

دانشكده مهندسي كامپيوتر

گروه مهندسی نرم افزار

عنوان پروژه:

کرک نرم افزار Acme Photo ScreenSaver Maker به وسیله OllyDBG

پیش نویس اول پروژه کلاسی شماره ۵ درس کامپایلر پیشرفته

دانشجو:

مرتضی ذاکری

استاد:

دکتر سعید پارسا

پاییز ۱۳۹۵

فهرست مطالب

۱	مە	۱ مقده
۱	ۍ انجام کار	۲ شرح
۱	ابزارهای مورد نیاز	۲_۱
۲	نصب نرم افزار	۲_۲
۲	نوع حمله	۳_۲
۴	فرايند تحليل كد	۴_۲
۱۷	به گیری	۳ نتيج
۱۷	ع و ماخذع	۴ منابع

۱ مقدمه

در این گزارش نحوه کرک نرم افزار Acme Photo ScreenSaver Maker نسخه ۴٬۵۰ را بر روی ویندوز ۱۰ بررسی می کنیم. Acme Photo ScreenSaver Maker نرم افزاری جالب و قدرتمند برای ساخت محافظ صفحه نمایش از عکس های شما در کمترین زمان ممکن، است. این برنامه با محیط کاربری ساده و زیبا به شما کمک می کند تا عکس های خود را به راحتی به اسکرین سیور تبدیل کنید. شما می توانید تو سط این برنامه بر روی عکس های خود افکت های زیبا و موزیک های دلخواه قرار دهید تا زیبایی خاصی به آن دهید، این برنامه برای زیبایی کار دارای تنظیمات متفاوتی است که شما بدون هیچ تخصصی می توانید از آن بهره ببرید. مهچنین می توانید نوشیته های دلخواه خود را درون برنامه تایپ کنید و به آن افکت های زیبایی ببخ شید و در ا سکرین سیور خود از آن ا ستفاده نمایید. از نقاط واقعا مثبت این برنامه می توان به پشتیبانی آن از فونت ها و نوشته های فارسی اشاره کرد چون اکثر برنامه ها حروف فارسی را جدا جدا می نویسند.

این نرم افزار رایگان نیست و برای استفاده از تمامی امکانات آن بایستی آن را از شرکت ایجاد کننده خریداری کنیم. اما می توان با Debug کد آن ساز و کار بررسی Registration Code را تشخیص داده و آن را دور زد. در ادامه به شرح روش انجام این کار می پردازیم.

۲ شرح انجام کار

۱_۲ ابزارهای مورد نیاز

ابزارهایی که در این گزارش استفاده شده اند عبارت اند از:

- PEiD-0.95-20081103 جهت شــناسـایی زبان برنامه نویسـی برنامه و نوع Packer
 استفاده شده در صورت وجود.
 - OllyDBG 110: جهت اجرای برنامه در مد Debug و کرک آن.

۲_۲ نصب نرم افزار

ابتدا نرم افزار Help گزینه ... Acme Photo ScreenSaver Maker را دریافت و آن را نصب می کنیم. نرم افزار را اجرا می کنیم و از منوی Help گزینه ... About را می زنیم. همان طور که مشاهده می شود نرم افزار ثبت نشده و به همین دلیل محدودیت هایی دارد. از جمله این که هر بسته ای که شما با این نرم افزار ایجاد می کنید می تواند حداکثر ۷ عدد عکس در خود داشته باشد. برای رفع این محدودیت باید نرم افزار را خریداری کرده یا این محدودیت را در داخل کد برنامه تشخیص داده و آن را غیر فعال کنیم.



۲_۳ نوع حمله

در پنجره شکل فوق بر روی گزینه Register کلیک می کنیم و در قسمت های نشان داده شده متن دلخواهی را وارد می کنیم.

Acme Photo ScreenSaver N	Maker 🔀
	Acme Photo ScreenSaver Maker Version 4.50
	Produced by Acme Photo Software
	http://www.acme-photo-screensaver-maker.com
	support@acme-photo-screensaver-maker.com
	Copyright(C) 2013 Acme Photo Software
Shareware Version	
Unregistered version can at	most package 7 photos in the final screen saver.
You can unlock this functio	n limit after purchasing a full licensed version.
Licensed to Name:	Morteza
Registration Code:	1234567 Verify
Purchase	ОК

گزینه Verify می زنیم. پیام خطای زیر ظاهر می شـود که نشـان دهنده نادرسـت بود مقادیر ورودی توسط ما است.



نوع حمله برای قانونی کردن یا شکست قفل نرم افزار ها یا در ا صطلاح همان Crack عموما بر سه دسته کلی است، که عبارتند از:

۱. Serial Fishing: در این حالت یک (یا چند) شماره سریال ثابت در کد اجرایی برنامه ثبت شده و برنامه سریال ورودی کاربر را با این شماره (ها) مقایسه می کند. پس کافی است تا (یکی از) این شماره (ها) را به د ست آوریم. با توجه به سادگی بیش از اندازه، این روش امروزه به ندرت استفاده می شود.

- ۲. Key Generator یا Key Generator: در این روش برنامه صحت شمارسریال ها را با یک الگوریتم در داخل کد خود برر سی می کند. بنابراین بایستی این ساز و کار الگوریتم را تشخیص داد و سپس برنامه ای به نام KeyGen نوشت که سریال های معتبر تولید کند. این روش کمی پیچیده تر است و تشخیص ساز و کار الگوریتم ممکن است زمانبر باشد.
- ۳. Patching: در این روش فایل اجرایی اصلی برنامه تحلیل می شود و مسیر دسترسی به پیغام موفقیت یا پیغام های مشابه آن و نیز پیغام های خطا (مشابه شکل فوق) که ناشی از نادر ست بودن اطلاعات ورودی است، از داخل کد استخراج می شود، سپس تغییراتی در مسیرهای اجرایی کد داده می شود به نحوی که کنترل اجرای برنامه به پیغام موفقیت بر سد و در این حالت برنامه کا درمده یا قفل آن شکسته شده است. در نهایت فایل تغییر داده شده این در می در این حالت برنامه علی خطا (می این می شود به نحوی که کنترل اجرای برنامه به ویغام موفقیت بر سد و در این حالت برنامه کا درمده یا قفل آن شکسته شده است. در نهایت فایل تغییر داده شده را به یک فایل اجرایی تبدیل کرده و آن را جایگزین فایل اجرایی اصلی می کنند. Patching شایع ترین نوع Crack برنامه ها و نرم افزار ها است و لازمه آن درک کامل بخش هایی از ساختار فایل اجرایی است که مربوط به عملیات بررسی صحت اطلاعات می شود.

