بسمه تعالی

گزارش کامل Sysinternals Suite

فهرست مطالب

معرفی Sysinternals Suite

Sysinternals Suite به صورت یک پک ارائه شده توسط شرکت مایکروسافت است که در آن بیش از ۵۰ نرم افزار یا ابزار برای کارهای مختلف از جمله عیب یابی و رفع مشکلات ویندوز, امنیت, پردازش ,شبکه و اطلاعات سیستم را در اختیار ما قرار می دهد.

استفاده از این نرم افزار به متخصصین و توسعه دهندگان آی تی توصیه می شود که بسیار در زمینه عیب یابی سیستم ها به آن ها کمک خواهد کرد.

در ادامه این گزارش به بررسی تمام ابزارهای موجود در این پک و کاربرد آن ها می پردازیم.

دسته بندی Sysinternals Suite

برای راحتی کار و پی بردن آسان تر به کارایی هر کدام از این ابزار ها و به دلیل تعداد زیاد آن ها ابزارها را در دسته بندی مشخصی قرار می دهیم.

در این گزارش ابزار ها را طبق کاربرد آن ها در شش دسته تقسیم بندی کرده ایم:

دسته اول Sysinternals File and Disk Utilities

ابزار های موجود در این دسته مربوط به مدیریت و عیب یابی فایل ها و دیسک ها می باشد.

دسته دوم Sysinternals Networking Utilities

ابزار های موجود در این دسته مربوط به مدیریت و عیب یابی شبکه می باشد.

دسته سوم Sysinternals Process Utilities

ابزار های موجود در این دسته مربوط به مدیریت و عیب یابی پروسس ها می باشد.

دسته چهارم Sysinternals Security Utilities

ابزار های موجود در این دسته مربوط به مدیریت و عیب یابی امنیتی می باشد.

دسته پنجم Sysinternals System Information Utilities

ابزار های موجود در این دسته مربوط به مدیریت و عیب یابی اطلاعات سیستمی می باشد.

دسته ششم Sysinternals Miscellaneous Utilities

ابزار های موجود در این دسته مربوط به مدیریت عیب یابی موضوعات متفرقه می باشد.

که به صورت کامل تر درباره ی این دسته ها و ابزارهایی که درون آن ها قرار می گیرد در زیر بحث خواهیم کرد.

دسته اول Sysinternals File and Disk Utilities

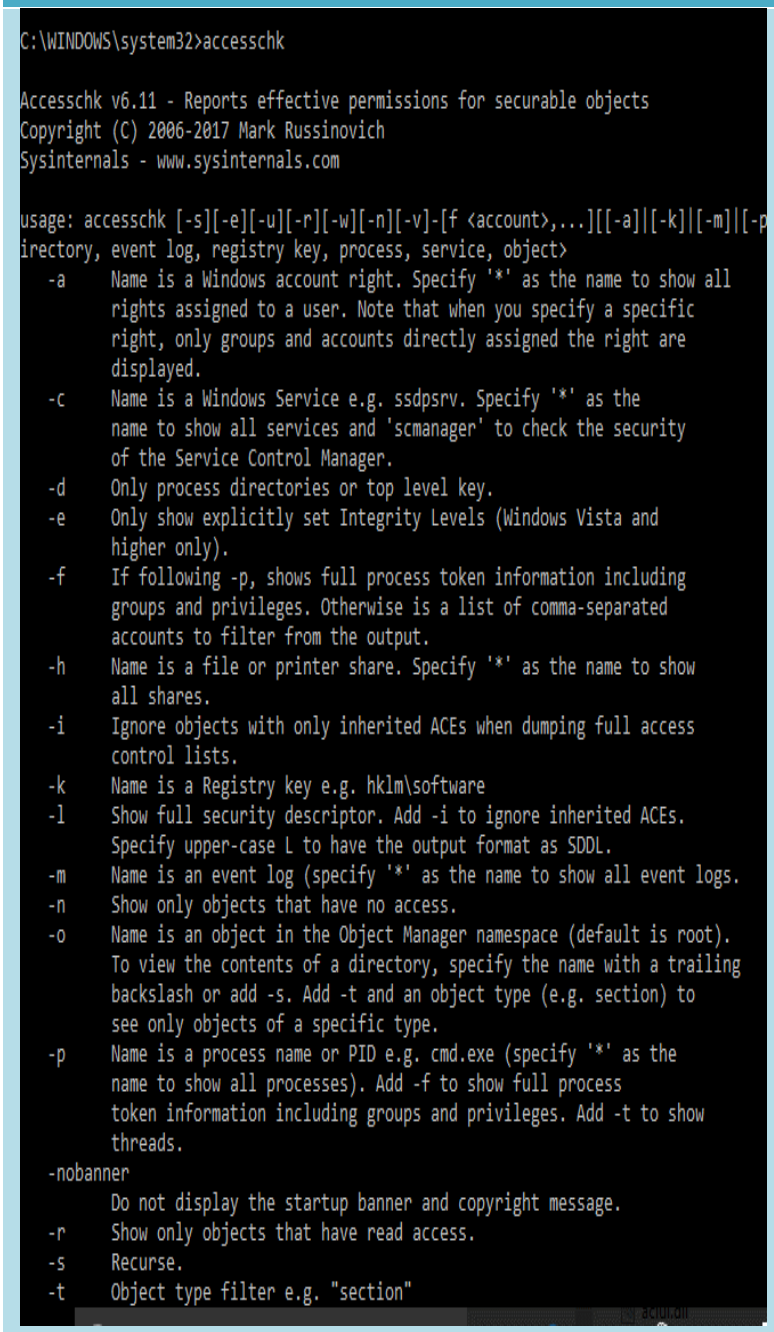
در این دسته حدود ۲۰ ابزار از جمله AccessChk و AccessEnum وCacheSet و Contigو.....وجود دارد که به شرح تک تک آن ها می پردازیم.

معرفی ابزارهای موجود در دسته اول

ابزار AccessChk

ابزار شماره ۱	
نام ابزار	AccessChk
لینک دانلود	https://download.sysinternals.com/files/AccessChk.zip
تاریخ انتشار	September ۱۱, ۲۰۱۷
معرفی این ابزار	این ابزار به شما نشان می دهد که دسترسی به کاربر یا گروهی که مشخص می کنید دارای فایل ها، کلید های رجیستری یا سرویس های ویندوز است. برای اطمینان از اینکه محیط امن ایجاد کرده باشیم، مدیران ویندوز اغلب باید بدانند چه نوع دسترسی کاربران خاص یا گروه ها به منابع از جمله فایل ها، دایرکتوری ها، کلید های رجیستری، اشیاء و ....وجود دارد. اگر شما یک نام کاربری و مسیر را مشخص می کنید این ابزار مجوز های موثر را برای آن حساب گزارش می دهد؛ در غیر این صورت دسترسی موثر برای حساب های اشاره شده در توصیفگر امنیتی نشان داده خواهد شد.
نحوه ی استفاده از ابزار	این ابزار یک برنامه است که به صورت کنسول اجرا می شود. پس از دانلود این ابزار به command prompt در ویندوز می رویم و آدرس جایی را که این نرم افزار وجود دارد زده تا این ابزار اجرا

ابزار شماره ۱	
	شود سپس با تایپ AccessChk و اجرای ابزار دستورات کاربردی آن با توضیح نشان داده می شود. برای مثال ما ابزار AccessChk.exe را در مسیر windows\system۳۲ کپی می کنیم با تایپ آن طبق شکل زیر برنامه اجرا می شود:

