

آموزش سافت ترینر: آموزش به صورت متنی همراه با عکس

مقدمه

روش هک بازی ها روشی منطقی است که همیشه جواب می دهد. برای این که بتوانید یک بازی را هک کنید باید نکاتی را در مورد بازی ها بدانید.

شرکت های سازنده بازی ها، به طور عمدی رمزهایی را در بازی های خود قرار می دهند. این رمزها پس از مدتی با عنوان کدهای تقلب بازی یا کشف می شوند و یا این که شرکت سازنده بازی آن را پخش می کند.

برای این که شما بتوانید از رمزهای بازی ها استفاده کنید باید آنها را یافته و وارد نمایید. نوع وارد کردن رمزها نیز متفاوت است. مثلا بعضی از بازی ها را باید به حالت مکث (Pause) برده و سپس رمزها را وارد کنید مثل بازی Robocop در جنسیس سگا. در بعضی از بازیها بدون اینکه Pause را بزنید کدها را وارد می کنید مثل Duke Nukem در کامپیوتر. در بعضی از بازیها باید از طریق قسمت Options آنها کدها را فعال کنید مثل بازی Mortal Kombat در پلی استیشن یک و بعضی از بازیها را باید با فشردن یک کلید وادار کنید که یک کادر متنی ظاهر کنند و شما کدها را در آن کادر وارد نمایید مثل بازی Delta Force در کامپیوتر. البته روش های دیگری هم در کامپیوتر وجود دارد. مثلا با دستکاری یکی از فایل های بازی کار وارد کردن کد انجام می گیرد مثل بازی Virtua Cop یا با اضافه کردن یک عبارت به خط فرمان داس مثل بازی Max Payne .

به هر روشی که وارد کردن کدها انجام شود روش کار کردن آن کدها یکی است. کدهای وارد شده یک داده را در بازی به حالت یخ زده در می آورند (Freezing). این عمل اساس روش هک بازی است.

در روش هک بازی ما هیچ نیازی به کدهای تقلب نداریم. در واقع ما خودمان برای هر چیزی که بخواهیم کد تقلب می سازیم.

تمام چیزهایی که برای ادامه یادگیری باید بدانید * بسیار مهم *****

در این قسمت تعریف هایی را در مورد عبارات به کار رفته در آموزش، می آوریم. برای ادامه یادگیری حتما باید این مطلب را بخوانید.

متغیر یا پروسه (Process): بازی هایی که شما آنها را می گشایید تعداد بی نهایت زیادی متغیر یا پروسه را فعال می کنند. برای مثال شما در یک بازی متغیرهای زیر را حتما دارید: تعداد جانها- تعداد گلوله ها-

تعداد بیکسل های صفحه نمایش - تعداد ادامه (Continue) - متغیری که مشخص می کند انگشت کار کتر شما دقیقا در کدام نقطه است! و ...

می بینید که هر چیزی در بازی کاملا کنترل می شود. اما همانطور که حتما متوجه شده اید ما به همه این پروسه ها نیاز نداریم. ما فقط به تعداد جانها و مقدار جان، تعداد گلوله ها، تعداد شلیک های مجاز تا خالی شدن اسلحه، تعداد ادامه ها، مقدار پول و ... توجه می کنیم. در واقع این پروسه ها هستند که بازی ما را کنترل می کنند و ما در بازی فقط باید به این متغیرها توجه کنیم. مشخص است که بقیه متغیرها توسط خود بازی کنترل می شود.

ارزش یا مقدار (Value): هر متغیر، می تواند مقادیر مختلفی را بگیرد. متغیر در اینجا دقیقا مثل X در یک تابع مثل $y = \sqrt{x^2 + x}$ است. وقتی می گویم "دقیقا" منظورم واقعا همان است. هر متغیر در بازی یک دامنه تغییر هم دارد. مثلا در این تابع X می تواند مقادیر بزرگتر از صفر و کوچکتر از 1- را بگیرد. برای متغیر بازی ها هم به همین شکل است. برای مثال می توانید در جدول زیر دامنه متغیرهای صحیح (Integer) را ببینید.

نام متغیر	محدوده	توضیح
Integer 1 byte	صفر تا 255	تعداد جان و مقدار جان و تعداد Continue
Integer 2 byte	صفر تا 65535	تعداد جان و مقدار پول و تعداد وسایل
Integer 4 byte	صفر تا 4294967295	مقدار پول و خطوط جان
Integer 8 byte	صفر تا 18446744073709551616	معمولا برای پول (بالاتر از 4 میلیارد)

اگر توضیحات جدول هم برای شما گنگ است، ناراحت نشوید. به زودی آنقدر در این کار مهارت پیدا می کنید که من هم مشکلاتم را از شما می پرسم. فقط کافی است که توضیحات مرا با دقت تمام بخوانید. اگر جایی را هم نفهمیدید سؤالات خود را پرسید.

انواع داده ها (Data Types): داده هایی که به درد ما می خورند چند دسته هستند.

- پر کاربردترین نوع داده ها داده های صحیح یا Integer هستند که در بالا دامنه آنها را مشاهده کردید. همانطور که می بینید اکثر چیزهایی که ما می خواهیم در توضیحات آمده است. بنابراین بیشتر کار ما روی این نوع داده خواهد بود.

- نوع دیگر داده ها، داده های شناور یا Float هستند. این داده ها می توانند علاوه بر اعداد صحیح، اعداد اعشاری را نیز پشتیبانی کنند. برای مثال این داده ها می توانند عدد $34/85$ را در خود ذخیره کنند.
- نوع دیگری که کمتر به کار می آید و شاید اصلا به شما کمک نکند نوع داده های متنی است. در بازی ها این داده ها معمولا ثابت هستند.

حال باید ببینیم که چگونه باید داده ها را پیدا کنیم.

روش یافتن داده دلخواه از میان میلیونها داده

فکر می کنید برای پیدا کردن یک داده در میان میلیونها داده چه کاری باید انجام دهیم؟ اصلا ما برای چه می خواهیم یک متغیر را پیدا کنیم؟

جواب سؤال دوم را اول می دهیم! ما می خواهیم یک داده یا متغیر را پیدا کنیم و مقدار آن را به دلخواه خود تغییر دهیم. مثلا می خواهیم داده مربوط به تعداد جانها را پیدا کرده و مقدار آن را افزایش دهیم. اگر به یاد داشته باشید ما گفتیم که روش هک بازی ها یک روش منطقی است. اما این روش منطقی چگونه است؟

برای پاسخ به این سؤال می خواهیم مثالی بزنم. شما در یک شهر، فردی را جستجو می کنید. ابتدا چه چیزی نیاز دارید؟ بلی، آدرس. اما شما آدرس دقیق او را نمی دانید. فقط میدانید در این شهر زندگی می کند. خود این مسأله کمک بزرگی به شما می کند. شما شغل فرد مورد نظر را هم می دانید. بنابراین شما پس از این که فهمیدید او در این شهر است به دنبال اداره ای که او کار می کند می گردید. پس از یافتن اداره شما باید نام او را بگویید. وقتی نام او را گفتید او را می یابید.