برای نرم افزار Acme که مورد بحث ما است؛ در حال حاضر ذهنیتی نسبت به انتخاب یکی از روش های فوق یا هر روش دیگری نداریم. اما می توان حدس هایی زد(!). از آن جایی که Registration Code بعد از خرید برنامه توسط وب سایت شرکت در اختیار گذاشته می شود، بعید است که از روش اول برای بررسی صحت آن استفاده شده باشد. همچنین از آن جا که یافتن الگوریتم نیز زمانبر است و ممکن است موفق نشویم روش دوم نیز کارآمد نیست. لذا چنان چه در ادامه هم خواهیم دید با یافتن متن همه پیام ها داخل کد، متوجه می شویم که به آسانی می توان از رویکرد Patching برای ایجاد یک فایل اجرایی ثانویه معتبر (!) بهره گرفت.

۲_۴ فرایند تحلیل کد

در این قسمت گام به گام اقدامات انجام شده برای Crack نرم افزار Acme شرح می دهیم.

پیام خطای ناشی از نادرست بود اطلاعات ثبت نرم افزار را یادداشت می کنیم.

۲. فایل اجرایی برنامه را PEiD باز می کنیم. مشاهده می شود که نرم افزار با زبان
 ۲. فایل اجرایی برنامه را Disassembler نوشته شده است و کد آن هم Pack نشده است. این بدین
 معنی است که می توان براحتی آن را توسط سه Disassembler و Debugger گشود.

🔛 PEiD ∨0.95							
File: C:\AcmeSoft\Acme Photo ScreenSaver Maker\Apssm.exe							
Entrypoint: 00006C9C File Offset: 00006C9C	EP Section:.textFirst Bytes:68,00,70,40						
Linker Info: 6.0	Subsystem: Win32 GUI >						
Microsoft Visual Basic 5.0 / 6.0 Multi Scan Task Viewer Options About ✓ Stay on top							

(> - + +	LEMTWHC/KI	R S 🔚 📰 ?			
CPU - main thread, mo	ule ntdll			- 0	x
560974 895C24 08	MOV DWORD PTR SS:[ESP+8],EBX			∧ Registers (FPU) < <	<
560978 ^ E9 OCO6FE	F JMP ntdll.77550F89			EAX 00406C9C Apssm. ModuleEntryPoint>	
56097D 8D49 00	LEA ECX, DWORD PTR DS: [ECX]			ECX 0000000	
560980 8BD4	MOV EDX,ESP			EDX 00000000	
7560982 0F34	SYSENTER			EBX 00200000	
7560984 8DA424 00	0000(LEA ESP, DWORD PTR SS:[ESP]			ESP 0019FFF0	
756098B 🖉 EB 03	JMP_SHORT_ntdll.KiFastSystemCallRet			EBP 00000000	
756098D CC	INT3			ESI 0000000	
756098E CC	INT3			EDI 00000000	
756098F CC	INT3				
7560990 C3	RETN			EIP 77560974 httd11.77560974	
7560991 8DA424 00	0000(LEA ESP, DWORD PTR SS:[ESP]			C 0 ES 002B 32bit 0(FFFFFFFF)	
7560998 8DA424 00	00000(LEA ESP,DWORD PTR SS:[ESP]			P 0 CS 0023 32bit 0(FFFFFFFF)	
756099F 90	NOP			A 0 SS 002B 32bit 0(FFFFFFFF)	
75609A0 8D5424 04	LEA EDX, DWORD PTR SS:[ESP+8]			Z 0 DS 002B 32bit 0(FFFFFFFF)	
75609A4 CD 2E	INT 2E			5 0 F5 0053 32bit 203000(FFF)	
75609A6 C3	RETN			T 0 GS 002B 32bit 0(FFFFFFFF)	
75609A7 CC	1013			V D 0	
BX=00200000	11ALX			0 0 LastErr ERROR_ENVVAR_NOT_FOUND (000000CB)	
tack 55:[0019FFF8]	0000000			EFL 00000202 (ND,NB,NE,A,NS,PD,GE,G)	
ddress ASCII dump		0019FF	0 00000000		^
04A8000		0019FF	4 00406C9C Aps	ssm. <moduleentrypoint></moduleentrypoint>	
04A8020		0019FF	8 00000000		
04A8040		0019FFI	C 00000000		
04A8060					
04A8080					
04A80A0					
04A80C0					
04A80E0					
04A8100					
04A8120					
04A8140					
04A8160					
04A8180					
0440440					
U4A61AU					

[\] Debug

۴. پس از اجرا برنامه در حالت Pause قرار می گیرد. پنجره اجرایی پیش فرض باز شده مربوط به ماژول Intdll است که یه ماژول سیستمی حاوی توابع سیستمی می باشد. ما ابتدا باید کد فایل اجرایی Apssm.exe با فشردن کلیدهای E + L پنجره حاوی لیستی از همه ماژول های درگیر در عملیات نشان داده می شود. از این پنجره فایل ا صلی خودمان را انتخاب می کنیم (دو بار کلیک)که در این جا اولین فایل ا ست. در این پنجره همچنان می توان دید که برنامه ما از توابع سیستمی کدام فایل ها استفاده می کند که می تواند جالب باشد.