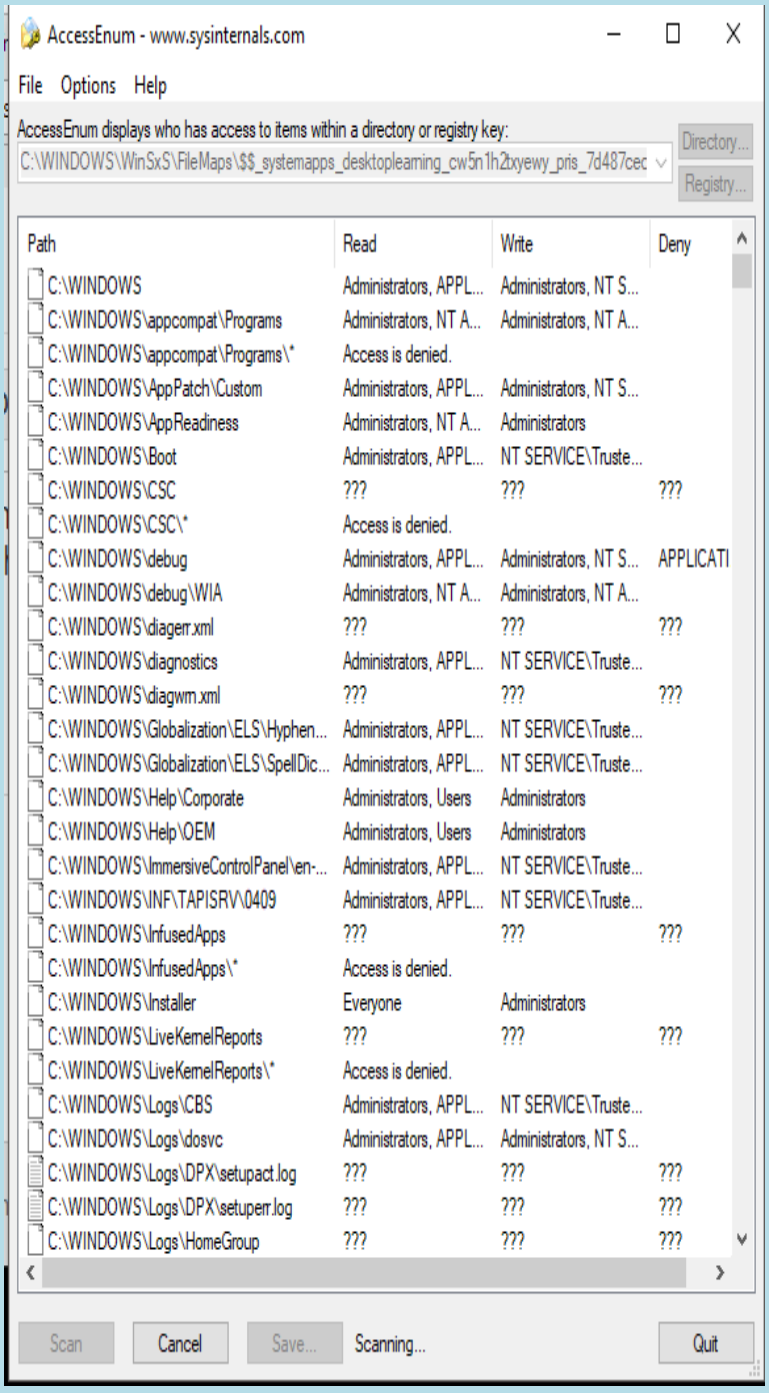
ابزار شماره ۱	
	

```
C:\WINDOWS\system32>accesschk

Accesschk v6.11 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: accesschk [-s][-e][-u][-r][-w][-n][-v]-[f <account>,...][[-a]|[-k]|[-m]|[-p
irectory, event log, registry key, process, service, object>
   -a     Name is a Windows account right. Specify '*' as the name to show all
          rights assigned to a user. Note that when you specify a specific
          right, only groups and accounts directly assigned the right are
          displayed.
   -c     Name is a Windows Service e.g. ssdpsrv. Specify '*' as the
          name to show all services and 'scmanager' to check the security
          of the Service Control Manager.
   -d     Only process directories or top level key.
   -e     Only show explicitly set Integrity Levels (Windows Vista and
          higher only).
   -f     If following -p, shows full process token information including
          groups and privileges. Otherwise is a list of comma-separated
          accounts to filter from the output.
   -h     Name is a file or printer share. Specify '*' as the name to show
          all shares.
   -i     Ignore objects with only inherited ACEs when dumping full access
          control lists.
   -k     Name is a Registry key e.g. hklm\software
   -l     Show full security descriptor. Add -i to ignore inherited ACEs.
          Specify upper-case L to have the output format as SDDL.
   -m     Name is an event log (specify '*' as the name to show all event logs.
   -n     Show only objects that have no access.
   -o     Name is an object in the Object Manager namespace (default is root).
          To view the contents of a directory, specify the name with a trailing
          backslash or add -s. Add -t and an object type (e.g. section) to
          see only objects of a specific type.
   -p     Name is a process name or PID e.g. cmd.exe (specify '*' as the
          name to show all processes). Add -f to show full process
          token information including groups and privileges. Add -t to show
          threads.
   -nobanner
          Do not display the startup banner and copyright message.
   -r     Show only objects that have read access.
   -s     Recurse.
   -t     Object type filter e.g. "section"
```

ابزار AccessEnum

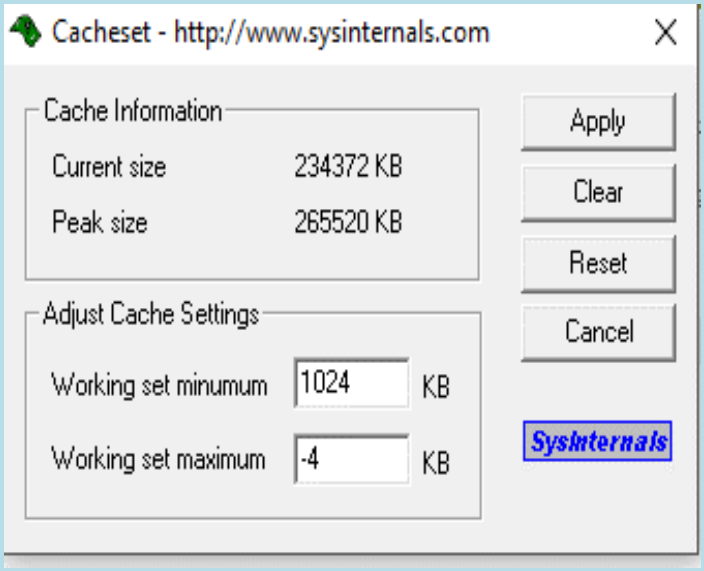
ابزار شماره ۲	
نام ابزار	AccessEnum
لینک دانلود	https://download.sysinternals.com/files/AccessEnum.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	در حالی که مدل امنیتی قابل انعطاف با استفاده از سیستم های مبتنی بر ویندوز NT امکان کنترل کامل امنیت و مجوزهای فایل را فراهم می کند، مدیریت مجوز ها به طوری که کاربران دسترسی مناسب به فایل ها، دایرکتوری ها و کلید های رجیستری را نداشته باشند دشوار می سازد. هیچ راه ورودی برای مشاهده دسترسی کاربر به یک درخت از دایرکتوری ها یا کلید ها وجود ندارد. AccessEnum یک منظره کامل از سیستم فایل و تنظیمات امنیتی رجیستر را در عرض چند ثانیه به شما می دهد و این یک ابزار ایده آل برای کمک به شما برای پی بردن به سوراخ های امنیتی و قفل کردن مجوز ها در صورت لزوم است.
نحوه ی استفاده از ابزار	AccessEnum از API های امنیتی استاندارد Windows استفاده می کند تا فهرست لیست های خود را با خواندن، نوشتن و رد کردن اطلاعات دسترسی به آن ها مورد استفاده قرار دهد. این ابزار را از لینک داده شده دانلود می کنید سپس آن را طبق

ابزار شماره ۲	
	شکل زیر اجرا کرده و دایرکتوری مورد نظر را انتخاب می کنید:



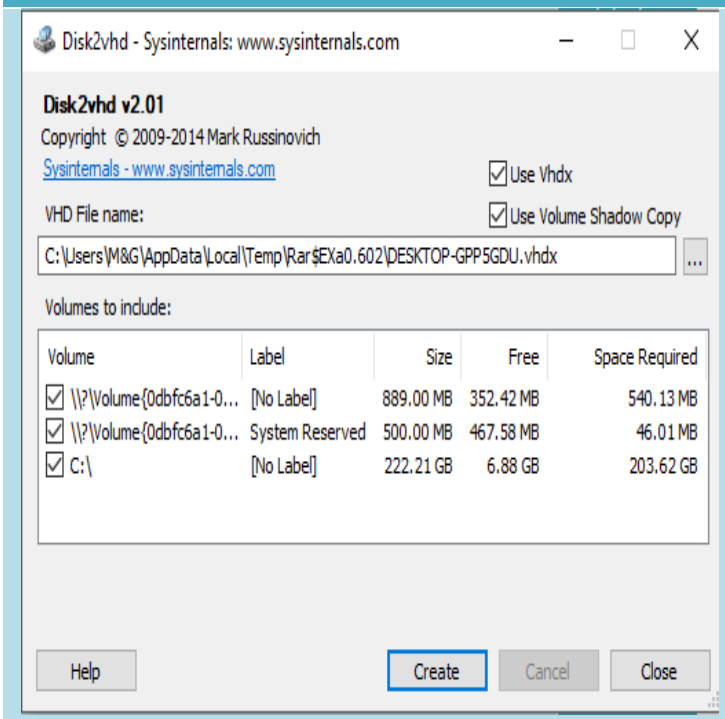
ابزار CacheSet

ابزار شماره ۳	
نام ابزار	CacheSet
لینک دانلود	https://download.sysinternals.com/files/CacheSet.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	CacheSet به شما اجازه می دهد تا پارامترهای کار شده در حافظه فایل سیستم را دستکاری کنید. بر خلافCacheMan ، CacheSetبر روی تمام نسخه های NT اجرا می شود و بدون تغییر در نسخه های جدید Service Pack کار خواهد کرد. علاوه بر اینکه توانایی شما برای کنترل حداقل و حداکثر اندازه مجموعه های کاری را فراهم می کند، همچنین به شما اجازه می دهد تنظیم مجدد کار Cache را انجام دهید و آن را از حداقل نقطه شروع کنید. همچنین بر خلافCacheMan ، تغییرات ساخته شده با CacheSet تاثیر فوری بر اندازه Cache دارند .
نحوه ی استفاده از ابزار	این ابزار بر روی Client: Windows Vista and و Server: Windows Server ۲۰۰۸ و نسخه های بالاتر اجرا می شود. این ابزار را از لینک داده شده دانلود می کنید سپس آن را طبق شکل زیر اجرا کرده و رنج مورد نظر را انتخاب می کنید:

ابزار شماره ۳	
	

ابزار Disk۲vhd

ابزار شماره ۴	
نام ابزار	Disk۲vhd
لینک دانلود	https://download.sysinternals.com/files/Disk۲vhd.zip
تاریخ انتشار	January ۲۱, ۲۰۱۴
معرفی این ابزار	Disk۲vhd یک ابزار است که VHD را ایجاد می کند. (ایجاد هارد دیسک مجازی). برای ایجاد یک هارد مجازی از مایکروسافت Hyper-V که یک مجازی ساز است نیز استفاده می کنیم. تفاوت بین Disk۲vhd و دیگر ابزارهای مبدل هارد فیزیکی به مجازی این است که شما می توانید Disk۲vhd را روی یک سیستم آنلاین فعال کنید.
نحوه ی استفاده از ابزار	این ابزار را از لینک داده شده دانلود می کنید سپس آن را طبق شکل زیر اجرا کرده و دیسک مجازی خود را ایجاد می کنید:

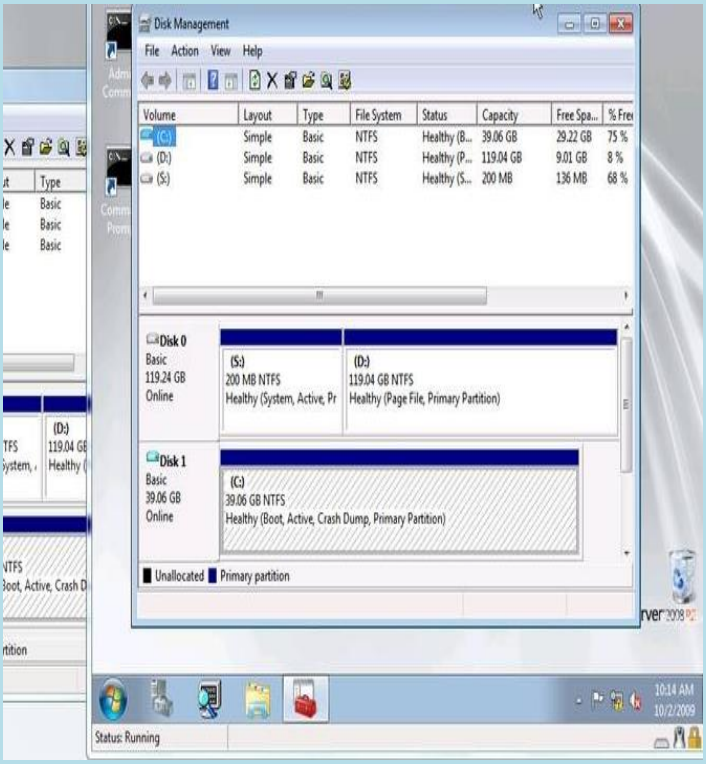
ابزار شماره ۴	
	 این یک VHD برای هر دیسک ایجاد می کند که در آن حجم های انتخاب شده ساکن هستند. این اطلاعات پارتیشن بندی دیسک را حفظ می کند، اما فقط محتویات داده ها را برای حجم بر روی دیسک که انتخاب می شوند، کپی می کند. سص نکته: از PC ها با حداکثر مجاز دیسک مجازی ۱۲۷ گیگابایت پشتیبانی می کند. اگر یک VHD را از یک دیسک بزرگتر ایجاد کنید، از یک VM مجازی PC قابل دسترسی نخواهد بود. نکته:Disk۲vhd از تبدیل حجم دیسک با Bitlocker

ابزار شماره ۴	

پشتیبانی نمی کند. اگر میخواهید یک VHD را برای چنین حجمی ایجاد کنید، Bitlocker را خاموش کنید و منتظر بمانید که حجم برای اولین بار کاملا رمزگشایی شود.

Disk۲vhd در ویندوز ویستا، ویندوز سرور ۲۰۰۸ و بالاتر از جمله سیستم های x۶۴ اجرا می شود.

در اینجا یک تصویر از کپی یک سیستم عامل ویندوز سرور ۲۰۰۸ R۲ Hyper-V در یک ماشین مجازی در بالای سیستم آن ساخته شده است:



استفاده از خط فرمان

Disk۲vhd شامل گزینه های خط فرمان است که شما را قادر

ابزار شماره ۴	
	به ایجاد کردن VHD ها می کند. Example: disk۲vhd * c:\vhd\snapshot.vhd دستور کامل: disk۲vhd <[drive: [drive:]...]|[*]> <vhdfile>

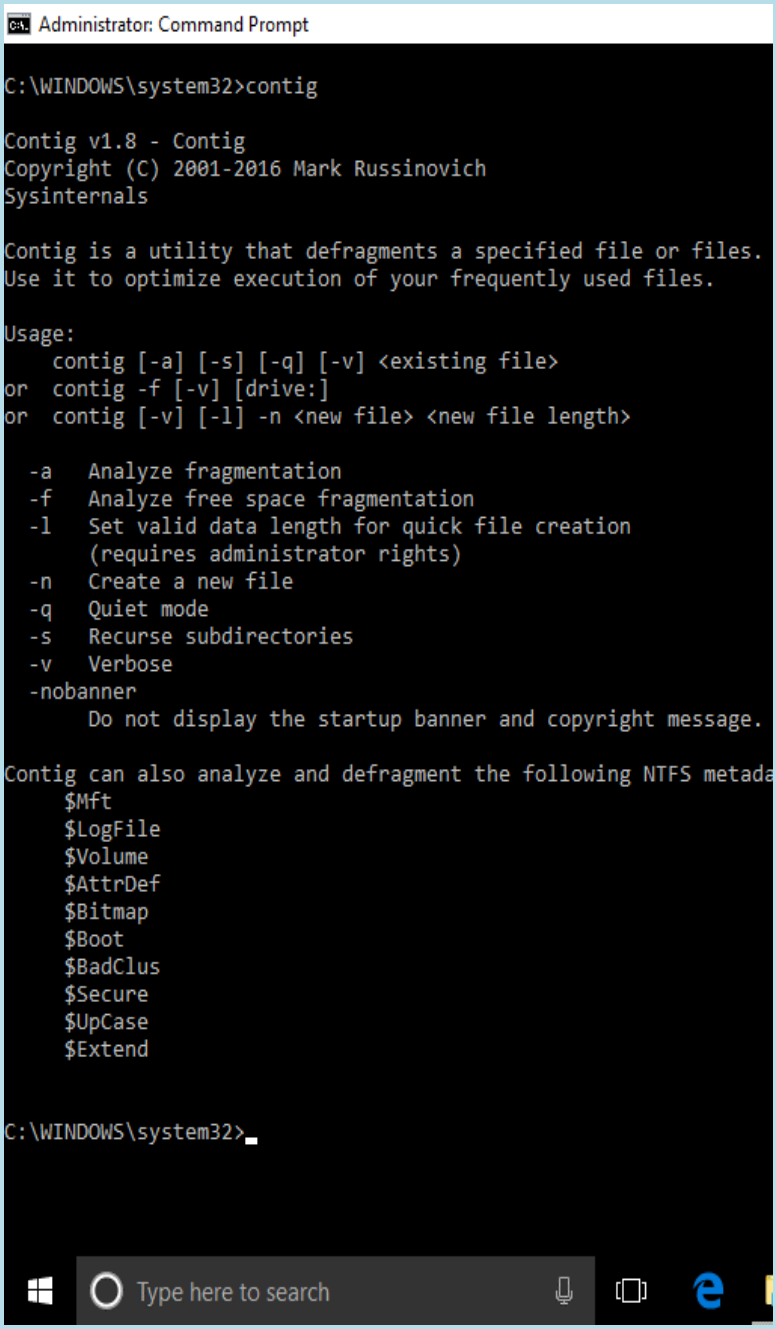
ابزار Contig

ابزار شماره ۵	
نام ابزار	Contig
لینک دانلود	https://download.sysinternals.com/files/Contig.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	Contig برای defragment فایل های شخصی، یا گروه های مشخص شده از فایل طراحی شده و سعی در انتقال فایل ها به ابتدای پارتیشن ندارد. بر خلاف ابزارDefragmenter ساخته شده در

ابزار شماره ۵	
	ویندوز، Contigمی تواند فایل های شخصی، دایرکتوری های فردی و زیر مجموعه های سیستم فایل را با استفاده از علامت نویسی منحصر به فردdefragment کند. استفاده ترکیبی از پارامتر s- و نماد * به کل دایرکتوری ها و درایوها اجازه می دهد defragmented شود: برای مثال contig -s C: \ * همه فایل ها را بر روی هارد دیسکC defrag می کند. پارامترهای "s-"به معنی مرور مجدد دایرکتوری ها هستند. اضافه کردن پارامتر v- دستور را در حالت verbose اجرا می کند. برای مثال: contig -v -s C: \ * هنگامی که سیستم فایل NTFS است، contigهمچنین می تواند فایل های زیر را تجزیه و تحلیل و defragment کند:

ابزار شماره ۵	
	• \$Mft • \$LogFile • \$Volume • \$AttrDef • \$Bitmap • \$Boot • \$BadClus • \$Secure • \$UpCase • \$Extend برای مثال: contig -v -s $ mft یک تغییر کوچک در رجیستری ویندوز اجازه می دهد تمام پوشه ها از ویندوز اکسپلورر پاکسازی شوند. و فایل های فشرده جدید با نام و طول مشخص می توانند ایجاد شوند.
نحوه ی استفاده از ابزار	این ابزار یک برنامه است که به صورت کنسول اجرا می شود. پس از دانلود این ابزار به command prompt در ویندوز می رویم و آدرس مکانی را که این نرم افزار وجود دارد را می نویسیم تا این ابزار اجرا شود سپس با تایپ Conig و اجرای ابزار دستورات کاربردی آن با توضیح نشان داده می شود.

