlaySound	004E												
FadeDefaultMusic	004F												
PlayMusic	0050												
StopMusic	0051		51	00									
RestartMusic	0052		52	00									
	0053												
SwitchMusic	0054												
	0055												
	0056												
	0057												
	0058												
	0059												
SwitchMusic2	005A												
	005B												
	005C												
	005D												
ApplyMovement	005E		5E	00	npc	npc	mov	mov					

WaitMovement	005F												
LockAll	0060		6 0	0 0									
ReleaseAll	0061		6 1	0 0									
Lock	0062		6 2	0 0	np c	npc							
Release	0063												
AddPeople	0064		6 4	0 0	np c	npc							
RemovePeople	0065		6 5	0 0	np c	npc							
LockCam	0066		6 6	0 0									
	0067												
FacePlayer	0068		6 8	0 0									
CheckSpritePosition	0069												
	006A												
CheckPersonPosition	006B												
ContinueFollow	006C												
FollowHero	006D												
StopFollowHero	006E												
GiveMoney	006F		6 F	0 0	am	am	am						
TakeMoney	0070		7 0	0 0	am	am	am						
CheckMoney	0071												
ShowMoney	0072												
HideMoney	0073												
UpdateMoney	0074												
ShowCoins	0075												
HideCoins	0076												
UpdateCoins	0077												
CheckCoins	0078												
GiveCoins	0079												
TakeCoins	007A												

TakeItem	007B												
CheckStoreItem	007C		7C	00	04	80	05	80	0C	80			
CheckItem	007D												
	007E												
	007F												
	0080												
	0081												
	0082												
	0083												
	0084												
CheckUndergroundPcStatus	0085												
	0086												
	0087												
	0088												
	0089												
	008A												
	008B												
	008C												
	008D												
	008E												
	008F												
	0090												
	0091												
	0092												
CheckPokemonParty	0093												
StorePokemonParty	0094												
SetPokemonPartyStored	0095												
GivePokemon	0096		96	00	sp	sp	lv	00	00	00	0C	80	
GiveEgg	0097		97	00	sp	sp	00						
	0098												
CheckMove	0099												

CheckPlaceStored	009A												
	009B												
	009C												
	009D												
	009E												
	009F												
	00A0												
CallEnd	00A1												
	00A2												
WFC	00A3												
	00A4												
Interview	00A5												
DressPokemon	00A6												
DisplayDressedPokemon	00A7												
DisplayContestPokemon	00A8												
CapsuleEditor	00A9												
SinnohMaps	00AA		AA	00									
BoxPokemon	00AB												
DrawUnion	00AC												
TrainerCaseUnion	00AD												
TradeUnion	00AE												
RecordMixingUnion	00AF												
EndGame	00B0		B0	00									
HallFameData	00B1												
	00B2												
WFC1	00B3												
ChooseStarter	00B4		B4	00									
	00B5												
	00B6												
	00B7												
	00B8												

	00B9												
ChoosePlayerName	00BA												
ChoosePokemonName	00BB												
FadeScreen	00BC												
ResetScreen	00BD												
Warp	00BE		BE	00	mid	mid	00	00	xx	xx	yy	yy	00
RockClimbAnimation	00BF		BF	00	pi	pi							
SurfAnimation	00C0		C0	00	pi	pi							
WaterfallAnimation	00C1		C1	00	pi	pi							
FlyAnimation	00C2		C2	00	mid	mid	xx	xx	yy	yy	pi	pi	
	00C3												
	00C4												
	00C5												
Tuxedo	00C6												
CheckBike	00C7												
RideBike	00C8		C8	00	rd								
	00C9												
	00CA												
BerryHiroAnimation	00CB												
StopBerryHiroAnimation	00CC												
SetVariableHero	00CD												
SetVariableRival	00CE												
SetVariableAlter	00CF												
SetVariablePokemon	00D0												
SetVariableItem	00D1												
	00D2												
SetVariableAttackItem	00D3												
SetVariableAttack	00D4												
SetVariableNumber	00D5												

SetVariableNickname	00D6												
SetVariableObject	00D7												
SetVariableTrainer	00D8												
	00D9												
SetVarPokemonStored	00DA												
SetVarHeroStored	00DB												
SetVarRivalStored	00DC												
SetVarAlterStored	00DD												
StoreStarter	00DE												
	00DF												
	00E0												
	00E1												
	00E2												
	00E3												
	00E4												
TrainerBattle	00E5		E5	00	tid	tid	tid 2	tid 2					
EndTrainerBattle	00E6												
	00E7												
	00E8												
	00E9												
ActLeagueBattlers	00EA		EA	00									
LostGoPokeCenter	00EB												
CheckLost	00EC												
	00ED												
	00EE												
	00EF												
	00F0												
	00F1												
ChooseFriend	00F2												
WirelessBattleWait	00F3												
	00F4												
	00F5												
	00F6												
PokemonContest	00F7												