0							
	E Executa	ble modules					
	-			lu l	and the second se		
11	Base	Size	Entry	Name	File version	Path	^
	00400000	00062000	00406C9C	Apssm	4.05	C:\AcmeSoft\Acme Photo ScreenSaver Maker\Apssm.exe	
	64F00000	00092000	64F4F7C0	apphelp	10.0.14393.0 (r	C:\WINDOW5\system32\apphelp.dll	
	66000000	00153000	66001AF8	MSVBVM60	6.00.9815	C:\WINDOWS\SYSTEM32\MSVBVM60.DLL	
	73FA0000	0000A000	73FA2A90	CRYPTBAS	10.0.14393.0 (r	C:\WINDOW5\System32\CRYPTBASE.dl1	
	73FB0000	0001E000	73FBBA20	SspiCli	10.0.14393.576	C:\WINDOWS\System32\SspiCli.dll	
	74040000	00041000	740571C0	sechost	10.0.14393.0 (r	C:\WINDOW5\5ystem32\sechost.dll	
	74090000	00211000	7419F950	combase	10.0.14393.0 (r	C:\WINDOWS\System32\combase.dll	
	74260000	0005A000	742F2960	bcryptPr	10.0.14393.0 (r	C:\WINDOWS\System32\bcryptPrimitives.dll	
	74500000	001A1000	745BE5C0	KERNELBA	10.0.14393.206	C:\WINDOWS\System32\KERNELBASE.dll	
	74680000	00094000	746E8590	OLEAUT32	10.0.14393.447	C:\WINDOWS\System32\OLEAUT32.dl1	
	74750000	0007B000	74765A20	msvcp_wi	10.0.14393.0 (r	C:\WINDOWS\System32\msvcp_win.dll	
	747E0000	000E0000	7480E340	ucrtbase	10.0.14393.0 (r	C:\WINDOWS\System32\ucrtbase.dll	
	748C0000	000EA000	748F8660	ole32	10.0.14393.0 (r	C:\WINDOWS\System32\ole32.dll	
	74630000	000BE000	74B656A0	msvcrt	7.0.14393.0 (rs	C:\WINDOWS\System32\msvcrt.dll	
	74BF0000	0015F000	74BFA890	USER32	10.0.14393.0 (r	C:\WINDOWS\System32\USER32.dll	
	74D60000	00026000	74D64E60	GDI32	10.0.14393.206	C:\WINDOWS\System32\GDI32.dll	
	74D90000	000E0000	74DA5FD0	KERNEL 32	10.0.14393.206	C:\WINDOW5\System32\KERNEL32.DLL	
1	74E70000	000C1000	74E914E0	RPCRT4	10.0.14393.0 (r	C:\WINDOWS\System32\RPCRT4.dll	
1	74F40000	00015000		win32u	10.0.14393.51 (C:\WINDOWS\System32\win32u.dll	×
1							

- ۵. پنجره ای اکنون باز شده است کد همان فایل اجرایی ما است. برای یافتن محل پیغام خطای شماره ثبت، که در ابتدای کار آن را دیدیم باید متن پیام را جست و جو نماییم.
 برای این منظور روی پنجره کلیک راست کرده و از منوی باز شده گزینه Search for و سپس گزینه All referenced text strings را می زنیم.
- ۶. در این پنجره همه متن های ر شته ای برنامه نشان داده شده است. برای یافتن پیغام خطای شماره ثبت کلیک راست کرده و گزینه Search for را انتخاب می کنیم. کافی است در پنجره باز شده ابتدای متن پیام که عبارت ... Invalid User Name بود را وارد کنیم و سپس 0k را می زنیم.

R Text strings referenced in Apssm:.text	
Address Disassembly	Text string
00471A55 PUSH Apssm.00419EDC	UNICODE "Temp\tempicon.ico"
00471BFE PUSH Apssm.0041B828	UNICODE "24bit"
00471D27 PUSH Apssm.0041B838	UNICODE "48*"
004729F6 PUSH Apssm.0041B8CC	UNICODE "Logo.gif"
00472C1A PUSH Apssm.0041B8E4	UNICODE "mailto:"
00472EDF PUSH Apssm.0041B8F8	UNICODE "**********"
0047322A PUSH Apssm.0041B938	UNICODE "Full Licensed Version"
00473385 PUSH Apssm. 004 Enter text to search for	× your User Name and Registration Code"
004/33F2 PUSH Apssm.004	he About Window"
0047345F PUSH Apssm.004 Invalid	a secure on-line order or try other ordering options"
0047346E PUSH HUSSM.004	the registration code now
Beh71489 BUCH ODCCD Beh	zo av
88474055 1031 Hp351.884	
8847518F PUSH Apscm 884	
AA475393 PUSH Anssm. AA4	Cancel billins"
0047539E MOU EDX.Apssm.0041BAD8	UNICODE "klist"
00475385 PUSH Apssm.00414EDC	UNICODE "ISP.ini"
00475406 MOV EDX,Apssm.004110AC	UNICODE "Fantasy"
0047541F PUSH Apssm.00414EDC	UNICODE "ISP.ini"
0047547B PUSH Apssm.00414EDC	UNICODE "ISP.ini"
00475512 MOV EDX,Apssm.004110AC	UNICODE "Fantasy"
0047552B PUSH Apssm.00414EDC	UNICODE "IsP.ini"
0047559E MOV DWORD PTR SS:[EBP-F0],Apssm.0041109	UNICODE "Info"
004755EF MOV DWORD PTR SS:[EBP-D0],Apssm.0041BB1	UNICODE "Thank you for your registration!"
004755F9 MOV DWORD PTR SS:[EBP-E0],Apssm.0041BB5	(UNICODE "The program is a full licensed version now."
004756A9 MOU DWORD PTR SS:[EBP-F0],Apssm.0041BD9	UNICODE "Error"
004/56FH MUU DWORD PIR 55:[EBP-D0],HDSSm.0041BBF	UNICUDE "Invalid User Name or Registration Code?"
00475704 MOU DWORD FIR SS:[EBF-E0],HPS5M.0041866	UNICODE "Headse paste the user name and neglistration code exactly the same as they ap
80475768 MOU FDX Ancom 80418008	UNITODE USER HAME UT NEU DUE IS HULL : INITODE "USERSReshedahijulmoogeetuumuzaenderetu kkimkoonestuukuva 1246508- #/\\40\$<\&*/
804763RD PIISH Ancom 80418F04	INTCODE "confriends" and "
AAL74076 DUCH ANCON AAL4DEDA	

۲. همه پیام های مرتبط با موضوع ثبت نرم افزار مشاهده می شود. در آدرس های نشان
 داده شده در شکل با استفاده در کلید F2، نقطه توقف یا Break Point ایجاد می

كنيم.

00475512	MOV EDX,Apssm.004110AC	UNICODE "Fantasy"
0047552B	PUSH Apssm.00414EDC	UNICODE "IsP.ini"
0047559E	MOV DWORD PTR SS:[EBP-F0],Apssm.0041109	UNICODE "Info"
004755EF	MOV DWORD PTR SS:[EBP-D0],Apssm.0041BB1	UNICODE "Thank you for your registration!"
004755F9	MOV DWORD PTR SS:[EBP-E0],Apssm.0041BB5	UNICODE "The program is a full licensed version now."
004756A9	MOV DWORD PTR SS:[EBP-F0], Apssm. 0041BD9	UNICODE "Error"
004756FA	MOV DWORD PTR SS:[EBP-D0],Apssm.0041BBF	UNICODE "Invalid User Name or Registration Code!"
00475704	MOV DWORD PTR SS:[EBP-E0],Apssm.0041BCC	UNICODE "Please paste the User Name and Registration Code
		· · · · · ·