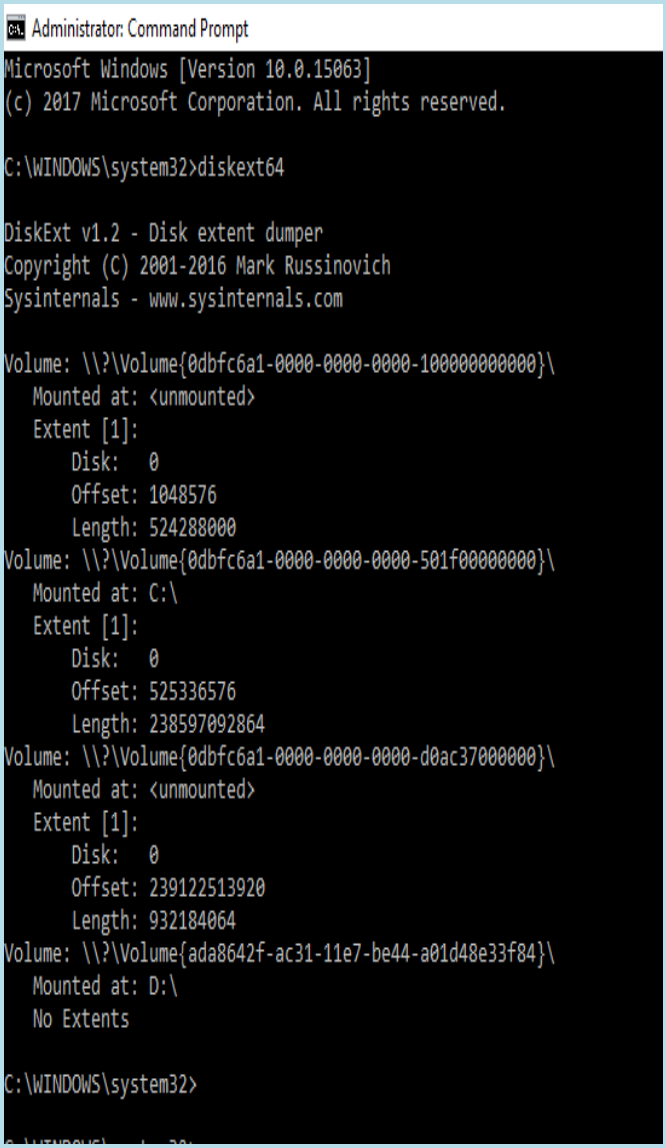
ابزار شماره ۵	
	برای مثـال مـا ابـزار Conig.exe را در مسـیر windows\system۳۲ کپی می کنیم با تایپ آن طبق شکل زیر برنامه اجرا می شود:



ابزار DiskExt

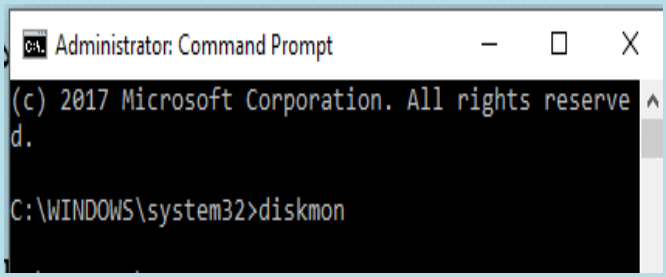
ابزار شماره ۶	
نام ابزار	DiskExt
لینک دانلود	https://download.sysinternals.com/files/DiskExt.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	فرمان IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS اطلاعاتی درباره دیسک هایی که پارتیشن های یک جلد در آن قرار گرفته اند نشان می دهد (دیسک های چند پارتیشن بندی شده می توانند روی چندین دیسک قرار بگیرند) و در جایی که روی دیسک پارتیشن ها قرار دارند.
نحوه ی استفاده از ابزار	این ابزار یک برنامه است که به صورت کنسول اجرا می شود. پس از دانلود این ابزار به command prompt در ویندوز می رویم و آدرس مکانی را که این نرم افزار وجود دارد را می نویسیم تا این ابزار اجرا شود سپس با تایپ DiskExt و اجرای ابزار دستورات کاربردی آن با توضیح نشان داده می شود. برای مثال ما ابزار DiskExt.exe را در مسیر

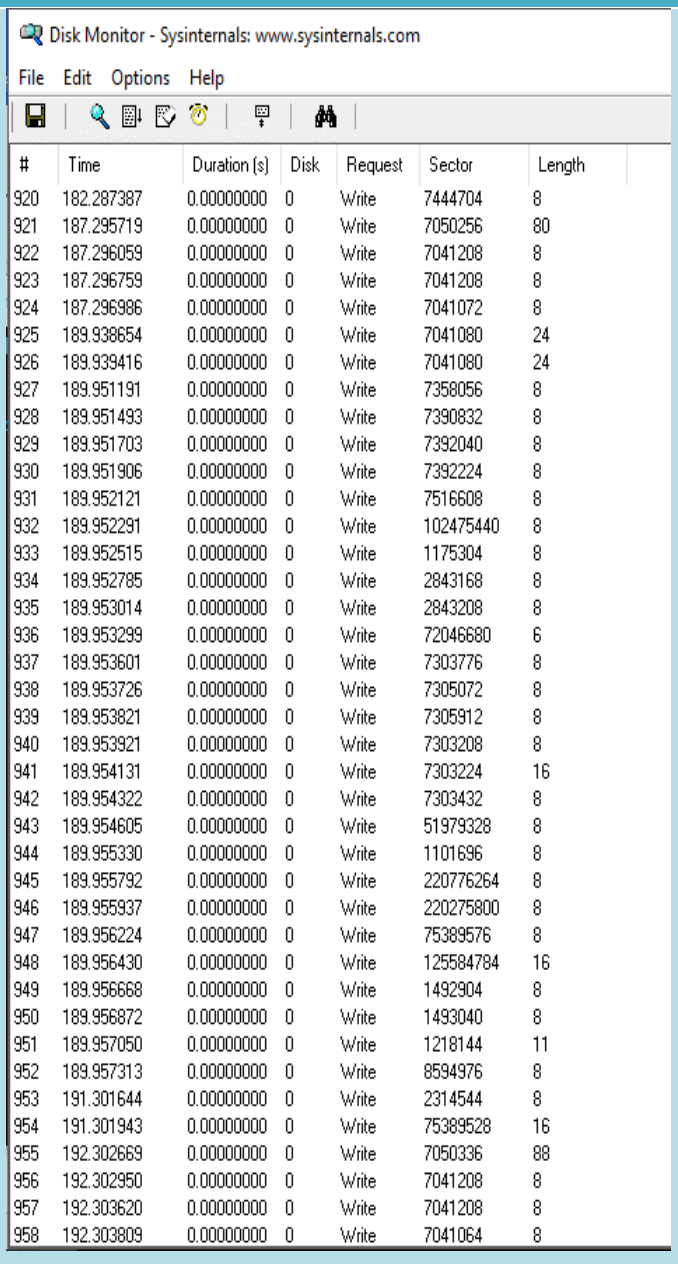
ابزار شماره ۶	
	windows\system۳۲ کپی می کنیم با تایپ آن طبق شکل زیر برنامه اجرا می شود



ابزار DiskMon

ابزار شماره ۷	
نام ابزار	DiskMon
لینک دانلود	https://download.sysinternals.com/files/DiskMon.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	این ابزار تمام فعالیت های دیسک سخت را ضبط می کند و سیستم شما مانند فعالیت دیسک نرم افزار عمل می کند. DiskMon یک برنامه کاربردی است که تمام فعالیت های هارد دیسک را در یک سیستم ویندوز نشان می دهد. ارائه یک نماد سبز در هنگام فعالیت دیسک خوانده شده و یک آیکون قرمز زمانی که فعالیت دیسک نوشتن وجود دارد. DiskMon از kernel event tracing استفاده می کند. event tracing در SDK پلتفرم مایکروسافت مستند شده است و SDK حاوی کد منبع به TraceDmp است، که DiskMon مبتنی بر آن است.
نحوه ی استفاده از ابزار	فایل zip را از لینک گفته شده دانلود می کنید سپس آن را از حالت فشرده خارج کرده آن را درون WINDOWS\system۳۲ بریزید سپس در حالت admin به cmd رفته و کلمه ی

ابزار شماره ۷	
	DiskMon را تایپ می کنیم.سپس برنامه به صورت گرافیکی برای شما اجرا خواهد شد. 

ابزار شماره ۷


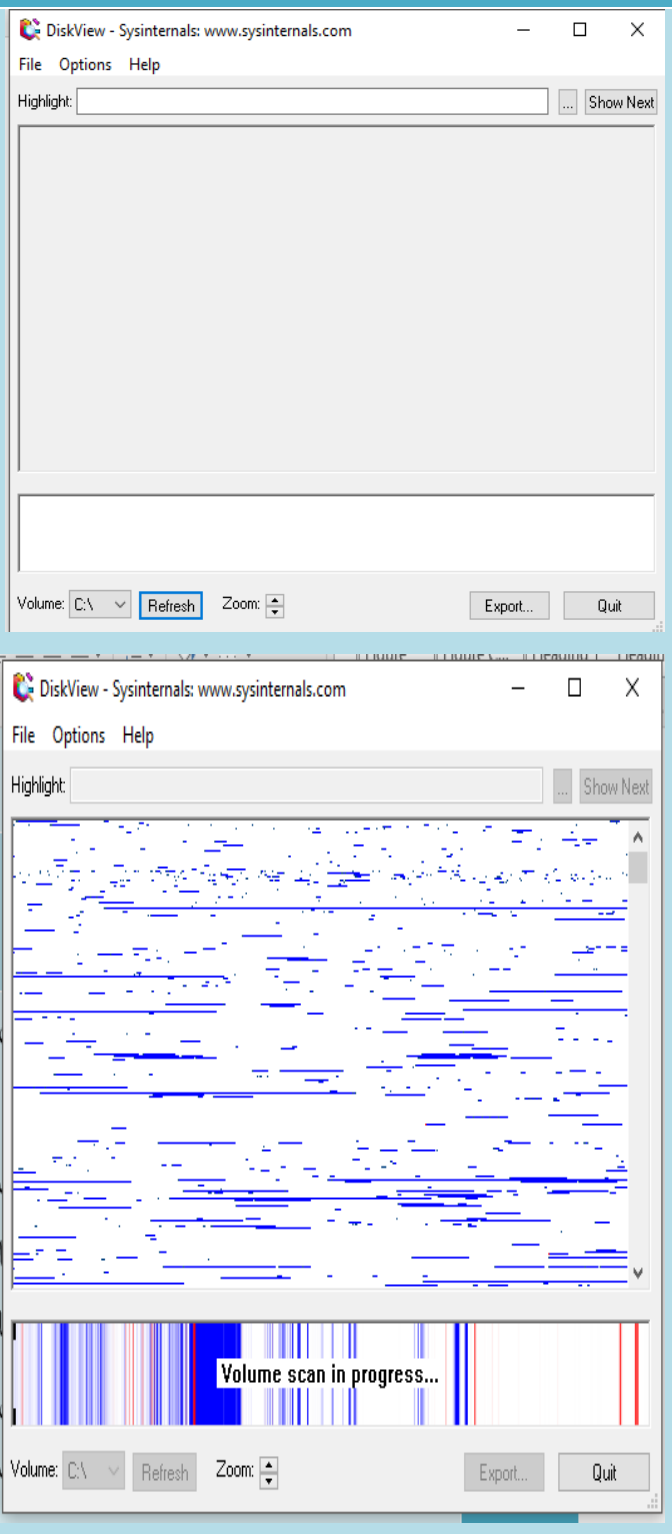
Disk Monitor - Sysinternals: www.sysinternals.com