	00F8												
	00F9												
	00FA												
	00FB												
	00FC												
	00FD												
	00FE												
	00FF												
	0100												
Graphic Reload	0101		0 1	0 1									
	0102												
	0103												
	0104												
	0105												
	0106												
	0107												
	0108												
	0109												
	010A												
	010B												
	010C												
	010D												
	010E												
	010F												
	0110												
FlashContest	0111		1 1	0 1									
EndFlash	0112												
	0113												
	0114												
	0115												
ShowLinkCountRecord	0116												
	0117												
	0118												
	0119												

	011A												
WarpMapElevator	011B												
CheckFloor	011C												
	011D												
	011E												
	011F												
SetPositionAfterShip	0120												
	0121												
	0122												
	0123												
WildBattle	0124		24	01	sp	sp	lv						
StarterBattle	0125		25	01	sp	sp	lv						
ExplanationBattle	0126		26	01									
HoneyTreeBattle	0127												
crash	0128												
Randombattle	0129		29	01									
	012A												
WriteAutograph	012B		2B	01									
	012C												
	012D												
CheckDress	012E												
	012F												
	0130												
GivePoketch	0131		31	01									
	0132												
ActivatePoketchApp	0133												
StorePoketchApp	0134												
	0135												
	0136												
	0137												

	0138												
	0139												
	013A												
	013B												
	013C												
	013D												
	013E												
	013F												
	0140												
	0141												
	0142												
ExpectDecisionOther	0143												
	0144												
	0145												
	0146												
Pokemart	0147		47	01	00	mad	mad						
Pokemart1	0148		48	01	00	mad	mad						
Pokemart2	0149		49	01	00	00							
Pokemart3	014A		4A	01	00	mad	mad						
DefeatGoPokecenter	014B		4B	01									
	014C												
CheckGender	014D												
HealPokemon	014E		4E	01									
	014F												
	0150												
	0151												
	0152												
UnionRoom	0153												
	0154												
	0155												

	0156												
	0157												
ActivatePokedex	0158												
	0159												
GiveRunningShoes	015A												
CheckBadge	015B												
EnableBadge	015C		5C	01									
DisableBadge	015D												
	015E												
	015F												
	0160												
	0161												
	0162												
	0163												
	0164												
	0165												
	0166												
	0167												
PrepareDoorAnimation	0168												
WaitAction	0169												
WaitClose	016A												
OpenDoor	016B												
CloseDoor	016C												
	016D												
	016E												
	016F												
	0170												
	0171												
	0172												
	0173												
	0174												
	0175												
	0176												
CheckPartyNumber	0177												

OpenBerryPouch	0178												
	0179												
	017A												
	017B												
	017C												
	017D												
	017E												
	017F												
	0180												
	0181												
	0182												
	0183												
	0184												
	0185												
	0186												
SetOverworldPosition	0187												
SetOverworldMovement	0188												
ReleaseOverworld	0189												
SetDoorPassable	018A												
SetDoorLocked	018B												
	018C												
ShowSavingClock	018D												
HideSavingClock	018E												
	018F												
	0190												
ChoosePokemonMenu	0191												
ChoosePokemonMenu2	0192												
StorePokemonMenu2	0193												
	0194												
PokemonInfo	0195												
	0196												
	0197												
StorePokemonNumber	0198												
	0199												
CheckPartyNumber2	019A												

	019B												
	019C												
	019D												
	019E												
	019F												
	01A0												
	01A1												
	01A2												
	01A3												
	01A4												
	01A5												
	01A6												
	01A7												
	01A8												
	01A9												
	01AA												
	01AB												
EggAnimation	01AC												
	01AD												
	01AE												
	01AF												
	01B0												
	01B1												
	01B2												
MailBox	01B3												
	01B4												
RecordList	01B5												
	01B6												
	01B7												
	01B8												
CheckHappiness	01B9												
	01BA												
	01BB												
	01BC												
CheckPosition	01BD												

	01BE												
	01BF												
CheckPokemonParty2	01C0												
CopyPokemonHeight	01C1												
SetVariablePokemonHeight	01C2												
ComparePokemonHeight	01C3												
CheckPokemonHeight	01C4												
	01C5												
MoveInfo	01C6												
StoreMove	01C7												
	01C8												
DeleteMove	01C9												
	01CA												
	01CB												
	01CC												
	01CD												
	01CE												
	01CF												
	01D0												
	01D1												
	01D2												
	01D3												
	01D4												
	01D5												
	01D6												
BerryPoffin	01D7												
	01D8												
BattleRoomResult	01D9												
	01DA												
	01DB												
	01DC												
	01DD												
	01DE												
	01DF												