ببخشید که اینقدر یک مسأله ساده را توضیح دادم. قصدم توهین نبود بلکه می خواستم به شما بگویم که چقدر کار ما آسان است. در واقع این مثال ساده اساس کار روش هک بازی هاست.

شما در داخل بازی هستید. در این بازی شما 5 جان دارید. ما باید متغیرهایی که ارزش آنها 5 است را از دیگر متغیرها جدا کنیم. پس از جدا کردن می بینیم که هزاران متغیر با ارزش 5 وجود دارد که فقط یکی یا دو تای آنها تعداد جانهایتان را کنترل می کنند.

برای ادامه چه باید بکنیم؟ مسلما همه می دانید. ما باید تعداد جانهایمان را در بازی تغییر دهیم. می پرسید چرا؟ چون با این کار ارزش متغیری که تعداد جانها را کنترل می کند نیز تغییر می یابد و ما می توانیم به مقصد نزدیکتر شویم. بنابراین ما به بازی رفته و یک جان خود را به طور عمدی از دست می دهیم. با این

کار ما اکنون 4 جان داریم. حال در میان متغیرهایی که پیدا کرده بودیم به دنبال متغیرهایی می گردیم که ارزش آنها 4 است. نیمی از متغیرها حذف می شوند. با ادامه این کار و با افزودن یا کاستن تعداد جانها جستجو را ادامه می دهیم و در انتها به یک یا دو متغیر می رسیم. اگر ارزش این متغیرها را تغییر دهیم، تعداد جانها نیز در بازی تغییر می کند. به عبارت دیگر در ابتدا، بازی متغیر را کنترل می کرد و اکنون، متغیر بازی را کنترل می کند.

آشنایی با محیط نرم افزارهای هک بازی ها

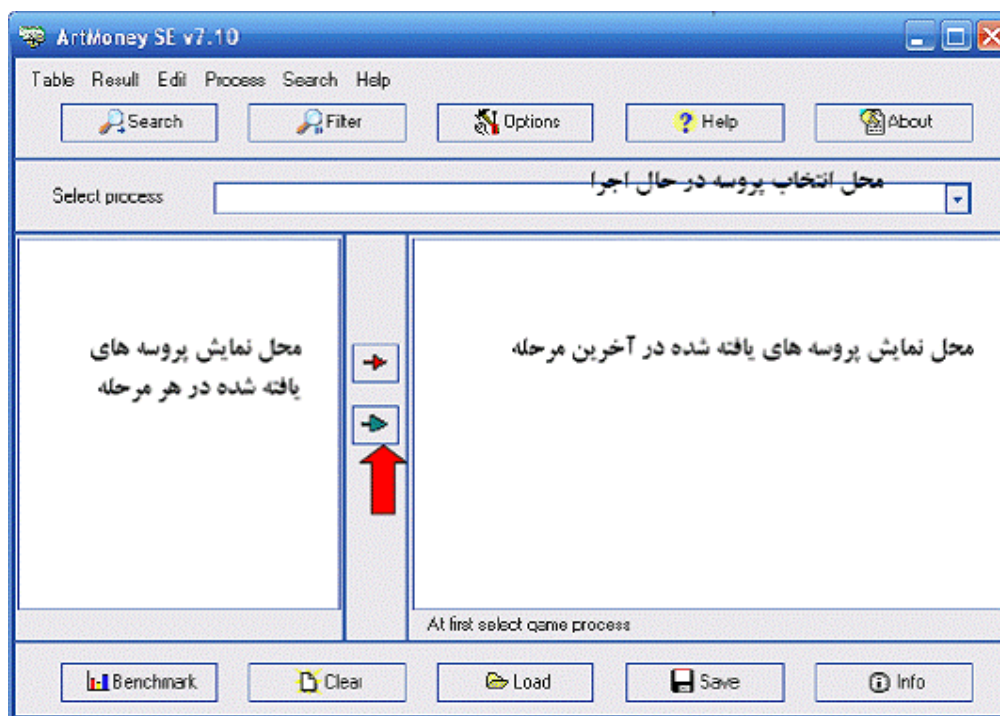
برنامه های زیادی وجود ندارند که کار هک بازی ها را انجام می دهند. البته همانطور که گفتم نباید نرم افزارهایی مثل Cheat Machine را هم نرم افزار هک بازی ها بدانیم. شاید ساده ترین نرم افزار در این زمینه، نرم افزار OMatic باشد. در این نرم افزار شما فقط می توانید داده های صحیح، که مقدار آنها را می دانید را بیابید. ممکن است که بگویید باز هم خوب است اما مشکل اینجاست که هیچ امکاناتی هم برای ذخیره یافته ها در این نرم افزار وجود ندارد. در واقع شما باید هر بار که می خواهید بازی کنید باید آن را هک کنید. علاوه بر این اکثر بازی های جدید از خطوط جان (Bar Of Life) استفاده می کنند که توسط این نرم افزار قابل هک نیستند. بقیه نرم افزارها هم باید اول فکری برای سر و وضع خود بکنند چون در اکثر آنها شما به جای نوشته های روی کلید ها، فقط خطوط مبهم می بینید. اما...

به آخرین نرم افزار می رسیم. ArtMoney قدرتمندترین نرم افزار در این زمینه است. محیط آن بسیار ساده و نتایج جستجوی آن شگفت انگیز است. با وجود پیچیدگی زیادی که در این نرم افزار گنجانده شده - که علت آن پیچیدگی بعضی از بازی هاست - اما یک کاربر ساده هم به راحتی با آن می تواند تعداد جانها را هک کند! البته اگر روش منطقی بالا را بدانند یا این که حداقل انگلیسی اش خوب باشد

محیط نرم افزار ArtMoney ساده و بسیار مرتب و منظم است. تنها اشکال نرم افزار این است که نسخه Pro ی آن را باید بخرید. نمی توانید باور کنید که کاری که ما با روش های عادی در مدت 20 دقیقه انجام می دهیم، این نسخه در عرض 2 دقیقه انجام می دهد. اگر پولش را داشتید و توانستید آن را بخرید، شماره سریال را به ما هم بگویید. من نسخه Pro را دانلود کرده ام، اما هرچه اینترنت را زیر و رو کردم شماره سریال آن را پیدا نکردم.

ما کارمان را با نسخه SE که مجانی است آغاز می کنیم. اگر روزی شماره را یافتیم به شما هم خبرش را می دهیم.

محیط کار ArtMoney را در شکل زیر می بینید.



تا یادم نرفته بگویم که من با نسخه 7.10 نرم افزار کار می کنم. الان تا جایی که من دیده ام نسخه 7.11 هم در سایت وجود دارد.