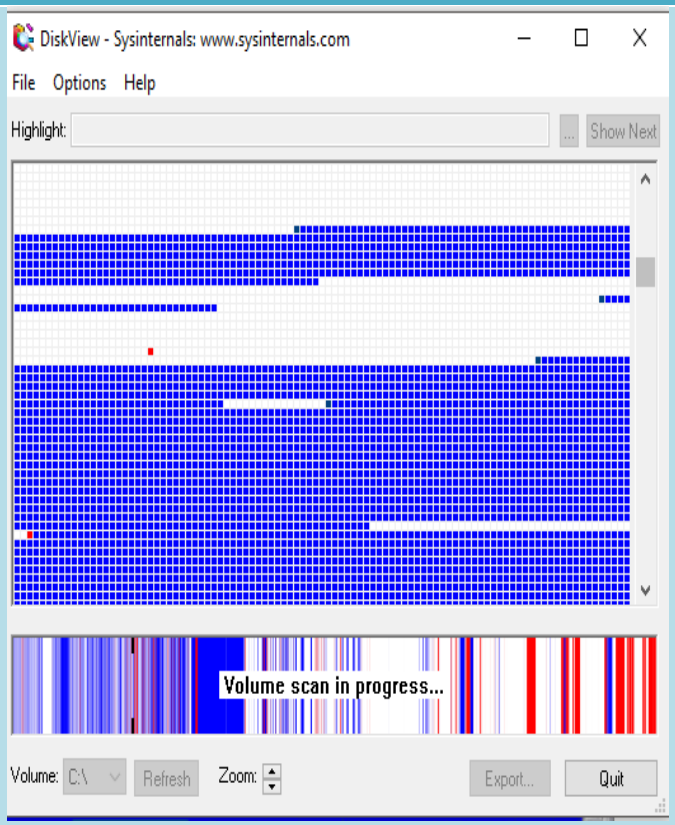
File Edit Options Help

#	Time	Duration (s)	Disk	Request	Sector	Length
920	182.287387	0.00000000	0	Write	7444704	8
921	187.295719	0.00000000	0	Write	7050256	80
922	187.296059	0.00000000	0	Write	7041208	8
923	187.296759	0.00000000	0	Write	7041208	8
924	187.296986	0.00000000	0	Write	7041072	8
925	189.938654	0.00000000	0	Write	7041080	24
926	189.939416	0.00000000	0	Write	7041080	24
927	189.951191	0.00000000	0	Write	7358056	8
928	189.951493	0.00000000	0	Write	7390832	8
929	189.951703	0.00000000	0	Write	7392040	8
930	189.951906	0.00000000	0	Write	7392224	8
931	189.952121	0.00000000	0	Write	7516608	8
932	189.952291	0.00000000	0	Write	102475440	8
933	189.952515	0.00000000	0	Write	1175304	8
934	189.952785	0.00000000	0	Write	2843168	8
935	189.953014	0.00000000	0	Write	2843208	8
936	189.953299	0.00000000	0	Write	72046680	6
937	189.953601	0.00000000	0	Write	7303776	8
938	189.953726	0.00000000	0	Write	7305072	8
939	189.953821	0.00000000	0	Write	7305912	8
940	189.953921	0.00000000	0	Write	7303208	8
941	189.954131	0.00000000	0	Write	7303224	16
942	189.954322	0.00000000	0	Write	7303432	8
943	189.954605	0.00000000	0	Write	51979328	8
944	189.955330	0.00000000	0	Write	1101696	8
945	189.955792	0.00000000	0	Write	220776264	8
946	189.955937	0.00000000	0	Write	220275800	8
947	189.956224	0.00000000	0	Write	75389576	8
948	189.956430	0.00000000	0	Write	125584784	16
949	189.956668	0.00000000	0	Write	1492904	8
950	189.956872	0.00000000	0	Write	1493040	8
951	189.957050	0.00000000	0	Write	1218144	11
952	189.957313	0.00000000	0	Write	8594976	8
953	191.301644	0.00000000	0	Write	2314544	8
954	191.301943	0.00000000	0	Write	75389528	16
955	192.302669	0.00000000	0	Write	7050336	88
956	192.302950	0.00000000	0	Write	7041208	8
957	192.303620	0.00000000	0	Write	7041208	8
958	192.303809	0.00000000	0	Write	7041064	8

ابزار DiskView

ابزار شماره ۸	
نام ابزار	DiskView
لینک دانلود	https://download.sysinternals.com/files/DiskView.zip
تاریخ انتشار	March ۲۵, ۲۰۱۰
معرفی این ابزار	ابزاری گرافیکی برای نشان دادن سکتورهای دیسک. DiskView یک نقشه گرافیکی از دیسک شما را نشان می دهد، به شما این امکان را می دهد که محل فایل را تعیین کنید یا با کلیک روی یک خوشه، ببینید کدام فایل آن را اشغال می کند. برای دریافت اطلاعات بیشتر در مورد یک فایل که یک خوشه اختصاص داده شده است، دوبار کلیک کنید.
نحوه ی استفاده از ابزار	این ابزار را از لینک داده شده دانلود می کنید سپس آن را طبق شکل زیر اجرا کرده و دیسک خود را اسکن می کنیم: وقتی برنامه اجرا شد طبق شکل صفحه ی گرافیکی به شما نشان داده می شود.دیسک خود را انتخاب کرده و دکمه ی refresh را می زنیم.

ابزار شماره ۸	
	

ابزار شماره ۸	
	

ابزار Disk Usage

ابزار شماره ۹	
نام ابزار	Disk Usage
لینک دانلود	https://download.sysinternals.com/files/DU.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	مشاهده disk usage توسط دایرکتوری.

ابزار شماره ۹	
	disk usage گزارش استفاده از فضای دیسک برای دایرکتوری که شما مشخص می کنید را می دهد. به طور پیش فرض، دایرکتوری ها را مجددا نمایش می دهد تا حجم کل یک دایرکتوری و زیر شاخه های آن را نشان دهد.
نحوه ی استفاده از ابزار	به شرح دستورات موجود در این ابزار و کارایی آن ها می پردازیم. قاعده ی نوشتاری دستور ها به صورت زیر است: du [-c[t]] [-l <levels> | -n | -v] [-u] [-q] <directory> پارمتر c- : خروجی به صورت CSV است از ct- برای تعریف تب استفاده کنید. پارمتر l- : مشخص کردن عمق اطلاعات زیر شاخه (به طور پیش فرض تمام سطوح است). پارمتر n- : بازگشت نکنید. پارمتر v- : نمایش اندازه دایرکتوری های متوسط با واحد کیلوبایت. پارمتر u- : تعداد هر نمونه از یک فایل hardlinked .

ابزار شماره ۹	
	پارمتر q- : Quiet (no banner) فرمت خروجی CSV به صورت های زیر است: Path, CurrentFileCount, CurrentFileSize, FileCount, DirectoryCount, DirectorySize

ابزار EFSDump

ابزار شماره ۱۰	
نام ابزار	EfsDump
لینک دانلود	https://download.sysinternals.com/files/EFSDump.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	نمایش اطلاعات فایل های رمز نگاری شده باتوجه به معرفی سیستم های رمزنگاری فایل توسط ویندوز ۲۰۰۰ ، کاربران قادرند از داده های حساس خود محافظت کنند. چندین API جدیدبرای اولین بار از این امکان پشتیبانی میکنند که شامل یک کاربر پرس و جوی فایل رمز نگاری شده

ابزار شماره ۱۰	
	اند . این API ها به شما اجازه ی مشاهده ی کاربران مجاز جهت دستیابی به فایل های رمزنگاری شده را میدهند. این applet از API برای نشان دادن اینکه کدام حساب کاربری برای دسترسی به فایل های رمز نگاری شده مجاز است، استفاده میکند.
نحوه ی استفاده از ابزار	جهت استفاده از EfsDump از پارامتر s– جهت بازسازی زیرشاخه ها استفاده میشود.برای این ابزار در سمت client نیاز به نصب ویندوز vista یا بالاتر و در سمت سرور نیاز به نصب windows server ۲۰۰۸ یا بالاتر خواهید داشت.