۸. با دو بار کلیک روی کد "Error" به محل استفاده آن می رویم؛ یعنی آدرس O04756A9 دقت شود که آدرس ها در مبنای ۱۶ هستند و هر رقم معادل ۴ بیت است به این ترتیب آدرس های برنامه ۳۲ بیتی هستند (حاوی ۴ بایت یا ۸ رقم مجزا) زیرا اساسا نرم افزار ما ۳۲ بیتی است. همچنین ما در حال کار بر روی کدهای اسمبلی ما شین های 85% هستیم. یعنی مجموعه د ستور العمل هایی که در این جا با آن ها سر رو کار داریم، مجموعه دستورالعمل های ماشین های 85% هستند (سوی کدهای اسمبلی ما شین های 85% هستیم. یعنی مجموعه د ستور العمل هایی که در این جا با آن ها سر رو کار داریم، مجموعه دستورالعمل های ماشین های 85% هستند مستقل از این که چه معماری داخلی دارند و یا این که محصول کدام شرکت هستند (نوعی استادارد). مثلا پردازنده های سری ™Intel یک ویک وی این دستورالعمل ها ماشین های 100 را دارند و یا این که محصول کدام شرکت هستند مستقل از این را دارند(یده). مثلا پردازنده های سری ™Debugger برای مجموعه دستورالعمل های این ار دارنده ای این که محصول کدام شرکت های 100 این دستورالعمل های این دستورالعمل های این که محصول کدام شرکت هستند (نوعی می استاندارد). مثلا پردازنده های سری ™ODU یک Pobugger برای مجموعه دستورالعمل ما شرکت هموعه دستورالعمل های ماشین ما نیز بر روی همین ریزپردازنده اجرا می می شود.

۹. خطای "... Invalid User Name or" نیز در آدرس 004756FA قرار دارد. ایده شروع Crack نباید به عملیات Crack این است: کنترل اجرای برنامه بعد از فشردن گزینه Verify نباید به

این قسمت ها برسد، در عوض کنترل اجرا یا مسیر اجرایی باید به قسمتی که پیام "Thank you for your registration" وجود دارد يعنی آدرس 004755EF برســد. در حالت کلی روند اجرای برنامه به ترتیب از آدرس کمتر به سهمت آدرس بیش تر یا از بالا به پایین است. د ستورات پرش نقش اصلی را در تعیین مسیر اجرایی دارند و این نظم را بر هم می زنند. پس به دنبال اولین د ستور پر شی می گردیم که قبل پیام خطا قرار دارد و مقصد آن نیز بعد از پیام خطا است. این دستور حتما وجود دارد چرا که در صورت صحیح بود کد ثبت، این پیام ها دیده نمی شوند یعنی از روی آن ها پرش می شود. از آدرس 004756A9 به سمت ادرس های قبلی حرکت می کنیم. اولین د ستور یرش در آدرس 00475665 است: JMP 004757F2 که یک دستور پرش غیر شرطی به مق صد 004757F2 در همین فایل ا ست. مق صد نیز بعد از تمامی پیغام های خطا قرار دارد. نرم افزار Olly DBG به صورت خودکار با کلیک کردن بر روی دستور مقصد آن را نشان می دهد. آن چه گفته شد بدین معنی است که اگر این پرش انجام شود برنامه Register خواهد شد، زیرا از سد پیغام های خطا به سلامت عبور کرده است. از آن جایی که پرش غیر شرطی است کافی است به نحوی کنترل اجرا به آن بر سد در این صورت حتما اجرا خواهد شد. اما اگر کنترل اجرا به آن نرسد، یعنی از روی آن پرش كند، (به دستور بلافصله قبل از آن برسد) اجرا نمى شود. دستور بلافاصله بعد از اين د ستور LEA^۲ است. با کلیک روی آن و سپس Ctrl + R تمامی آدرس هایی که د ستور موجود در آن ها به این دستور پرش می کنند نشان داده می شود. این از جمله امکاناتی است که Olly DBG را بسیار محبوب می نمایید.

^r Load Effective Address

Reference	es in Apssm:.text to 0047566A	
Address	Disassembly	Comment
00473F53	JNZ Apssm.0047566A	
004743D3	JNZ Apssm.0047566A	
00474418	JN2 Apssm.0047566A	
0047450D 00474DFF	JA ADSSM 0047566A	
00474EAD	JA ADSSM.0047566A	
00475018	JNZ Apssm.0047566A	
00475175	JNZ Apssm.0047566A	
0047566A	LEA EAX,DWORD PTR SS:[EBP-78]	(Initial CPU selection)
		•

۱۰. همان طور که مشاهده می شود از ۸ مکان مختلف با دستورات پرش شرطی INZ و AL به این مکان پرش می شـود. این رفتار حالت ایسـتای برنامه اسـت و در هنگام اجرا مشخص می شود که از کدام دستور به این محل پرش خواهد شد. به هر حال هر کدام از این پرش ها که اتفاق بیفتند، کنترل اجرا از روی دستور JMP پرش می کند و برنامه Register نخواهد شد. پس باید ضمن اجرا برنامه کاری کنیم تا هریک از این پرش ها که شـرط آن ها برقرار است، انجام نشـوند یعنی شـرط آن ها را برهم بزنیم یا این که مقصد آن ها را عوض کنیم، که حتی در صورت برقرار بود شرط باز هم به این مقصد پرش نکنند. روش دوم خیلی راحت تر است اما باید در انتخاب مقصد خیلی دقت شود چرا که ممکن اسـت **کنترل به طور کلی** به هم بریزد. راه حل هوشــمندانه به این صورت خواهد بود که مقصد دستور پرش را دسـتور بعدی قرار دهیم (!!!) یعنی **چه** د **ستور پرش اجرا شود چه اجرا نشود کنترل برنامه تغییری نخواهد کرد**. چون م میر بعد از اجرای د ستور پرش شرطی نیز معتبر ا ست یعنی از قبل تحت شرایطی قطعا کنترل اجرا به آن می ر سیده است، به این ترتیب هیچ مشکلی در کنترل اجرای برنامه به وجود نمی آید، تنها وجود این دسـتور پرش بی اثر می شروایی در کنترل اجرای ۱۱.در این مرحله برای آن که هنگام اجرای برنامه روی هریک از دستورات پرش شرطی پیدا شده در مرحله قبل متوقف شویم، تا مقصد آن را عوض نماییم، روی هر کدام از آن ها Break Point قرار می دهیم.