	01E0												
	01E1												
	01E2												
	01E3												
	01E4												
	01E5												
	01E6												
	01E7												
	01E8												
	01E9												
ShowSinnohSheet	01EA		E A	0 1									
ShowNationalSheet	01EB		E B	0 1									
	01EC												
	01ED												
	01EE												
	01EF												
	01F0												
CheckFossil	01F1												
	01F2												
	01F3												
	01F4												
	01F5												
CheckPokemonLevel	01F6												
	01F7												
	01F8												
	01F9												
	01FA												
	01FB												
Message	01FC												
Message	01FD												
Message	01FE												
Message	01FF												
	0200												
	0201												

Setflag2 GreatMarsh	0202												
	0203												
WarpLastElevator	0204		04	02									
GeoNet	0205												
GreatMarshBinoculars	0206												
	0207												
PokemonPicture	0208		08	02	sp	sp	01	00	30	00			
HidePicture	0209		09	02									
	020A												
	020B												
	020C												
	020D												
	020E												
	020F												
	0210												
	0211												
	0212												
	0213												
	0214												
	0215												
	0216												
	0217												
	0218												
	0219												
	021A												
	021B												
	021C												
	021D												
	021E												
	021F												
	0220												
RememberMove	0221												
	0222												

	0223												
TeachMove	0224												
CheckTeachMove	0225												
	0226												
	0227												
CheckPokemonTrade	0228												
TradeChosenPokemon	0229												
StopTrade	022A												
	022B												
	022C												
	022D												
	022E												
	022F												
	0230												
	0231												
	0232												
	0233												
	0234												
	0235												
	0236												
	0237												
	0238												
DecideRules	0239												
	023A												
HealPokemonAnimation	023B												
	023C												
ShipAnimation	023D												
	023E												
	023F												
	0240												
	0241												
	0242												
PhraseBox1W	0243												
PhraseBox2W	0244												
	0245												

	0246												
	0247												
	0248												
CheckPhraseBoxInput	0249												
	024A												
PreparePCAnimation	024B												
OpenPCAnimation	024C												
ClosePCAnimation	024D												
CheckLottoNumber	024E												
CompareLottoNumber	024F												
	0250												
	0251												
CheckBoxesNumber	0252												
	0253												
	0254												
	0255												
	0256												
SprtSave	0257												
RetSprtSave	0258												
ElevLgAnimation	0259												
	025A												
	025B												
	025C												
	025D												
	025E												
	025F												
	0260												
CheckAccessories	0261												
	0262												
	0263												
	0264												
	0265												
	0266												
PokeCasino	0267												
	0268												

	0269												
	026A												
	026B												
	026C												
UnownMessageBox	026D												
	026E												
	026F												
	0270												
ThankNameInsert	0271												
	0272												
	0273												
	0274												
	0275												
	0276												
	0277												
	0278												
	0279												
LeagueCastleView	027A		7 A	0 2									
	027B												
	027C												
	027D												
	027E												
	027F												
	0280												
	0281												
	0282												
	0283												
	0284												
	0285												
	0286												
	0287												
	0288												
	0289												
	028A												

	028B												
PokemonPartyPicture	028C		8C	02	val	val							
	028D												
	028E												
CheckFirstTimeChampion	028F												
	0290												
	0291												
	0292												
	0293												
ShowBattlePointsBox	0294												
HideBattlePointsBox	0295												
	0296												
	0297												
	0298												
	0299												
	029A												
	029B												
	029C												
ChoiceMulti	029D												
HiddenMachineEffect	029E												
CameraBumpEffect	029F		9F	02	del	del							
DoubleBattle	02A0												
ApplyMovement2	02A1												
	02A2												
	02A3												
	02A4												
ChooseTradePokemon	02A5												
	02A6												
	02A7												
	02A8												
	02A9												
ComparePhraseBoxInput	02AA												

	02AB												
ActivateMysteryGift	02AC												
	02AD												
	02AE												
	02AF												
	02B0												
	02B1												
	02B2												
	02B3												
	02B4												
	02B5												
	02B6												
	02B7												
	02B8												
	02B9												
	02BA												
	02BB												
CheckWildBattle2	02BC												
WildBattle2	02BD		BD	02	sp	sp	lv	1F	00	8E	00		
	02BE												
BikeRide	02BF												
	02C0												
ShowSaveBox	02C1												
HideSaveBox	02C2												
	02C3												
	02C4												
	02C5												
SpinTradeUnion	02C6												
CheckVersionGame	02C7												
	02C8												
	02C9												
FloralClockAnimation	02CA												
	02CB												
	02CC												