ابزار Junction

ابزار شماره ۱۱	
نام ابزار	junction
لینک دانلود	https://download.sysinternals.com/files/Junction.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	ویندوز۲۰۰۰ ونسخه های بالاتر از لینک نمادین پشتیبانی میکنند که در آن یک دایرکتوری به عنوان یک لینک نمادین

ابزار شماره ۱۱	
	به دایرکتوری دیگر در کامپیوتر به ارجاع میشود. به عنوان مثال دایرکتوری D:\SYMLINKرا به عنوان هدف مشخص کنیم، یک برنامه دسترسی به D: \ SYMLINK \ DRIVERS میتواند به C: \ WINNT \ SYSTEM۳۲ \ DRIVERS دسترسی داشته باشد. لینک های نمادین دایرکتوری به عنوان اتصالات NTFS ویندوز شناخته میشوند. متاسفانه، ویندوز هیچ ابزاری برای ایجاد اتصالات ندارد پس شما مجبور خواهید بود،کیت منابع Win۲Kرا تهیه کنید که همراه با برنامه لینک شده برای ایجاد اتصالات وجود دارد. اتصال (junction) نه تنها اجازه ی ایجاد اتصالات NTFS را میدهد بلکه اجازه می دهد که نقاط اصلاح شده فایل ها یا دایرکتوری ها را ببینید. نقاط اصلاح شده درواقع مکانیسمی است که در آن اتصالات NTFS مستقر هستند و توسط سرویس ذخیره سازی از راه دور (RSS) ویندوز و همچنین نقاط پایه مورد استفاده قرارمیگیرد. نکته: ویندوز از اتصالات به دایرکتوری ها در اشتراک های راه دور پشتیبانی نمی کند.
نحوه ی استفاده از ابزار	طریقه استفاده:

ابزار شماره ۱۱	
	[-s] پارامتر s- : بازسازی زیرشاخه ها یک نمونه: برای تعیین اینکه آیا فایل یک اتصال است، نام فایل را مشخص کنید: junction c:\test لیست اتصالات زیر یک دایرکتوری که شامل سوئیچ s- است. junction -s c:\ برای ایجاد یک اتصال c: \ Program-Files برای " c: \ Program Files"دستورات زیر را وارد نمایید. C:\>md Program-Files C:\>junction c:\Program-Files "c:\Program Files" برای حذف اتصالات از دستور d– استفاده کنید junction -d c:\Program-Files

ابزار شماره ۱۱	

ابزار LDMDump

ابزار شماره ۱۲	
نام ابزار	LDMDump
لینک دانلود	https://download.sysinternals.com/files/LdmDump.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	دامپ نمودن (تخلیه) محتویات دیسک منطقی مدیریت پایگاه داده بـر روی دیسـک دیگـر ویـنـدوز ۲۰۰۰ نـوع جدیـدی از پارتیشن بندی دیسک را ارائه میدهد،که توسط جزء ای به نام مدیریت منطقی دیسک مدیریت می شود. دیسک های پایه استاندارد، جداول پارتیشنDos را اجـرا مـی کنند، در حالی که دیسک های پویا ازپارتیشن بندی LDM یا مدیریت منطقی دیسک استفاده میکنند.پارتیشن بندی LDM چندین مزیت در مقایسه با نسـخه هـای DOS دارد،از جملـه تکـرار در میـان دیسـک هـا، ذخیـره سـازی روی دیسـک از پیکربندی حجم پیشرفته (حجم اسپانیایی، حجم آینه، حجـم راه راه و حجم RAID-۵) ارائه می دهـد. بـه غیـر از مـدیریت دیسک MMC-snapin وابزاری بـه نـام dmdiag درkit منبـع

ابزار شماره ۱۲	
	ویندوز ۲۰۰۰، هیچ ابزار دیگری برای بررسی داخلی پایگاه داده LDM روی دیسک وجود ندارد که طرح بندی پارتیشن بندی سیستم را توصیف می کند. LDMDump ابزاری است که به شما اجازه می دهد تا دقیقا همان چیزی را که در کپی دیسک پایگاه داده LDM ذخیره شده است، بررسی نمایید. LDMDump محتویات هدر اختصاصی پایگاه داده LDM ، جدول محتویات و پایگاه داده شی (که در آن تعاریف پارتیشن، اجزا و حجم ذخیره می شود را نشان می دهد و سپس نتیجه آن را با جدول پارتیشن و لیست حجم خلاصه می کند.
نحوه ی استفاده از ابزار	جهت استفاده از LDMDump به سادگی میتوان آن را به شناسه یک دیسک منتقل کرد. به شرح دستورات موجود در این ابزار و کارایی آن ها می پردازیم. قاعده ی نوشتاری دستور ها به صورت زیر است: ldmdump [-] [-d#] پارامتر - : گزینه های پشتیبانی شده و واحد اندازه گیری مورد استفاده

ابزار شماره ۱۲	
	برای مقادیر خروجی را نمایش می دهد. پارامتر -d#: شماره دیسک را برای بررسی توسط LDMDump مشخص میکند. به عنوان نمونه: "ldmdump /d۰" این دستور نشان دهنده ی آن است که اطلاعات پایگاه داده LDM بر روی دیسک ۰ ذخیره شده است. API ای برای دسترسی به اطلاعات دقیق در مورد پارتیشن LDM دیسک ، موجود نیست و فرمت پایگاه داده LDM کاملا غیرقانونی است. LDMDump بر اساس مطالعه محتویات پایگاه داده LDM در انواع سیستم های مختلف و همچنین در شرایط تغییر یافته توسعه داده شد.

ابزار MoveFile

ابزار شماره ۱۳	
نام ابزار	MoveFile
لینک دانلود	https://download.sysinternals.com/files/PendMoves.zip

ابزار شماره ۱۳	
تاریخ انتشار	July ۴,۲۰۱۶
معرفی این ابزار	فراهم نمودن امکان جا به جایی زمانبندی و حذف دستورات در راه اندازی مجدد سیستم چندین برنامه کاربردی مانند service packs و hotfixes وجود دارد که توانایی جایگزینی فایل درحال استفاده را ندارند. همانطور که می دانیم، زمان هایی وجود دارد که ما نیاز داریم فایل هایی را منتقل کرده ویا اقدام به حذف فایل هایی از قبیل (بدافزار / بوت / ویروس ها)نماییم. گاهی اوقات این کار قابل انجام نیست، زیرا فایل ها در حال استفاده هستند، که دراین صورت مانع از فعالیت در فایل ها تا زمانی که بسته شوند ویا کامپیوتر راه اندازی مجدد شود،خواهند شد. MoveFile یک API را جهت انتقال / تغییر نام و یا حذف فایلها در هنگام restart ویندوز سیستم فراهم می کند. انجام این کار به فایل اجازه میدهد که این عملیات بار دیگر قبل از ارجاع فایل ها توسط سیستم انجام شود. این اپلت محتویات درحال تغییر نام و یا حذف را لغو میکند وهمچنین خطایی را نیز در هنگام ایجاد فایل منبع غیر قابل دسترسی گزارش می کند.
نحوه ی استفاده از ابزار	نمونه ای از خروجی که نشان می دهد فایل نصب موقتی برای حذف در هنگام راه اندازی مجدد سیستم برنامه ریزی شده

ابزار شماره ۱۳	

است:

```
Shell

C:\\>pendmoves
PendMove v1.2
Copyright (C) 2013 Mark Russinovich
Sysinternals - www.sysinternals.com

Source: C:\\Config.Msi\\3ec7bbbf.rbf
Target: DELETE
```

نحوه نوشتن دستورات :

movefile [source] [dest]

اگر درکد بالا آدرس مقصد خالی ("") قرداده شود،منبع درهنگام بوت حذف میشود. مثالی که در آن test.exe را حذف می شود:

```
Shell

movefile test.exe ""
```

ابزار FindLinks

ابزار شماره ۱۴	
نام ابزار	FindLinks
لینک دانلود	https://download.sysinternals.com/files/FindLinks.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	FindLinks فایل index و هر لینک سخت (مسیر فایل های متناوب در همان حجم) را که برای فایل مشخص شده وجود دارد را گزارش می دهد. داده های فایل اختصاص داده شده تا زمانی باقی می ماند که در آن حداقل به یک نام فایل اشاره شده باشد.
نحوه ی استفاده از ابزار	طریقه استفاده: findlinks <filename> دستور زیرمسیر فایلی را که به داده های همان فایل ارجاع داده

ابزار شماره ۱۴	
	شده، گزارش میدهد. C:\Windows\Notepad.exe: **C:\>findlinks c:\windows\notepad.exe Shell Copy FindLinks - Locate file hard links Copyright (C) 2011 Mark Russinovich Sysinternals -www.sysinternals.com c:\\windows\\notepad.exe Index: 0x000057D9 Links: 3** Linking files: C:\Windows\winsxs\amd64_microsoft-windows-notepadwin_31bf3856ad364e35_6.1.7600.16385_none_9 C:\Windows\winsxs\amd64_microsoft-windows-notepad_31bf3856ad364e35_6.1.7600.16385_none_cb0f C:\Windows\System32\notepad.exe

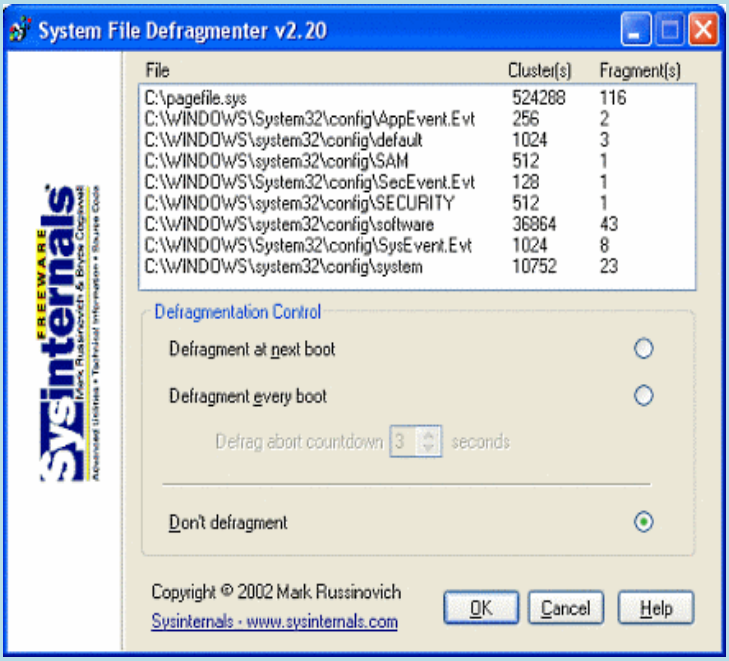
ابزار NTFSInfo

ابزار شماره ۱۵	
نام ابزار	NTFSInfo
لینک دانلود	https://download.sysinternals.com/files/NTFSInfo.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	به کارگیری NTFSInfo برای دیدن جزئیات اطلاعات در مورد حجم NTFS شامل سایز، محل Master File Table (MFT) و MFT-zone به عنوان سایز NTFS-file metadata