بخش های برنامه به ترتیب از بالا به این شکل هستند:

- **محل انتقال پروسه فعال:** شما ابتدا برنامه ArtMoney را باز می کنید و پس از آن به داخل بازی می روید. با فشردن یک کلید میان بر که بعداً حتماً خواهیم گفت به برنامه ArtMoney برمی گردید. در این قسمت که در شکل هم می بینید، نام بازی را یافته و انتخاب می کنید. مراحل بعدی را متعاقباً خواهیم دید.
- **محل نمایش پروسه های یافته شده در هر مرحله:** در این قسمت هزار پروسه از پروسه های یافته شده در هر مرحله از فیلترینگ نمایش داده می شود. البته تنظیم پیش فرض برنامه اینگونه است و شما می توانید مقدار آن را اضافه یا کم کنید.
- **کلیدهای انتقال:** وقتی به یک یا دو پروسه در سمت چپ رسیدید، با این کلیدها آنها را به سمت راست منتقل می کنید. نرسید چرا!!!
- **محل نمایش پروسه های یافته شده در آخرین مرحله:** پس از انتقال پروسه ها به این سمت آنها را ویرایش کرده و ذخیره می نمایید.

روند کامل این تغییرات و اینکه چه زمانی از هر کدام استفاده خواهیم کرد را بعداً می بینیم.

کلیدهای میان بر برنامه ArtMoney

اولا این کلید ها را تغییر ندهید. ثانياً زیاد از آنها استفاده نکنید چون ممکن است بازی شما قفل کند (مخصوصاً در کامپیوترهای ضعیف).

بعد از این اولاً و ثانياً می خواهیم دو (یا چند) کلید ویندوز که می توانید از آنها استفاده کنید را بگویم.

• **Alt+Tab**: کلید پیش فرض ویندوز برای تغییر پنجره هاست. عیبش این است که در بعضی از بازی ها کار نمی کند.

• **Ctrl+Alt+ Del**: همه شما این کلید را می شناسید. با این کلید پنجره **Manager Task** ویندوز باز می شود و عیب این میان بر هم همین است. چون باید پس از خروج از بازی، یک پنجره را هم ببندید.

• **Ctrl+Shift+Esc**: دقیقاً همان کاری را انجام می دهد که کلید بالایی می کرد.

اما کلیدهای میان بر **ArtMoney**:

• **Ctrl+F12**: با این کلید به صفحه **ArtMoney** بر می گردید. بسیار خوب کار می کند. عیبش این است که ممکن است در هنگامی که شما برای جستجو به **ArtMoney** رفته اید، در بازی تغییراتی ایجاد شود. مثلاً یک جان خود را از دست بدهید. با این فرض ها، اگر می خواهید از این کلید استفاده کنید حتماً باید بازی را در حالت **Pause** قرار دهید.

• **Ctrl+F11**: با این کلید پروسه فعال کنونی انتخاب می شود که زیاد به درد بخور نیست.

• **Ctrl+F9**: بهترین کلید **ArtMoney** برای بازگشت به برنامه است و هیچ عیبی هم ندارد. لازم هم نیست که بازی را در حالت **Pause** قرار دهید چون این کلید خودش بازی را قفل می کند.

• **Ctrl+F10**: اگر از کلید **Ctrl+F9** برای بازگشت به **ArtMoney** استفاده کرده اید، برای بازگشت به بازی هم باید از کلید **Ctrl+F10** استفاده کنید چون این کلید علاوه بر برگشتن به بازی، آن را از حالت قفل هم خارج می کند.

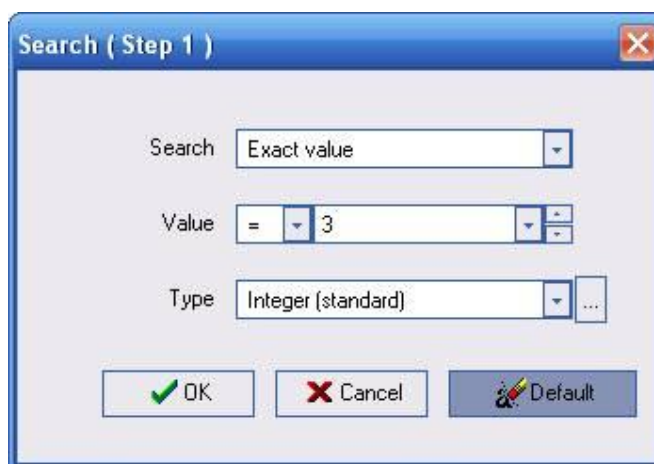
• **Ctrl+F8**: این کلید فقط بازی را قفل می کند.

روش عملی هک بازی _____ قسمت اول _____ ساده

می خواهیم در بازی **Virtua Cop 2** تعدادجانها را افزایش دهیم و یا حتی بی نهایت کنیم.

برنامه ArtMoney 7 را باز کنید. از منوی Search زیر منوی Object گزینه Process را انتخاب کنید.

حال بازی را باز کرده و بازی جدیدی را شروع کنید. کلیدهای ترکیبی Ctrl+F9 را فشار دهید. با این کار به محیط برنامه برمی گردید. حال از محل انتخاب پروسه های در حال اجرا نام بازی را انتخاب کنید و کلید Search را فشار دهید. با فشار دادن این کلید پنجره زیر ظاهر می شود.



گزینه های این پنجره را در انتها توضیح خواهیم داد. بدون مقدمه کلید Default را فشار داده و تعداد جانها را می نویسیم. اگر از نسخه SE استفاده می کنید با تساوی کاری نداشته باشید. کلید OK را فشار دهید. لیستی از پروسه ها را در سمت چپ تصویر برنامه می بینید. به بازی برگردید. برای این کار از کلید Ctrl+F10 استفاده کنید. یک جان خود را از دست بدهید. به برنامه ArtMoney برگشته و روی Filter کلیک کنید. پنجره ای شبیه آنچه در بالا می بینید را خواهید دید که روی آن نوشته شده است: Filter. مقدار را از 3 به 2 کاهش داده و OK را بزنید. می بینید که تعداد پروسه ها کاهش می یابد. باز هم به بازی برگردید و یک جان دیگر از دست بدهید. به برنامه برگردید و به دنبال عدد 1 بگردید (با گزینه Filter). بار دیگر به بازی رفته و جان خود را از دست بدهید. حال بازی از شما می خواهد که Continue کنید. پس از Continue شما باز هم 3 جان دارید. بنابراین به برنامه برگشته و به دنبال عدد 3 بگردید (باز هم با Filter). پس از تکرار این مراحل به 1 یا 2 پروسه خواهید رسید. با فشردن کلید قرمز یا سبز در پنجره پروسه ها را به طرف راست منتقل کرده و نام آنها را تغییر دهید. روی عدد موجود در زیر عبارت Value یک بار کلیک کنید و سپس عدد دلخواه را وارد کنید.