	02CD												
	02CE												
	02CF												
	02D0												
	02D1												
	02D2												
	02D3												
	02D4												
	02D5												
	02D6												
	02D7												
	02D8												
	02D9												
	02DA												
	02DB												
	02DC												
	02DD												
	02DE												
	02DF												
	02E0												
	02E1												
	02E2												
	02E3												
	02E4												
	02E5												
	02E6												
	02E7												
	02E8												
	02E9												
	02EA												
	02EB												
	02EC												
	02ED												
	02EE												
	02EF												

	02F0												
	02F1												
	02F2												
	02F3												
	02F4												
	02F5												
	02F6												
	02F7												
	02F8												
	02F9												
	02FA												
	02FB												
	02FC												
	02FD												
	02FE												
	02FF												
	0300												
	0301												
	0302												
	0303												
	0304												
	0305												
	0306												
	0307												
	0308												
	0309												
	030A												
	030B												
	030C												
	030D												
	030E												
	030F												
	0310												
	0311												
	0312												

	0313												
	0314												
	0315												
	0316												
	0317												
	0318												
	0319												
	031A												
	031B												
	031C												
	031D												
	031E												
	031F												
	0320												
	0321												
	0322												
	0323												
	0324												
	0325												
	0326												
	0327												
PortalEffect	0328												
	0329												
	032A												
	032B												
	032C												
	032D												
	032E												
	032F												
	0330												
	0331												
	0332												
	0333												
	0334												
	0335												

	0336												
	0337												
	0338												
	0339												
	033A												
	033B												
	033C												
	033D												
	033E												
	033F												
	0340												
	0341												
	0342												
	0343												
	0344												
	0345												
	0346												
DisplayFloor	0347												
	0348												
	0349												
	034A												
	034B												
	034C												
	034D												
	034E												
	034F												
	0350												
	0351												
	0352												
	0353												
	0354												
	0355												
	0356												
	0357												
	0358												

	0359												
	035A												
	035B												
	035C												
	035D												
	035E												
	035F												
	0360												
	0361												
	0362												
	0363												
	0364												
	0365												
	0366												
	0367												
	0368												
	0369												
	036A												
	036B												
	036C												
	036D												
	036E												
	036F												
	0370												
	0371												
	0372												
	0373												
	0374												
	0375												
	0376												
	0377												
	0378												
	0379												
	037A												
	037B												

	037C												
	037D												
	037E												
	037F												
	0380												
	0381												
	0382												
	0383												
	0384												
	0385												
	0386												
	0387												
	0388												
	0389												
	038A												
	038B												
	038C												
	038D												
	038E												
	038F												
	0390												
	0391												
	0392												
	0393												
	0394												
	0395												
	0396												
	0397												
	0398												
	0399												
	039A												
	039B												
	039C												
	039D												
	039E												

	039F												
	03A0												
	03A1												
	03A2												
	03A3												
	03A4												
	03A5												
	03A6												
	03A7												
	03A8												
	03A9												
	03AA												
	03AB												
	03AC												
	03AD												
	03AE												
	03AF												
	03B0												
	03B1												
	03B2												
	03B3												
	03B4												
	03B5												
	03B6												
	03B7												
	03B8												
	03B9												
	03BA												
	03BB												
	03BC												
	03BD												
	03BE												
	03BF												
	03C0												
	03C1												

	03C2												
	03C3												
	03C4												
	03C5												
	03C6												
	03C7												
	03C8												
	03C9												
	03CA												
	03CB												
	03CC												
	03CD												
	03CE												
	03CF												
	03D0												
	03D1												
	03D2												
	03D3												
	03D4												
	03D5												
	03D6												
	03D7												
	03D8												
	03D9												
	03DA												
	03DB												
	03DC												
	03DD												
	03DE												
	03DF												
	03E0												
	03E1												
	03E2												
	03E3												
	03E4												

	03E5												
	03E6												
	03E7												
	03E8												
	03E9												
	03EA												
	03EB												
	03EC												
	03ED												
	03EE												
	03EF												
	03F0												
	03F1												
	03F2												
	03F3												
	03F4												
	03F5												
	03F6												
	03F7												
	03F8												
	03F9												
	03FA												
	03FB												
	03FC												
	03FD												
	03FE												
	03FF												
	0400												
	0401												
ExitMarsh	0402		02	04									