ابزار شماره ۱۵	
	سیستم فایل با فناوری نو NTFS استاندارد فایل سیستم‌های موجود در خانواده ویندوزهای NT است که از جمله آنها می‌توان به ویندوزهای ۲۰۰۰، XP و ۲۰۰۳ اشاره نمود. NTFSInfo یک اپلت کوچک است که اطلاعاتی در مورد حجم NTFS نشان می دهد. تخلیه آن شامل اندازه واحدهای تخصیص درایو، که در آن فایل های NTFS کلیدی قرار دارند، و اندازه فایل های متادیت NTFS است.
نحوه ی استفاده از ابزار	NTFSInfo در تمام نسخه های NTFS کار می کند، اما NTFS برای ویندوز ۵.۰ NT دارای فایل های متا داده های مختلف است که تا کنون برنامه نویسی نشده است. برای اینکه NTFSInfo برای کار شما باید دارای امتیاز اداری باشید طریقه نوشتن: NTFSInfo x پارامتر X : حجم NTFS که می خواهید بررسی کنید.

ابزار PageDefrag

ابزار شماره ۱۶	
نام ابزار	pageDefrag
لینک دانلود	https://download.sysinternals.com/files/PageDefrag.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	یکپارچه سازی فایل های صفحه بندی وRegistry hives این ابزار به عنوان یک راه حل برای بهبود عملکرد کلی سیستم در هنگام اجرای کارهای خرابکارانه در فایل های سیستم و رجیستری درنسخه های قدیمی تر ویندوز طراحی شده است. PageDefrag با استفاده از تکنیک های پیشرفته ای که ارائه می دهد بیان میکنند که کدام یک از defragmenters های تجاری توانایی برای دیدن فایل های پیجینگ و رجیستری خود ندارند. PageDefrag محتوای فایل های رجیستری را نابود نمی کند، بلکه فقط این فایل ها را در هارد دیسک قرار میدهد. سایر خدمات مانند NTREGOPT می تواند فایل های رجیستری را بهینه سازی کند. پس از شروع، یک رابط ساده لیستی را با فایل های سیستم شناسایی می کند. ورودی ها اطلاعاتی نظیر تعداد واحدهای تخصیص یافته شده و تعداد قطعات موجود می باشد. در بخش پایین پنجره برنامه، گزینه ای برای شروع روش نابودی وجود دارد. از آنجایی که این نوع از اطلاعات به منظور عملکرد

ابزار شماره ۱۶	
	مناسب مورد نیاز سیستم است، پردازش آنها می تواند زمانی انجام شود که ویندوز آفلاین باشد.
نحوه ی استفاده از ابزار	هنگام اجرای PageDefrag (pagedfrg.exe) یک لیست backup ارائه می شود که به شما می گوید که چه گروه هایی از فایل های پیجینگ شما، پرونده های ثبت وقایع و پرونده های رجیستری (SAM، SYSTEM، SYSTEM.ALT، SECURITY، SOFTWARE، DEFAULT.) را شامل میشود وچندفایل ضمیمه وجود دارد.  طریقه استفاده از ابزار: pagedfrg [-e | -o | -n] [-t <seconds>]

ابزار شماره ۱۶	
	پارامتر e - : Defrag هر بوت. پارامتر o– : یکبار Defrag پارامتر n–: هیچگاه Defrag را انجام نده پارامتر t– : شمارش معکوس را به تعداد مشخصی از ثانیه تنظیم میکند.

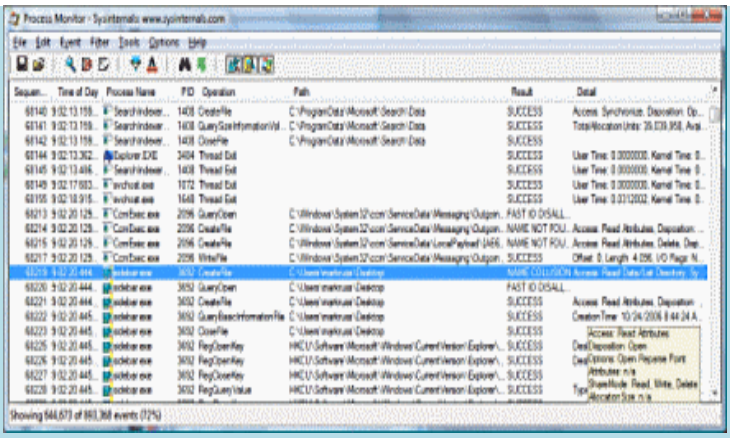
ابزار Process Monitor

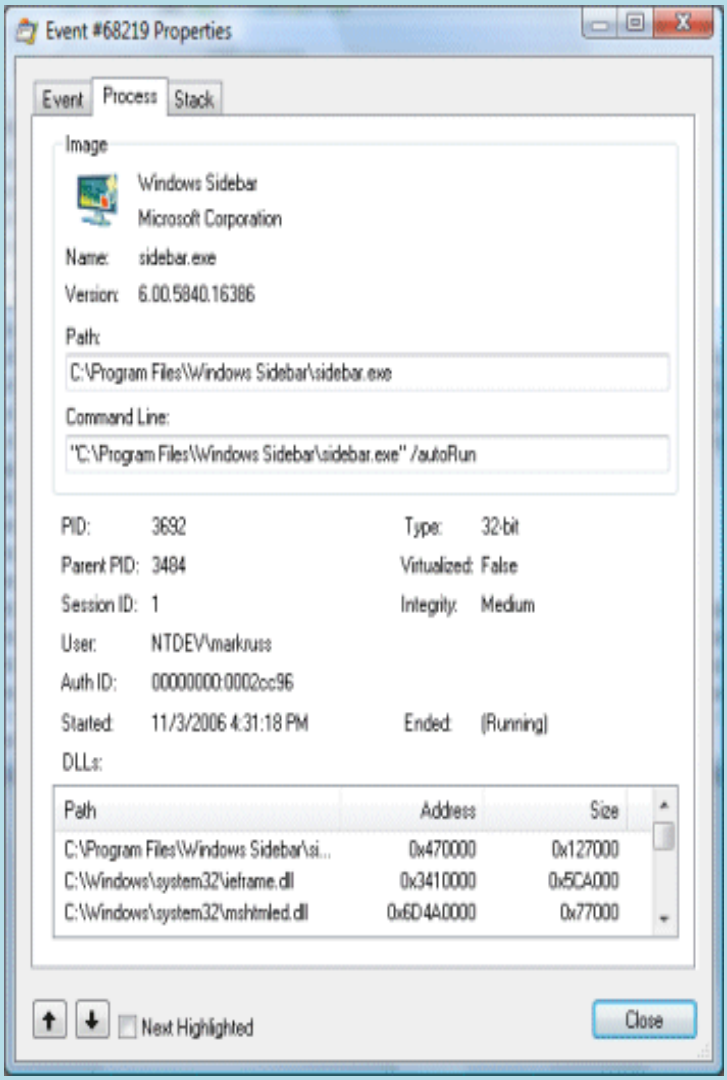
ابزار شماره ۱۷	

نام ابزار	ProcessMonitor
لینک دانلود	https://download.sysinternals.com/files/ ProcessMonitor.zip
تاریخ انتشار	September ۱۲, ۲۰۱۷
معرفی این ابزار	نظارت بـر فایـل سیسـتم، رجیسـتری، رونـد، موضـوع و فعالیـت های DLLدر زمان واقعی این ابزار به طور همزمان تمـام فعالیـت های سیستم فایل را در سیستم عامل ویندوز مایکروسافت نظارت و نمـایش مـی دهـد. دو ابـزار قـدیمی، FileMon و RegMon را ترکیب می کند و در سیستم مدیریت، کامپیوتر قـانونی و اشـکال زدایی نرم افزار مورد استفاده قرار می گیرد. Process Monitorابزاریست جهت مانیتور و ثبت تمـام اقـدامات علیه رجیستری ویندوز مایکروسافت میباشد. مانیتور فرایند بـرای شناسایی تلاش های شکست خورده ویا بـرای خوانـدن و نوشـتن کلید های رجیستری مورد استفاده قرارمیگیرد.. همچنـین اجـازه ی فیلتر کردن بر روی کلیـدهای خـاص، پـردازش هـا، پـردازش شناسه ها، و ارزش ها را میدهد. علاوه بر این نشان می دهـد کـه چگونه برنامه ها از فایل ها و DLL ها استفاده می کنند و برخـی از خطاهـای بحرانـی در فایـل هـای سیسـتم و مـوارد دیگـر را تشخیص می دهد. مانیتور فرایند شامل قابلیت های قدرتمند نظارت و فیلتـر کـردن است، از جمله: داده های بیشتری برای پارامترهـای ورودی و خروجـی عملیـات

	درنظرگرفته شده است فیلترهای غیر مخرب به شما این امکان را می دهند که بدون دانستن اطلاعات، فیلتر کنید درنظرگرفتن نخ برای هر عملیات در بسیاری از موارد امکان شناسایی علت اصلی عملیات را میسر می سازد. گرفتن اطلاعات قابل اطمینان از جزئیات روند، از جمله مسیر تصویر، خط فرمان، کاربر و شناسه جلسه معماری پیشرفته ورود به سیستم برای ده ها میلیون حوادث رخ داده و ده ها میلیون گیگابایت داده های ورود داده می شود. ابزار درخت فرایند، رابطه بین تمامی فرآیندهای اشاره شده در ردیابی را نشان می دهد فرمت ورودی بومی تمام داده ها را برای بارگیری در یک Instance Process Monitor متفاوت نگه می دارد نمایشOpen File –امکان دریافت نرم افزار به صورتPortable –کاملا رایگان –نمایش میزان استفاده هر نرم افزار از cpu و...