References in Apssm.:text to 0047566A						
Address Disassembly	Comment					
00473F53 JNZ Apssm.0047566A						
004743D3 JNZ Apssm.0047566A						
004744F8 JNZ Apssm.0047566A						
00474580 JNZ HPSSM.0047500H						
AB474FAD JA AD55m_AB47566A						
00475018 JNZ Apssm.0047566A						
00475175 JNZ Apssm.0047566A						
0047566A LEA EAX,DWORD PTR SS:[EBP-78]	(Initial CPU selection)					
	×					

۱۲.اجرای برنامه را با یک بار فشردن کلید F9 ادامه می دهیم.

- ۱۳.بار دیگر برنامه متوقف می شود. البته نه در مکان هایی که Break Point قرار داده ایم. به هر حال با F9 ادامه می دهیم تا برنامه باز شود.
- ۱۴. اکنون اطلاعاتی دلخواه را در قســمت Register وارد می کنیم و گزینه Verify را می زنیم.
- JMP مشاهده می شود که برنامه در اولین آدرس حاوی دستور پرش شرطی به بعد از JMP متوقف شد (آدرس 300,000). همان مکانی که از قبل نقطه توقف گذاشته بودیم. اگر این پرش انجام شود Register انجام نمی شود است و برنامه پیغام خطا می دهد. این پرش در حال حاضر انجام می شود. در قسمت پایین سمت چپ پنجره اصلی برنامه Olly DBG می توان مشاهده کرد که آیا پرش انجام می شود یا خیر.

Jump is taken 0047566A=Apssm.0047566A ۱۶. ما اجازه نمی دهیم این پرش انجام شود. طول دستور "JNZ به طور کلی ۶ بایت است یعنی دستور بعدی از آدرس 2009 (6 + 2003) (2 + 2004) (2

CollyDbg - Apssm.exe - [CPU - m	nain thread, module Apssm]			- 0 ×
File View Debug Plugins	Options Window Help			- 8 ×
	LEMTWHC/K	B R S 🗄 📰 ?		
00473F4A . FF15 30134000	CALL DWORD PTR DS:[<&MSVBVM60vbaFree	MSVBVM60vbaFreeObj	∧ Registers (FPU) < ·	< < < < < < < < <
00473F50 . 66:85DB 1	TEST BX,BX		ESP 0019ED8C	
00473F53 0F84 11170000	JE Apssm.0047566A		EBP 0019EF40	
00473F59 . 8B0F	NOV ECX, DWORD PTR DS:[EDI]		ESI 660D9FF1 MSVBVM60vbaObjSet	
00473F5B . 57	PUSH EDI		EDI 00757C30	
00473FSC . FF91 04030000	ALL DWORD PIR DS:[ECX+304]	Assemble at 00473F53 X	FTP 00473F53 Apssm. 00473F53	
00473565 50	DISH EAY			
00473E66 52	DISH EDX	<u>96.00475554</u>	C 0 ES 002B 32bit 0(FFFFFFF)	
00473E67 . EED6	ALL EST		P 1 CS 0023 32D1t 0(FFFFFFFF)	
00473F69 . 88D8	IOV EBX. EAX	Fill with NOP's Assemble Cancel	A 0 55 0028 52010 0(FFFFFFFF)	
00473F6B . 8D4D BC L	EA ECX, DWORD PTR SS:[EBP-44]		S 1 ES 0053 32bit 228000(EEE)	
00473F6E . 51 F	PUSH ECX		T 0 65 0028 32bit 0(FFFFFFFF)	
00473F6F . 53 F	PUSH EBX		D O	
00473F70 . 8B03 M	MOV EAX, DWORD PTR DS:[EBX]		0 0 LastErr ERROR_SUCCESS (00000000)	
00473F72 . FF90 A000000	TALL DWORD PTR DS:[EAX+A0]		551 00300305 (NO NO NE A C DE L LE)	
00473F78 . 85C0 1	TEST EAX,EAX		EFL 00200288 (NO,ND,NE,A,S,PE,L,LE)	
00473F7A . DBE2	FCLEX		STO empty -??? FFFF 00D2D2D2 20E6E6E6	
00473F7C . 7D 12	JGE SHORT Apssm.00473F90		ST1 empty 8192.000000000000000	
00473F7E . 68 A000000 F	PUSH 0A0		ST2 empty -??? FFFF 0080D190 D190D190	
00473583 . 68 94434100 8	105H AD22H 00414594		ST3 empty -??? FFFF 00800080 00800080	
00473588 50			ST4 empty -??? FFFF 00000000 20141414	
00473E8A . EE15 84104000	ALL DWORD PTR DS: FKAMSVBVM60. vbaHnesi	MSVBVM60, vbaHresultCheckObi	ST5 empty 0.0005960464477539062	
Avera da UNT talva			ST6 empty 0.062500000000000000	
00475664=4prcm 00475664			3 2 1 0 E S P II O Z D T	
0047300A-Apssill.0047300A				(50)
Address ASCII dump			▲ 0019E08C 0019EFAC	^
004A8000ÿÿ			00195090 00757C30	
004A8020 (<u. td="" ÿüi<="" ē¼€ÿ×x.=""><td>iuÿ ým.āāāÿ</td><td></td><td>00195094 00000001</td><td></td></u.>	iuÿ ým.āāāÿ		00195094 00000001	
004A8040 ×N 0" a ((+^1)			00195096 00020860	
00448060			0019EDA0 0019EEE0	
00448040	. 1		0019EDA4 74C215B0 USER32.74C	21580
00448000 (u. 1u		0019EDA8 FFFFFFFF	
004A80E0			0019EDAC FFFFFFE	
004A8100 ÿÿ			0019EDB0 -0019EE18	
004A8120 00.0	pBq.		0019EDB4 6605D314 RETURN to !	ISVBVM60.6605D314 from ntdll.Ntdl
004A8140 d	Dq.d		0019EDB8 000208E0	
004A8160 [ð¼t	ÿÿ€.ÿ		0019EDBC 00000084	v .
Breakpoint at Anssm 00473E53			· · · · · · · · · · · · · · · · · · ·	Paused

اکنون چنان چه بر روی دستور کلیک کنید Olly DBG می گوید پرش انجام نمی شود.

۱۷. اجرای برنامه را با F9 پیگیری می کنیم. برنامه در آدرس 304743D3 که دومین آدرس حاوی دومین دستور پرش شرطی به بعد از JMP است متوقف می شود. اما اگر بر روی آن کلیک کنیم متوجه خواهیم شـد که شـرط لازم برای پرش یعنی O=Z در این اجرا برقرار نشده است (I=Z می باشد). پس پرشی صورت نمی گیرد. لذا نیازی نیست نوع دستور عوض شود و اجرا را با F9 ادامه می دهیم. دقت شود نیازی به فهم این نکته که چرا مثلا این پرش در این قســمت اتفاق نمی افتد و یا پرش قبلی اتفاق می افتاد، نداریم. آن چه برای ما مهم است روند کنترل اجرای برنامه است به نحوی که کنترل را

" Jump Not Zero

از محل هایی که می خواهیم عبور دهیم یا از محل هایی که نمی خواهیم عبور ندهیم. این که رفتار واقعی برنامه چیست در این جا و برای این هدف ما که همان Crack کردن برنامه است، کاربردی ندارد. هر چند می توانیم آن را نیز با بررسی دقیق تر کشف کنیم.