F	Description	Address	Value	Type
X	Lives	0011D4D5	3	Integer

سعی نکنید عدد بسیار بزرگی را وارد کنید. در صورتی که این کار را انجام دهید ممکن است بازی قفل کرده و متوقف شود. بنابراین همان مقدار اصلی موجود در بازی را وارد کنید. مثلا 3 را به عنوان تعداد جانها وارد کنید. نگران نباشید که این مقدار کم است. یک بار در مربع زیر حرف F کلیک کنید تا فعال شود (مانند شکل). با این کار این پروسه به اصطلاح یخ می زند یعنی دیگر تغییر نمی کند (Freezing). بنابراین شما می توانید بدون از دست دادن حتی یک جان بازی را تمام کنید. وقتی این اعمال را انجام دادید به بازی برگردید. ممکن است وقتی که به بازی وارد شدید تصور کنید که هیچ عملی انجام نشده است. برای این که تغییرات در بعضی از بازی ها اعمال شود لازم است که یک بار دیگر جانتان را از دست بدهید. با این کار بازی به پروسه مورد نظر مراجعه می کند و می خواهد یک جان را کم کند ولی چون پروسه یخ زده است بازی نیز می پذیرد که شما همچنان 3 جان داشته باشید. این یک پروژه خیلی ساده بود. برای تمرین اینکه عمل هک را حتما یاد گرفته اید تمرینات زیر را انجام دهید.

- سلاح شما در بازی Virtua Cop 2 پس از 5 بار شلیک خالی می شود و باید از کلید سمت راست ماوس کمک گرفته و آن را پر کنید. گرچه به نظر می رسد که این کار وقت زیادی نمی گیرد اما اگر بازی کنید می فهمید که همین کار باعث برخوردهای بسیاری می شود که موجب از دست دادن جانتان می شوند. البته اگر تعداد جانها را هک کنید مشکلی نخواهید داشت ولی اگر از من می شنوید همه چیز را در بازی یکجا هک نکنید. مثلا اگر تعداد جانها را هک کردید، دیگر گلوله ها را هک نکنید. این کار باعث می شود که شما از بازی خسته نشوید. البته توصیه قویتر من این است که بدون استفاده از روش هک، بازی کنید ولی اگر در جایی گیر کردید و نتوانستید رد شوید، از هک استفاده کنید. هر چه باشد لذت بازی در این است که شما سعی در حفظ جانتان بکنید و گرنه سازندگان بازی ها اصلا محدودیتی برای جانها قائل نمی شدند. خلاصه؛ می خواستم بگویم که کاری کنید که تعداد گلوله ها با شلیک کم نشود.

- تعداد جانها را در بازی The House of the Dead هک کنید. اگر می خواهید می توانید تعداد گلوله های این بازی را هم هک کنید.

- تعداد جانهایتان را در بازی Jaz Jack Rabbit 2 هک کنید.

- تعداد جانهای بازی Hercules را هک کنید.

- اگر می توانید، وقت بازی Mortal Kombat را هک کنید.

- تعداد نارنجک های Delta Force 1 را هک کنید.

• مقدار موجودی خود را در 5 Need For Speed هک کنید.

• یک بازی پلی استیشن را هک کنید

• تعداد Continue های بازی Virtua Cop 2 را هک کنید.

• و بالاخره تعداد گلوله ها را در Resident Evil 3 هک کنید

روش عملی هک بازی _____ قسمت دوم _____ پیشرفته

در این قسمت در مورد بازی Hercules توضیحاتی را می بینیم. در این بازی بیشتر از آن که تعداد جان ها مهم باشد مقدار جان مهم است. مقدار جان یا خط جان را در بازی ها معمولاً با یک خط که در ابتدای بازی پر است ولی بعداً با یک برخورد مقدار آن کم می شود دیده ایم. این گونه از داده ها می توانند بر چند نوع باشند.

• Integer 4 Byte یا Pointer: اکثر بازی هایی که از خطوط جان استفاده می کنند از این نوع خاص متغیر بهره می برند. البته شما به روش های مستقیم نمی توانید این نوع را هک کنید.

• Integer 2 Byte: تعداد کمی از بازی ها از این روش استفاده می کنند. در این روش برای خط جان (The Bar of Life) درصدهایی پیش بینی می شود. برای مثال برای پر بودن خط جان از 100 و برای نصف بودن جان از 50 استفاده می شود.

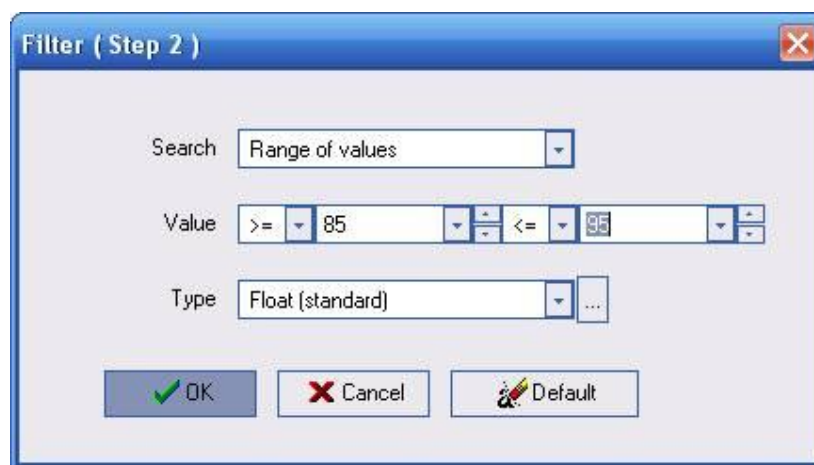
• Float: در لغت این کلمه به معنی شناور است. در این روش هم از نوع 4 بایتی و هم از نوع 8 بایتی استفاده می شود. برای مثال شما در بازی 85 درصد جانتان پر است. اما دقیقاً نمی دانید که 85 درصد درست است یا نه. ممکن است که 85/8 درصد جانتان پر باشد. همانطور که می دانید در Integer فقط اعداد صحیح بررسی می شوند.

حال به بررسی روش های بالا می پردازیم. ابتدا روش دوم و سوم را بررسی می کنیم. روش سوم را بار دیگر در توضیح روش اول خواهیم دید.

یافتن مقدار دلفواه با درصد

برای این که بتوانیم از روش درصدی استفاده کنیم باید از یک روش حدس زدن بهره بگیریم. روشن است که اگر حدس ما غلط باشد هیچ چیزی پیدا نمی کنیم. بازی را باز می کنیم و به برنامه ArtMoney می رویم. نام بازی را انتخاب کرده و کلید Search را میزنیم. با تنظیمات Default به دنبال عدد 100 می

گردیم. به بازی رفته و مقداری از جان خود را از دست می دهیم. برای مثال 10 درصد از جان خود را از دست می دهیم. به ArtMoney برگشته و کلید Filter را فشار می دهیم. در پنجره Filter در مقابل عبارت Search گزینه Range of Values را انتخاب می کنیم زیرا دقیقا مقدار جان خود را نمی دانیم. در قسمت اول عدد 85 و در قسمت دوم عدد 95 را می نویسیم. یکی از گزینه های Integer یا Float را از قسمت Type انتخاب می کنیم. واضح است که گزینه Float بهتر است. پس از اینکه مقدار را انتخاب کردید می توانید جستجو را انجام دهید. با تکرار این مراحل می توانید به نتیجه دلخواه خود برسید. برای این که به نتایج بهتری برسید می توانید از تکنیک افزایش و کاهش توأم استفاده کنید. به این معنی که مثلا یک بار که جان خود را از دست دادید در نوبت بعدی سعی کنید جان خود را افزایش داده و دوباره جستجو کنید. علت آن هم که مشخص است. بعضی از متغیرها از ابتدای بازی فقط کاهش پیدا می کنند. مثلا ممکن است متغیری برای تنظیم و کنترل زمان بازی باشد. طبیعی است که این متغیر فقط کاهش پیدا می کند و زمانی که شما به دنبال افزایش بگردید این متغیر حذف می شود و زودتر به نتیجه می رسید. بعدا در این باره بیشتر توضیح خواهم داد. وقتی مقدار را یافتید آن را تغییر داده و ذخیره کنید.



یافتن مقدار دلخواه وقتی هیچ چیز در مورد داده ندانیم

اگر شما از روش اول نتیجه نگیرید دو علت ممکن است داشته باشد.

- نوع متغیر مورد جستجوی شما Integer 2 Byte یا Float نباشد.
- متغیر کد شده باشد.

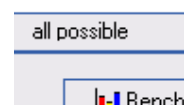
اگر علت اول باشد به روش زیر عمل کنید. در مورد قسمت دوم به صفحه بعدی رفته و در آنجا چگونگی یافتن متغیرهای کد شده را ببینید.

روش یافتن 4 Byte Integer

متغیرهایی که Integer 4 Byte باشند را نمی توان به روش های عادی پیدا کرد. متغیر Integer 4 byte در محدوده صفر تا 4294967295 تغییر می کند. بنابراین حدث زدن آن غیر ممکن است. قبلا در مورد محدوده متغیر ها بحث کرده ایم.

چون ما نمی توانیم از روش معمولی گفته شده سود ببریم، باید راه دیگری را امتحان کنیم. در ArtMoney 7 و حتی در نسخه های قبل از آن نوعی جستجو با عنوان Unknown Value وجود دارد. طریقه انجام کار بدین شکل است. باید بگوییم که بازی Hercules از نوع Integer 4 byte استفاده می کند.

برنامه ArtMoney را باز کرده و پس از آن بازی را اجرا کنید. با فشردن کلیدهای Ctrl+F12 به محیط برنامه برگشته و روی کلید Search کلیک نمایید. از قسمت Search گزینه Unknown Value را انتخاب کنید. در قسمت وسط نمی توانید چیزی بنویسید. در قسمت Type گزینه Pointer را انتخاب نمایید و یا گزینه Custom را انتخاب نموده و با فشردن کلیدی که روی آن 3 نقطه وجود دارد به پنجره Select Type وارد شوید. گزینه Integer 4 byte را فعال و بقیه را غیرفعال کنید. اطمینان حاصل کنید که در مقابل Bytes Order گزینه Normal انتخاب شده باشد. برای پذیرفتن تنظیمات OK را کلیک کرده و در پنجره Search هم روی OK کلیک کنید. پس از جستجو در زیر پنجره برنامه نوشته می شود: All possible یعنی تمام حالت های ممکن.



به بازی بروید و مقداری از جان خود را از دست بدهید. با فشردن کلیدهای Ctrl+F9 به ArtMoney برگردید و روی گزینه Filter کلیک کنید. قسمت Search و Type را بدون تغییر رها کرده و در قسمت Value گزینه مربوط را با توجه به توضیحات زیر انتخاب کنید:

- اگر مقدار متغیر (جان) را افزایش داده اید گزینه was increased را انتخاب کنید.
- اگر مقدار متغیر را کاهش داده اید گزینه was decreased را انتخاب نمایید.
- اگر مقدار متغیر تغییر کرده، ولی نمی دانید افزایش پیدا کرده یا کاهش (فراموش کرده اید) گزینه was changed را انتخاب کنید. ممکن است فکر کنید که این گزینه خیلی بی ربط است. اما این حالت را در نظر بگیرید: شما به بازی رفته اید و جان خود را افزایش داده اید (مثلا با خوردن یک آب حیات!) که در

بازی به رنگ آبی آنها را می بینید، مقدار جان هر کول در بازی Hercules افزایش پیدا می کند). اما درست زمانی که می خواهید از بازی خارج شوید و به ArtMoney برگردید، ناگهان چیزی (مثلا کلاخی در بازی Hercules) به شما برخورد می کند و جان شما کم می شود. شما نمی دانید که جان شما افزایش یافته یا کاهش، ولی احتمال می دهید که مقدار جانتان تغییر کرده است یعنی احتمال می دهید که مقدار افزایش جان شما در بازی با مقدار جان از دست داده برابر نباشد که چنین نیز هست (چون در بازی Hercules از نوع 4 بایتی استفاده شده احتمال بسیار کمی وجود دارد که مقدار افزوده شده با مقدار کاسته شده برابر باشد). در این حالت شما از گزینه was changed استفاده می کنید که با اندک ریسکی هم همراه است.

• اگر مقدار متغیر را تغییر نداده اید گزینه was not changed را انتخاب کنید. بعدا خواهم گفت که چرا حتما باید از این گزینه استفاده کنید.

• اگر مقدار متغیر را افزایش داده اید و می دانید که به چه اندازه این کار را انجام داده اید گزینه was increased by را انتخاب کنید و در کادر باز شده مقدار افزایش را وارد نمایید. البته در بازی Hercules این کار غیر ممکن است. این را هم بعدا خواهم گفت.

• اگر مقدار متغیر را به اندازه معلوم کاهش داده اید گزینه decreased by was

واضح است که نمی توانید از گزینه های 5 و 6 در مورد این بازی بهره ببرید.

با استفاده از این توضیحات گزینه مورد نظر خود را انتخاب کنید و OK را بزنید. با این کار جستجو ادامه یافته و تعداد یافته ها مشخص می شود. به بازی برگشته و کار را به همین شکل ادامه دهید تا به نتیجه نهایی برسید.

چند تذکر

حتما از گزینه was not changed استفاده کنید. اگر برای بازی های مختلف از روش Unknown Value استفاده کنید، خواهید دید که این گزینه بیشتر از تمام گزینه ها به شما در مسیر یافتن متغیر دلخواه کمک می کند. حتما می پرسید چگونه؟

برای این که از گزینه was not changed استفاده کنید باید به بازی بروید. در بازی حرکت کرده و جهت خود را عوض کنید و سعی کنید متغیرهای دیگری غیر از جان را تغییر دهید. برای مثال بدون اینکه در بازی Hercules حتی مقداری از جان خود را از دست دهید سعی کنید به عقب برگردید و در صورت امکان از شمشیرهای خود استفاده کرده و آنها را تمام کنید (در Hercules غیر از شمشیر اصلی

تمام شمشیرها پس از چند بار استفاده تمام می شوند) حال به برنامه بروید و از گزینه was not changed استفاده کنید. خواهید دید که بسیاری از متغیرهای زاید حذف می شوند. البته سعی کنید پس از یک بار استفاده از گزینه was not changed از گزینه های دیگر مثل was increased استفاده کنید و پس از چند بار استفاده از گزینه های دیگر، دوباره از گزینه was not changed استفاده نمایید. اما این که کجا می توان از گزینه های was increased by و decreased by استفاده کرد؛ جواب این را، خودتان وقتی تمرین پنجم را انجام دادید، پیدا خواهید کرد.