- ۱۸.در آدرس 004744F8 متوقف می شویم که سومین دستور پرش شرطی به بعد از دستور JMP است؛ ولی شرط پرش موجود در این آدرس هم برقرار نشده و پرش انجام نمی شود. لذا اجرا را با F9 پیگیری می کنیم.
- در آدرس MP است؛ ولی شرط پرش موجود در این آدرس هم برقرار نشده و پرش انجام دستور JMP است؛ ولی شرط پرش موجود در این آدرس هم برقرار نشده و پرش انجام نمی شود. لذا اجرا را با F9 پیگیری می کنیم. در حقیقت به نظر می رسد که با یک ساختار Switch-Case رو به رو هستیم که شرط خروج از آن برقراری شرط پرش یکی از Case ها است.
- ۲۰.در آدرس JNZ متوقف می شویم که حاوی دستور AL است و ظاهرا این بار دستور پرش شرطی ما پرش خواهد کرد(!!!). اما باید جلوی آن را بگیریم. اگر دستور را به JNZ تغییر دهیم مشاهده می شود که باز هم پرش انجام می شود. راه حل بهتر همان است که در گام ۱۰ بیان کردیم؛ یعنی، مقصد دستور پرش را دستور بعدی قرار دهیم. برای این کار بایستی عملوند دستور را به 00000000 تنظیم کنیم. به این ترتیب ماشین به دستور بعدی پرش می کند. OllyDBG نیز این را به خوبی نشان می دهد. جهت صفر کردن عملوند نیاز به ویرایش کد هگز دستور داریم که با فشردن کلید ترکیبی H + فشردن کلید می شود و در آن عملوند دستور را که ۴ بایت کم ارزش تر است به صفر تغییر می دهیم و تغییرات را AD می کنیم. مشاهده می شود که فلشی که به مقصد دستور پرش اشاره می کند در واقع به دستور اشاره کرده است.

CollyDbg - Apssm.exe - [CPU - main thread, module Apssm]		– a ×
Hie View Debug Plugins Options Window Help	K B B S III 2	_ 6 X
00474DE9 . 83C0 BF ADD EAX,-41	Switch (cases 4153)	∧ Registers (FPU) < < < < < < < <
0047400E 8378 12 (MP EAX,12 004740E5 0067400F5 No87 000000 AA passm.004740F5 00474075 V33C9 XDR ECX,ECX 00474076 SA88 65847000 VC,LBYTE PTR D5:[EAX+4758E8] 00474076 FF2480 06541 3MP PA08D0 PTR D5:[ECX+44758E8] 00474E00 FF2480 06541 3MP PA08D0 PTR D5:[ECX+44758E0] 00474E04 5817 00474E05 572 00474E06 572 00474E07 FF92 0803000C CALL DAMOR PTR D5:[EDX=003] 00474E08 50 00474E04 50	Edit code at 00474DEF ASCII 0 UNICODE	ESP 0019ED8C ESP 0019EF40 ESI 660E6C30 MSVBW60,vbaStrMove > 00770EF ES 0028 32bit 0(FFFFFFF) ES 0028 32bit 0(FFFFFFF) SS 0028 32bit 0(FFFFFFF)
000745E1 S045 A0 LEA EXT, DONDO PTR 55: [EBP-60] 000745E11 S0 PUSH EAX 000745E12 FF15 BS104000 (ALL DWORD PTR 55: [EBP-40] 000745E13 S806 MOV EXT, EAX 000745E14 S805 MOV EXT, EAX 000745E14 S805 MOV EXT, EAX 000745E15 S2 PUSH EAX 000745E16 S2 PUSH EAX 000745E16 S3 PUSH EAX 000745E17 S800 MOV EXT, LAX 000745E18 S3 PUSH EAX 000745E17 S61 A000000 (ALL DWORD PTR D5: [EBX] 000745E21 S63 000000 (ALL DWORD PTR D5: [EAX] 000745E21 S68 0400000 (ALL DWORD PTR D5: [EAX] 000745E21 S68 0400000 (PUST DVST, A00000 PTR D5: [EAX] 000745E21 S68 0400000 (PUST A000000000000000000000000000000000000	HEX-00 100 87 88 88 88 88 88	05 0026 12bit 0 (FFFFFFFF) 65 0028 32bit 2 (SB00(FFF) 65 0028 32bit 0 (FFFFFFF) LastErr ERROR_SUCCESS (00000000) D STO empty 3.93 0.000000000 STO empty 3.93 0.00000000000 STO empty 3.93 0.00000000000 STO empty 3.93 0.000000000000 ST3 empty 2.975 FFFE 0002002 ST3 empty 2.975 FFFE 000000000000 ST3 empty 2.975 FFFE 0000000000000000000000000000000000
00474DF5=Apssm. 00474DF5		3 2 1 0 E 5 P U O Z D I
Address? ASUT: dump 004A800		▲ 0015E508 00015E708 0015E70 0015E509 0075750 0015E50 0075750 0015E504 0000000 0015E50 0007550 0015E504 0000000 0015E50 0007550 0015E504 0000000 0015E50 0015E50 0015E50 0015E504 74221500 USER32.74221580 0015E50 0015E50 0015E504 76025E50 VSESW60.66050314 from ntd11.Ntd1 0015E508 00002650 00000064 ✓