اما تمرین ها... تمرین های این قسمت وقت گیر هستند بنابراین فقط 5 تمرین را برای شما می دهم.

• مقدار جان هر کول را نصف کنید! و کاری کنید که هر کول همیشه به اندازه نصف اندازه کامل جان داشته باشد.

• وقتی در بازی هر کول، یک مجسمه کوچک هر کول را می خورید، خط جان بزرگتر می شود یعنی می توانید جان خود را بیشتر افزایش دهید. کاری کنید که این کادر هم به حداکثر اندازه خود برسد.

• مقدار جان را در بازی Mega ManX3 هک کنید.

• مقدار جان را در Resident Evil: Nemesis هک کنید. این بازی یک تفاوت با دیگر بازی ها دارد و آن هم این است که هیچ خط جانی را در بازی نمی بینید. فقط وقتی به قسمت انتخاب اسلحه ها می روید، در یک کادر، عکس کاراکتر خود را می بینید. اگر این کادر سبز باشد، جان شما کامل است و هر چه این کادر رنگش به قرمز نزدیکتر شود، جان شما به صفر نزدیک تر می شود. یک راهنمایی اینکه در بازی اگر از گیاهان سبز (Green Herb) استفاده کنید، جان شما افزایش می یابد.

• اما بالاخره تمرین پنجم... سعی کنید تعداد جانهای بازی Cop 2 Virtua را که به روش معمولی هک کرده بودیم، به روش استفاده از Unknown Value هک کنید. حتما خواهید فهمید که was increased by و decreased by به چه دردی می خورد

روش عملی هک بازی _____ قسمت سوم _____ ترافلدها

• متغیرهای کد شده

اگر به هر روشی عمل کردید و نتوانستید بازی را هک کنید به احتمال 90 درصد متغیر مورد نظر شما کد شده است. 10 درصد بقیه را به امکان اشتباه اختصاص می دهیم و یک احتمال هم این است که از متغیرهای Reverse یا معکوس در بازی استفاده شده باشد که احتمال آن بسیار کم است.

روش هک بازی های کد شده بسیار وقت گیر است و ممکن است چند ساعت طول بکشد. علل این وقت گیر بودن به شرح زیر است.

- اگر از روش Coded Value استفاده کنید نمی توانید نوع داده را تعیین کنید. یعنی اگر شما پس از زدن کلید Search گزینه Coded Value را برگزینید دو قسمت Value و Type غیرفعال می شوند. به همین دلیل تمام انواع متغیرها جستجو می شوند.

- در پنجره Filter شما در قسمت Value فقط 2 گزینه می بینید. یکی was changed و دیگری was not changed. بنابراین شما نمی توانید به راحتی متغیر خود را بیابید.

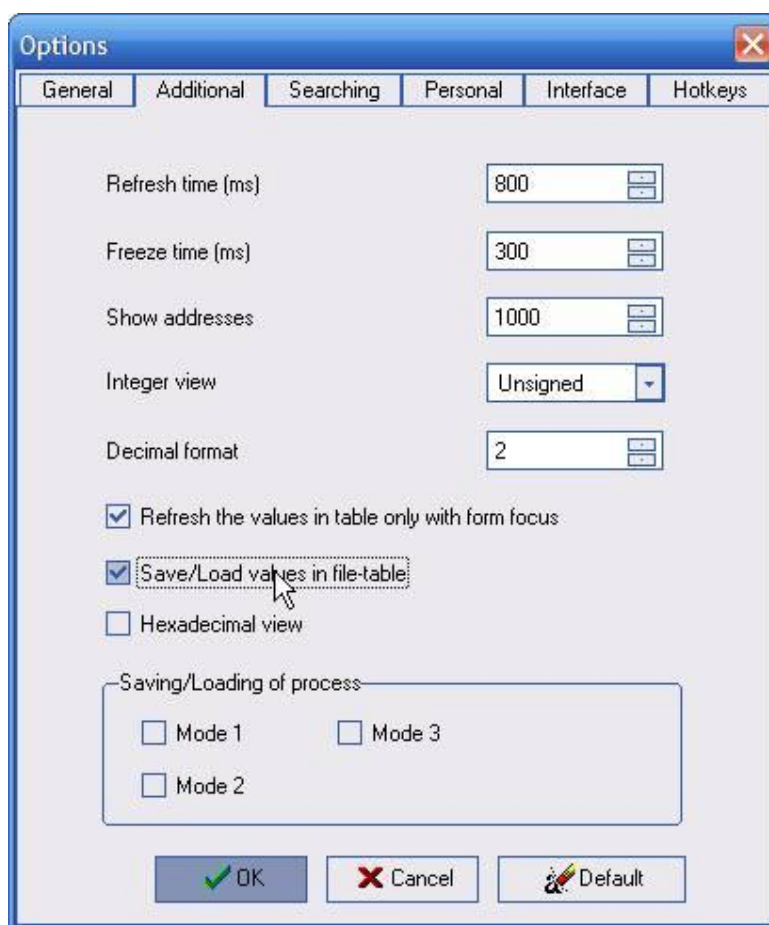
به هر حال اگر بخواهید حتما بازی را هک کنید از این روش استفاده نمایید ولی اگر نیاز مبرمی به یافتن آن ندارید بهتر است از خیر جستجو کردن بگذرید. به جای جستجو به این روش سعی کنید در بازی قرائنی برای متغیر دلخواه خود بیابید. برای مثال اگر تعداد جان شما کد شده است سعی کنید تعداد Continue های خود را افزایش دهید. مثلا در بازی Allods مقدار پول شما کد شده است اما شما می توانید تعداد شمشیرهای خود را هک کنید و سپس آنها را بفروشید و پول خوبی به دست بیاورید. در بازی War Craft 3 طلا کد شده است اما شما می توانید آن را به مقدار زیاد در معدن بیابید. ممکن است کل کار شما با یک اشتباه از بین برود که این به صرفه نیست.

2) چگونه جستجوی دستی

فرض کنیم شما به یکی از روش های Unknown یا Coded متغیری را جستجو کردید. با تمام دقتی که در انجام کارتان به خرج دادید نتوانستید به یک یا دو متغیر برسید و متغیرهایی که یافته اید اصلا کمتر نمی شوند. برای رفع مشکل و برای این که بازی شما هنگ نکند باید از روش زیر بهره بگیرید.