- ۲۱.در آدرس 00474DFD (دقیقا ۴ خط پایین تر از دستور گام ۲۰) یک پرش غیر شرطی JMP مشاهده می شود که مق صد آن در زمان اجرا م شخص می شود و ادرس ثابتی نیست. لذا این احتمال وجود دارد که این پرش کنترل اجرای برنامه را به پیغام خطا هدایت کند و همه کارهایی قبلی ما بی اثر شوند. از آن جایی که روی این دستور از قبل Break Point قرار نداده ایم چرا که اسا سا از وجود آن اطلاع ندا شتیم بهتر است جریان اجرایی برنامه را گام به گام و با فشردن کلید F8 پیگیری کنیم که در هر بار فشردن یک دستور را اجرا می کند. Olly DBG در هر مرحله آدرس دستوری را که کنترل اجرا روی آن متوقف شده است و با فشردن F8 اجرا خواهد شد، به رنگ سیاه نشان می دهد به این ترتیب به راحتی می توان روند اجرای گام به گام برنامه را جلو برد.
- ۱.۲۲ اجرا را گام به گام تا قبل از دستور JMP ادامه می دهیم و برای اطمینان این دستور را با کد هگز ۹۰ که معادل دستور NOP است جایگزین می کنیم. دقت کنید که همان طور که قبلا هم گفتیم تحت هیچ شرایطی آدرس ها نباید تغییر کند. بنابراین چون د ستور قبلی ۷ بایت طول دا شت و هر دستور NOP یک بایت است. این دستور با ۷ دستور NOP جایگزین می شود. در DIly DBG با کلیک راست بر روی دستور و سپس انتخاب گزینه Binary و سرس زیر گزینه Fill With NOPs این فرایند به صورت خودکار انجام می شود. اجرا را با FI ادامه می دهیم.

🔅 کرک نرم افزار Acme Photo ScreenSaver Maker به وسیله OllyDBG

🔆 Oll File	llyDbg - Apssm.exe View Debug Plugins Options Window Help					- ø ×
•		IWHC/KBRS				
d	C CPU - main thread, module Apssm					
	00474DE6 . 0EBEC3 MOVSX EAX.8X				A Pagistars (EDII)	
	00474DE9 . 83C0 BF ADD EAX,-41				EAX EFFECTO	<u> </u>
	00474DEC . 83F8 12 CMP EAX,12				ECX 000000CB	
	00474DEF . 0F87 00000000 JA Apssm.004	74DF5			EDX 00000020	
	00474DF5 > 33C9 XOR ECX,ECX				EBX 00000031	
	00474DF7 . 8A88 E8584700 MOV CL,BYTE	PTR DS:[EAX+4758E8]			ESP 0019ED8C	
	00474DFD 90 NOP				EBP 0019EF40	
	00474DFE 90 NOP				ESI 660E6C30 MSVBVM60vbaStrMove	
	00474DFF 90 NOP				EDI 00757C30	
	00474E00 90 NOP				ETR 004740ED Apccm 004740ED	
	00474E01 90 NOP					
	00474E02 90 NOP				C 0 ES 002B 32bit 0(FFFFFFFF)	
	00474E03 90 NOP				P 1 CS 0023 32bit 0(FFFFFFFF)	
	00474E06 57 PUSH EDT	b The bollebri			A 0 SS 002B 32bit 0(FFFFFFF)	
4	00474E07 . EE92 08030000 CALL DWORD P	TR DS: [FDX+308]			2 1 DS 0028 32011 0(FFFFFFFF)	
10	00474E0D . 50 PUSH EAX				5 0 F5 0053 32D11 228000(FFF)	
64	00474E0E . 8D45 A0 LEA EAX, DWOR	D PTR SS:[EBP-60]				
64	00474E11 . 50 PUSH EAX				0.0 LastErn ERROR SUCCESS (00000000)	
66	00474E12 . FF15 B8104000 CALL DWORD P	TR DS:[<&MSVBVM60vbaObjSe	MSVBVM60vbaObjSet		 Contraction (Contraction) 	
66					EFL 00200246 (NO,NB,E,BE,NS,PE,GE,LE)	
67					STO empty -??? FFFF 00D2D2D2 20E6E6E6	
68	Address ASCII dump		0019ED8C	0019EFAC		^
68	004A8000ı0oÿÿ		0019ED90	00757C30		
68	004A8020(<u.ē¼€ÿ×x.ÿūüüÿ th="" ÿm.āāāÿ<=""><th></th><th>0019ED94</th><th>00000001</th><th></th><th></th></u.ē¼€ÿ×x.ÿūüüÿ>		0019ED94	00000001		
69	004A8040 xN [^a []+^]		0019ED98	000208E0		
69	004A8060`io		0019ED40	00000215		
69	004A8080		00195040	74C215B0 USEP32	74C21580	
60	004480409 ju.ECu. ju.¬jyy		0019EDA8	FFFFFFFF		
60	004480E0 Dit Lt ôt		0019EDAC	FFFFFFE		
	00448100 99		0019EDB0	-0019EE18		
13	00448120 "00.1		0019EDB4	6605D314 RETURN	to MSVBVM60.6605D314 from ntdll.NtdllDefWindowPro	c_A
	004A8140 d		0019EDB8	000208E0		
	004A8160 0ð¥t		0019EDBC	0000084		
	004A8180 I • 0.1 V1		0019EDC0	0000000		
			Loos of DCA	1 01 50022C		

۲۳.در آدرس 00474EAD نیز متوقف می شویم. کلیه اقدامات مشابه گام ۲۰ خواهد بود. بعد از تغییر عملوند دستور با کلید F8 اجرای گام به گام را ادامه می دهیم. ۲۱.مشابه گام ۲۱ دستور JMP را به NOP تبدیل می کنیم. زیرا این دستور دقیقا به محل خطا پرش می کند.

ſ	00474EAA		83F8 12	CMP EAX.12	
	00474EAD		0F87 00000000	JA Apssm.00474EB3	
	00474EB3		33D2	XOR EDX,EDX	
	00474EB5		8A90 04594700	MOV DL, BYTE PTR DS:[EAX+475904]	
	00474EBB	•~	FF2495 FC584700	JMP DWORD PTR DS:[EDX*4+4758FC]	Apssm.0047566A
	00474EC2	>	8B07	MOV EAX, DWORD PTR DS:[EDI]	Cases 41 ('A'),4D ('M'),50 ('P'),53 ('S') of swi
	00474EC4		57	PUSH EDI	
	00474EC5		FF90 08030000	CALL DWORD PTR DS:[EAX+308]	
	00474ECB		8D4D A0	LEA ECX, DWORD PTR SS:[EBP-60]	
	00474ECE		50	PUSH EAX	
	00474ECF		51	PUSH ECX	
	00474ED0	•	FF15 B8104000	CALL DWORD PTR DS:[<&MSVBVM60vbaObjSe	MSVBVM60vbaObjSet
	DC - F00475	000	1 00475664 (Amazam 0	0475.554	

DS:[00475900]=0047566A (Apssm.0047566A)

۲۵.اجرا را با کلید F9 ادامه می دهیم. در آدرس 00475018 متوقف می شویم. پرش انجام نمی شود. پس بدون تغییر با کلید F9 ادامه می دهیم. ۲۶.در آدرس 00475175 متوقف می شویم. این پرش نیز انجام نمی شود. پس بدون تغییر با کلید F9 ادامه می دهیم. ۲۷.در آدرس 0047559E متوقف می شویم که حاوی پیام "Info" است که در گام ۷ روی آن Break Point قرار داده بودیم. اجرا را با F9 ادامه می دهیم. ۲۸. کنترل اجرا روی آدرس 004755E که محتوی پیغام حاصل از صحیح بود اطلاعات وارده توسط ماست یعنی "Thank you for your registration" متوقف می شود.