برای این که بتوانیم به نتیجه برسیم باید متغیرها را به طور دستی جدا کنیم. برای این کار تمام داده های یافته شده را به سمت راست انتقال می دهیم. نباید بیش از 10 عدد متغیر را منتقل کرد چون باعث دشواری بیشتر کار می شود. پس سعی کنید تعداد متغیرها را به کمتر از ده تا برسانید و سپس آنها را به سمت راست انتقال دهید. اگر می خواهید تمام متغیرها را یکجا به سمت راست منتقل کنید از کلید سبز رنگ و اگر می خواهید یکی یکی آنها را به سمت راست انتقال دهید، از کلید قرمز رنگ استفاده کنید.

متغیر اول را Freeze کنید. قبلا طریقه Freezing را دیدیم. به بازی بروید و کاری کنید که متغیر شما تغییر کند. اگر دیدید که مثلا با از دست دادن جان هیچ اتفاقی رخ نمی دهد، یعنی تعداد جان شما در بازی هیچ تغییری نمی کند، آنگاه به برنامه ArtMoney برگردید. می توانید پس از یافتن متغیر خود دیگر ادامه ندهید اما به هر حال بهتر است اثر تمام متغیرها را بررسی کنید. پس از این که یک متغیر را یافتید که با Freeze کردن آن بازی هک می شود، بقیه را پاک کنید. اگر با Freezing چند متغیر نتیجه یکسانی حاصل شد سعی کنید آن را که مقدارش کمتر است را انتخاب کنید. این برای خودتان بهتر است چون اگر در فایل ذخیره شده مقدار دلخواه شما از بین رفت، راحت تر بتوانید آن را به خاطر بیاورید. پس از پاک کردن بقیه متغیرها، نام متغیر را تغییر دهید. قبلا از فعال بودن این گزینه در Option برنامه مطمئن شوید.



سپس با فشردن Save یافته های خود را ذخیره کنید تا بعدا بتوانید از آنها استفاده کنید.

روش تنظیم روی حداکثر مقدار

برای تنظیم روی حداکثر مقدار ممکن، فایل amt را ذخیره کنید. بازی را ببندید و بار دیگر باز کنید. یک بازی جدید شروع کنید. به ArtMoney برگردید و فایل ذخیره شده خود را باز کنید. متغیرهای آن را از

حالت Freeze خارج کنید. اندکی صبر کنید و سپس Freeze را بزنید. البته این کار بهتر است در Integer 4 Byte انجام گیرد. پس از انجام این عمل فایل را ذخیره کنید.

بازگردانی یا Loading

وقتی متغیرهای دلخواه خود را یافتید و ذخیره نمودید برای استفاده مجدد در دفعات بعدی باید به این شکل عمل کنید.

برنامه ArtMoney را گشوده و پس از آن بازی را آغاز نمایید. بعد از شروع بازی به برنامه برگردید و نام بازی را از محل انتخاب پروسه ها در بالای صفحه انتخاب کنید. پس از انتخاب روی کلید Load کلیک کنید. سپس به آدرسی که فایل amt را در آنجا ذخیره کرده بودید بروید و آن را انتخاب نمایید. به بازی برگشته و از آن لذت ببرید. (پسوند amt پسوند مورد استفاده برنامه ArtMoney است. در نسخه های قدیمی تر به جای این پسوند از پسوند art استفاده می شد که قابلیت کمی در ذخیره نام متغیرها و مقدار آن داشت.)

روش دیگر این است که در ابتدا از منوی Table گزینه Load را انتخاب کنید و سپس بازی را اجرا نمایید. پس از رفتن به بازی به برنامه برگشته و نام آن را از منوی افنان بالای صفحه انتخاب کنید و به بازی بروید.

مرف آفر

پنجره Options را بررسی می کنیم.

General: در مقابل Object دو گزینه وجود دارد. یکی Process و دیگری File. گزینه Process به حالت پیش فرض فعال است و روش کار ما در بالا تماما بر اساس این گزینه بود. یعنی ما پروسه فعال بازی که در حال اجرا بود را جستجو می کردیم. اما در File شرایط کمی فرق می کند. برای کار با این گزینه، شما خود بازی را مستقیما هک نمی کنید. شما بازی را ذخیره می کنید. در هنگام ذخیره بازی یک فایل روی کامپیوتر شما تغییر می کند و یا ایجاد می شود که تمام متغیرهای مهم بازی را در خود دارد. روش هک دقیقاً به شکل قبلی است با این تفاوت که برای Filter کردن باید باز هم به بازی رفته و آن را ذخیره کنید و فایل جدید را بررسی کنید. این روش مزیت ها و معایبی دارد:

- مزیت این روش آن است که در فایل ذخیره شده تمام متغیرهای زاید حذف می شوند و بازی فقط متغیرهای مهم را ذخیره می کند. به همین علت سرعت عملیات بیشتر می شود و حتی ممکن است در همان اولین فیلتر به نتیجه برسید.

- یکی از مشکلات این روش آن است که معمولا بازی ها فایل های ذخیره شده خود را در جاهایی که در دید کاربر باشد قرار نمی دهند و یافتن فایل ذخیره شده دشوار است.

- مشکل دیگر این است که تمام بازیها امکانات ذخیره لحظه ای ندارند. مثلا Resident Evil یا Dino Crisis را فقط در بعضی از اتاق ها می توان ذخیره نمود.

درمقابل Show Processes نیز 3 گزینه دیده میشود. این گزینه ها مشخص می کنند که در منوی افنان بالای برنامه چه پروسه هایی نمایش داده شوند. در نسخه های قبلی ArtMoney، تمام پروسه های فعال در ویندوز دیده می شدند و پیدا کردن نام بازی مصیبتی بود. اما اگر در اینجا Visible را انتخاب کنید دیگر مشکلی نخواهید داشت.

اگر نتوانستید متغیر دلخواه خود را بیابید گزینه های روبروی viewer Library for process را یکی یکی امتحان کنید. ممکن است به نتیجه بهتری برسید. اگر نمی خواهید AUTO را انتخاب نمایید.

دو گزینه بعدی مربوط به زبان ArtMoney است. گزینه Economize disc space باعث می شود که در حافظه کامپیوتر صرفه جویی شود. بنابراین با انتخاب این گزینه دیگر نمی توانید از ابزارهای Unknown و Coded Value استفاده کنید چون این ابزارها به فضای زیادی نیاز دارند. اگر گزینه Enable Undo/Redo the filtration باعث می شود که یک نسخه از فیلتر قبلی در حافظه باقی بماند. در صورت انتخاب این گزینه می توانید اگر اشتباهی را مرتکب شدید آن را بازگردانید و دیگر کار را از اول شروع نکنید. به نظر من، اگر مقدار حافظه کامپیوتر شما زیاد است، حتما این گزینه را فعال و گزینه قبل از آن را غیرفعال کنید. مطمئن باشید که ضرر نمی کنید.

Additional: در مقابل عبارت Refresh time عددی با واحد میلی ثانیه نوشته می شود. به طور پیش فرض هر 800 میلی ثانیه یک بار برنامه ArtMoney به بازی رجوع می کند و مقدار آدرس را به روز می کند که زمان بسیار خوبی است، ولی شما به این سرعت بالا احتیاجی ندارید و می توانید اگر از کامپیوترهای قدیمی استفاده می کنید، مقدار را افزایش داده و حتی به 5000 میلی ثانیه برسانید. گزینه Freeze time نیز فواصل بین update کردن مقدار یک متغیر یخ زده را تنظیم می کند. به طور پیش فرض هر 500 میلی ثانیه یک بار برنامه ArtMoney بازی را مجبور به بازگرداندن مقدار متغیر می کند. در بعضی از بازی ها این مقدار هم کافی نیست و باید مقدار کمتری را انتخاب کنید.

در گزینه بعدی تعداد آدرس های یافته شده که نمایش داده می شوند را می بینید. همانطور که قبلا اشاره کرده بودم، می توانید این مقدار را اضافه یا کم کنید. گزینه چهارم و پنجم مربوط به نحوه نمایش اعداد

است که لزومی ندارد تغییری در آنها ایجاد شود اما گزینه Decimal Format برای بعضی از بازی ها باید تغییر کند.

گزینه Refresh the... باعث می شود که مقادیر متغیرها در کادر سمت راست با تغییر مقدار آنها در بازی تغییر یابد. بنا به گفته نویسنده برنامه، این گزینه برای کامپیوترهای کم سرعت توصیه نمی شود.

گزینه Save/Load... قبلا توضیح داده شد. گزینه Hexadecimal view برای نمایش اعداد در مبنای 16 به کار می رود (که در ایران زیاد شناخته شده نیستند).

سه گزینه Mode در پایین مربوط به نسخه Pro هستند. با استفاده از این گزینه ها و یک روش با عنوان Filter By Formula می توانید در یک مرحله و بدون نیاز به تکرار Filter به متغیر دلخواه خود برسید.

Searching: در مقابل Game type نوع بازی خود را انتخاب کنید. نوع Win32 بازی های ویندوزهای NT و 2000 و XP است. نوع Win16 بازی های ویندوزهای 3.1 و 95 و 98 و Me می باشد و نوع Dos برای بازیهای تحت داس است. بهتر است از گزینه Auto استفاده کنید.

گزینه Bytes order را تغییر ندهید. این گزینه را فقط کسانی که بازیهای شبیه سازی شده را با استفاده از سی پی یو Motorola بازی میکنند، باید انتخاب نمایند.

گزینه بعدی از روی معنی کاملا واضح است. (مکث بازی در هنگام جستجو که بهتر است انتخاب شود)

گزینه Search in address range زمانی به کار می رود که شما آدرس تقریبی متغیر را بدانید. این را نمی توانم اینجا توضیح بدهم چون خیلی تخصصی است. اگر می خواهید PM بزنید و دقیقا بگویید که چه می خواهید بدانید. سعی می کنم هر چه زودتر پاسخ شما را بدهم.

گزینه Scan priority دقت جستجو را مشخص می کند که هر چه بیشتر باشد احتمال یافتن بیشتر می شود اما به همان نسبت سرعت جستجو کاهش می یابد.

Personal: برای وارد کردن اطلاعات شخصی شماست. این اطلاعات در فایل ذخیره شده شما نیز حفظ می شوند.

Interface: پوسته برنامه را تغییر می دهد.

Hotkeys: کلیدهای میان بر را نمایش می دهد و ویرایش می کند. همانطور که قبلا هم گفتیم، این کلیدها را تغییر ندهید. همانطور که تا حالا هم فهمیده اید من چیزی را بدون علت نمی گویم. اگر این کلیدها را تغییر دهید، ممکن است با یکی از کلیدهای ویندوز یا برنامه ای مثل Word مشترک شوند و با این توصیف هر بار که شما کاری با ArtMoney می کنید، کامپیوتر یک کار هم باید در ویندوز انجام دهد که سرعت کامپیوترتان را پایین می آورد. از طرف دیگر اگر این کلیدها را عوض کنید و بعد هم مطالب من را بخوانید، همه کلیدها را اشتباه خواهید زد.

کار ما تقریباً با ArtMoney تمام شد. اما شما هم پس از اینکه تمام قسمتهایی را که من گفتم را یاد گرفتید، در برنامه بگردید و هر چیزی را هم که نفهمیدید خیلی راحت از من بپرسید. گفتم "پس از" این که مطالب را خواندید. نه این که همین الان بروید به قسمت راهنمایی سایت و هر چه می توانید نامه بنویسید. دوم اینکه از هر چه که سؤال می کنید، لطفاً از Memory Editor که در ArtMoney هست سؤال نپرسید. به امید موفقیت و به امید این که تماستان را با ما قطع نکنید. اگر ورژن جدیدی آمد، حتماً مطالب را اضافه می کنم.

تفاوت بین Range of Values و Sequence of Values

همانطور که قبلا هم دیدید، ما زمانی از Range of Values استفاده می کردیم که دقیقاً مقدار متغیر مورد جستجو را نمی دانستیم. اما از Sequence of Values چه زمانی استفاده می کنیم؟

در بعضی از بازی ها شما چیزهای مختلفی دارید. برای مثال شما 10 عدد الماس، 5 تا انگشتر طلا، 9 عدد انگشتر نقره ای و 7 تا چوب سحر آمیز دارید. اگر شما بخواهید، می توانید یکی یکی همه اینها را هک کنید. اما مسئله مهم وقت شماست.

ما احتمال می دهیم که این متغیرها در یک خانه از حافظه واقع شده باشند. با این حدث، ما از ابزار Sequence of Values استفاده می کنیم. به این ترتیب که بازی را اجرا کرده و نام بازی را در ArtMoney انتخاب می کنیم. روی کلید Search کلیک کرده و از قسمت Search گزینه Sequence of values را انتخاب می کنیم. قسمت دوم حذف می شود و به جای آن عبارت Number of values ظاهر می شود. در مقابل این گزینه عدد 4 را بنویسید چون ما 4 چیز برای هک داریم. از قسمت پایین گزینه Integer را انتخاب کنید. کلید OK را بزنید. صفحه ای باز می شود که 4 مکان برای نوشتن در آن می بینید. در اولی بنویسید 10 و به ترتیب در دومی و سومی و چهارمی بنویسید 5 و 9 و 7. با این عمل ممکن است که در همان جستجوی اول به نتیجه برسید. اگر به نتیجه نرسیدید و هیچ متغیری یافت نشد از ابزارهای معمولی استفاده کنید.

با تشکر: Sgame-Eminem

راستی نظر یادت نره.....

دوستان کلیه حقوق این مطالب متعلق به M E H D I. مدیر انجمن بازی هادر سایت
P30World.com می باشد لطفا کپی برداری نکنید با تشکر از M E H D I به خاطر تهیه چنین
آموزش هایی