۲۹. در نتیجه توانستیم کنترل اجرا را با موفقیت به این قسمت از برنامه برسانیم و برای این کار تعداد محدودی دستور را عوض کردیم. حال تغییرات داده شده را ذخیره می کنیم و یک فایل EXE جدید می سازیم که به صورت پیش فرض با مشخصات ما Register شده است. برای این کار در محیط برنامه را ست کلیک کرده، از منوی باز شده گزینه شده است. برای این کار در محیط برنامه را ست کلیک کرده، از منوی باز شده گزینه نیز گزینه Copy to Executable و سـپس All modification را می زنیم. در پنجره ظاهر شـده نیز گزینه Copy all را میزنیم. در پنجره نمایش داده شـده حاوی کد جدید کلیک راست کرده و گزینه Save file را میزنیم و فایل EXE جدید را با یک نام جدید ذخیره می کنیم.

🔆 OllyDbg - Apssm.exe		– 🛛 🗡
File View Debug Plugins Options Window Help	Copy selection to executable file X	
MX MI WY MIT T TEMTWHCZKBRS	Copy selection to executable file?	
CPU - main thread, module Apssm	Copy Copy all Skip Cancel	
E Constraint State State <t< th=""><th>∧ Registers (FPU) Ex. 00000000 Ex. 00000000 ES. 00000000 ES. 00000000 P. 1 CS. 0003 32bit 0(FFFFFFFF) A 0 ES.0003 32bit 200(FFFFFFFF) C 0 LS.0003 32bit 200(FFFFFFFF) J 0 SO 003 32bit 200(FFFFFFFF) J 0 LastErr EBR0_SUCCESS (0000000) EFL 002002000 (WU, WL, NE, A, NS, PE, GE, GC) EFL 00200200 (WU, WL, NE, NS, PF, CE, GC, GC) ST0 empty -777 FFFF 00002020 206666666 EST</th><th>< < <</th></t<>	∧ Registers (FPU) Ex. 00000000 Ex. 00000000 ES. 00000000 ES. 00000000 P. 1 CS. 0003 32bit 0(FFFFFFFF) A 0 ES.0003 32bit 200(FFFFFFFF) C 0 LS.0003 32bit 200(FFFFFFFF) J 0 SO 003 32bit 200(FFFFFFFF) J 0 LastErr EBR0_SUCCESS (0000000) EFL 002002000 (WU, WL, NE, A, NS, PE, GE, GC) EFL 00200200 (WU, WL, NE, NS, PF, CE, GC, GC) ST0 empty -777 FFFF 00002020 206666666 EST	< < <
0 Address AscII dump 0 Address AscII dump 0 0048800		Â
Break print at Annon 004755EE		Paurad



۳۰.به برنامه در حال Debug باز می گردیم. اجرا را با F9 ادامه می دهیم تا پیغام موفقیت که داخل برنامه به آن رسیدیم را بر روی پنجره داخل برنامه نیز مشاهده کنیم و سپس از محیط Olly DBG خارج می شویم.

CollyDbg - Apssm.exe File View Debug Plugin	Acme Photo Screen File(F) Edit(E) Guid	Saver Maker4.50 e(G) Help(H)				- [- • ×
C CPU - main threa 00475519 C78 00475603 FFC 00475605 50	Photos Mu	sic Background Caption	Headline Transition	Lyric Opening	Information Oth		
00475606 8D8 00475606 8D8 00475612 50 00475613 51 00475614 FFE			Maria Acme Photo ScreenSaver	Maker	[[*]	Add Photos	
00475616 . 50 00475617 . FF1 0047561D . 8DS 00475623 . 8DS 00475629 . 52 800475624 . 8DS	Save		Info	Acme Photo Scr Version 4. Produced by Acme Photo	eenSaver Maker 50 Software × er.com		
00 00475630 50 05 00475631 8D2 10 00475637 51 64 00475638 8D8 64 00475638 52	Save		Full Licen	nk you for your registration! program is a full licensed vers	ion now.		
66 0047563F . 8D4 66 0041BB5C=Apssm.C 67 Stack SS:[0019EE 67 Address ASCII c 68 A04ress ASCII c	PLAY		Li Registration Code:	******	ОК	Display Photos in Random Order	
68 004A8020 (<u< td=""> 69 004A8040 xN [°a [] 69 004A8060 69 004A8040 xN [°a [] 69 004A8040 69 004A8040 </u<>	Create	ill Screen Keep Scale 🛛 🗸	Static Photo) Floating Photo#	ОК	Photo Synchronize with Music(10 - 15 sec) Set Photo Interval Time (sec) 10	0
6C 004A80C0 (73 004A80E0 73 004A8100 ÿÿ 004A8120 "0o 004A8140 d	<					>	
004A8160 0ð¥t 004A8180I•c							Burning

🌉 Acme Photo ScreenSaver	Maker	\times
	Acme Photo ScreenSaver Maker Version 4.50 Produced by Acme Photo Software <u>http://www.acme-photo-screensaver-maker.com</u> <u>support@acme-photo-screensaver-maker.com</u> Copyright(C) 2013 Acme Photo Software	
Full Licensed Version		
Licensed to Name: Registration Code:	Morteza	
	ОК	

۳ نتیجه گیری

در این گزارش ما توانستیم یک فایل اجرایی Register شده و معتبر را از فایل ا صلی برنامه بسازیم و می توانیم این فایل را جایگزین فایل ا صلی کنیم (Patching). در نهایت برنامه با موفقیت Crack شد. همان طور که مشاهده کردیم Olly DBG دارای قابلیت های بسیار مناسبی برای Disassembly و Debug برنامه های ۳۲ بیتی می باشد. به کمک این نرم افزار می توان قفل بسیاری از برنامه های کاربردی را شکست و در اصطلاح آن ها را Crack کرد. علاوه بر این می توان برای ا شکال زدایی برنامه های دارای م شکل نیز از این ابزار بهره جست. کلیه فایل ها و ابزار های مورد استفاده در این گزارش پیوست شده است.

۴ منابع و ماخذ