نحوه ی استفاده از ابزار





ابزار PsFile

ابزار شماره ۱۸	
نام ابزار	PsFile
لینک دانلود	https://docs.microsoft.com/en-us/sysinternals/downloads/psfile
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	نمایش فایل هایی که به صورت remote باز شده اند فرمان " net file" لیستی از فایل هایی که سایر رایانه ها در سیستم باز کـرده اند بر اساس دستور شما اجرا می کند، با این حال نام های مسـیر طولانی را قطع می کند و اجازه نمـی دهـد کـه ایـن اطلاعـات را برای سیستم های از راه دور مشاهده کنید. PsFile یک ابزار خط فرمان است که لیستی از فایل های موجود در یک سیستم را کـه از راه دور باز می شود نشان می دهد و همچنین به شما اجازه می دهد تا بسته های باز شده را با نام یا شناسه فایل بسته کنید.
نحوه ی استفاده از ابزار	طریقه نصب: PsFile را بر روی مسیر اجرایی خـود کپـی کنیـد و "psfile" را تایپ کنید. رفتار پیش فرض PsFile اینگونه است که لیسـت فایـل هـای سیستم محلی را کـه توسـط سیسـتم هـای راه دور بـاز هسـتند،

ابزار شماره ۱۸	
	لیست میکند. با تایپ یک فرمان به دنبال "-" اطلاعات مربوط به نحو دستور نمایش داده میشود. قواعد نوشتاری: psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]] پارامتر u- : نام کاربری اختیاری را برای ورود به کامپیوتر از راه دور مشخص می کند. پارامتر p- : کلمه عبور نام کاربری را مشخص می کند. اگر حذف شده باشد، از شما خواسته میشودکه رمز عبور را وارد کنید بدون اینکه به صفحه نمایش بازتاب شود. پارامتر Id : شناسه (توسط PsFile اختصاص داده شده) فایل که برای نمایش اطلاعات و یا برای بستن آن. پارامتر Path :

ابزار شماره ۱۸	
	مسیر کامل یا جزئی فایلها برای مطابقت با نمایش اطلاعات یا بستن آن. پارامتر c- : بستن فایلهای شناسایی شده توسط شناسه یا مسیر

ابزار PsTools

ابزار شماره ۱۹	
نام ابزار	PsTools
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	به کارگیری NTFSInfo برای دیدن جزئیات اطلاعات در مورد حجم NTFS شامل سایز، محل Master File Table (MFT) و MFT-zone به عنوان سایز NTFS-file metadata سیستم فایل با فناوری نو (NTFS یا New Technology File System)استاندارد فایل سیستم‌های موجود در خانواده ویندوزهای NT است که از جمله آنها می‌توان به ویندوزهای ۲۰۰۰، XP و ۲۰۰۳ اشاره نمود

ابزار شماره ۱۹	
	PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر انتخاب شده. PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست .

ابزار شماره ۱۹	
	این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

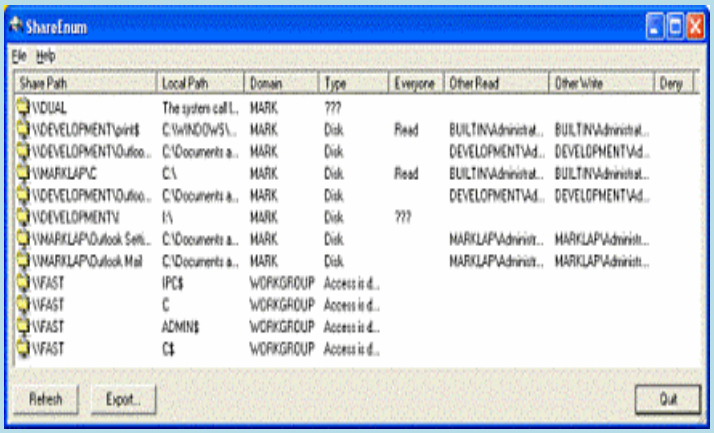
ابزار SDelete

ابزار شماره ۲۰	
نام ابزار	SDelete
لینک دانلود	https://download.sysinternals.com/files/SDelete.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	SDelete (Secure Delete) یک برنامه حذف ایمن است .شما می توانید با استفاده از SDelete به طور ایمن فایل های موجود را حذف کنید و همچنین به طور ایمن هر پرونده ای که در قسمت های غیر مجاز یک دیسک وجود دارد (از جمله فایل هایی که قبلا حذف شده یا رمزگذاری شده اند) را پاک کنید . SDelete وزارت دفاع را پاکسازی میکند و طبق استاندارد DOD ۵۲۲۰.۲۲-M عمل می کند تا به شما اطمینان دهد که با یک بار استفاده از SDelete اطلاعات حذف شده است،

ابزار شماره ۲۰	
	اطلاعات فایل شما برای همیشه از بین رفته است . توجه داشته باشید که SDelete فایل داده ها را بـه طـور ایمـن حذف می کند، اما نام فایل ها در فضای آزاد دیسک ذخیره نمی شود.
نحوه ی استفاده از ابزار	SDeleteیک ابزار خط فرمان است کـه تعـدادی گزینـه را مـی گیرد .در هر استفاده ، به شما این امکان را می دهد تـا یـک یـا چند فایل ویا دایرکتوری را حـذف کنیـد یـا فضـای آزاد را روی یک دیسک منطقی پاک کنید. sdelete [-p passes] [-s] [-q] <file or directory> ... sdelete [-p passes] [-z|-c] [drive letter] ... a- حذف ویژگی فقط خواندنی c- پاک کردن فضای آزادp passes- تعداد پاسهای بازنویسی را مشخص می کند (پیش فرض ۱ است). q- چاپ خطاها . s- یا r- زیر شاخه های بازیابی. z- صفر فضای آزاد (خوب برای بهینه سازی دیسک مجازی).

ابزار ShareEnum

ابزار شماره ۲۱	
نام ابزار	ShareEnum
لینک دانلود	https://download.sysinternals.com/files/ShareEnum.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	یک جنبه از امنیت شبکه ویندوز NT / ۲۰۰۰ / XP که اغلب نادیده گرفته شده است، اشتراک فایل است .نقص امنیتی رایج هنگامی رخ می دهد که کاربران فایل ها را با امنیت پایین تنظیم می کنند و کاربران غیر مجاز قادر به دیدن فایل های حساس می باشند هیچ ابزاری برای لیست کردن سهم قابل مشاهده بر روی شبکه و تنظیمات امنیتی آنها وجود ندارد، اما ShareEnum به شما اجازه می دهد که اشتراک فایل ها را در شبکه خود قفل کنید. هنگامی که شما ShareEnum را اجرا می کنید، از شمارهٔ NetBIOSاستفاده می کند تا همه رایانه ها را در حوزه های قابل دسترسی برای آن اسکن کند، و اشتراک فایل ها و تنظیمات امنیتی آنها را نشان میدهد. از آنجائیکه تنها مدیر دامنه امکان مشاهده تمام منابع شبکه را داراست، ShareEnum آن زمان به کار می آید که آن را ازحساب کاربری مدیر دامنه اجرا می کنید.	

ابزار شماره ۲۱	
نحوه ی استفاده از ابزار	ShareEnumاز WNetEnumResource برای ارزیابی دامنه ها و کامپیوترهای موجود در آنها و از NetShareEnum برای ارزیابی سهم هر رایانه استفاده میکند. 

ابزار Sigcheck

ابزار شماره ۲۲	
نام ابزار	Sigcheck
لینک دانلود	https://download.sysinternals.com/files/Sigcheck.zip
تاریخ انتشار	May ۲۲, ۲۰۱۷
معرفی این ابزار	یک ابزار خط فرمان است که شماره نسخه فایل، اطلاعات زمانبندی و جزئیات امضا دیجیتال، که از جمله زنجیره های گواهی هستند ، را نشان می دهد .همچنین شامل گزینه ای

ابزار شماره ۲۲	
	برای بررسی وضعیت فایل درVirusTotal ، سایتی کـه اسـکن خودکار را در برابر بیش از ۴۰ موتور آنتی ویـروس انجـام مـی دهد و گزینه ای برای آپلود یک فایل برای اسکن است.
نحوه ی استفاده از ابزار	sigcheck [-a] [-h] [-i] [-e] [-l] [-n] [[-s] |[-c|-ct] |[-m]][-q] [-r][-u][-vt][-v[r][s]][-f catalog file] <file or directory> sigcheck -d [-c|-ct] <file or directory> sigcheck -o [-vt] [-v[r]] <sigcheck csv file> sigcheck -t[u][v] [-i] [-c|-ct] <certificate store name|*> c-خروجی CSV با جدا کننده کاما d- محتویات یک فایل کاتالوگ را خالی کنید e- اسکن تصاویر قابل اجرا (صرف نظر از گسترش آنها) f- به امضا در فایل کاتالوگ مشخص شده نگاه کنید h- نمایش هش های پرونده i- نمایش نام فروشگاه و زنجیره امضاء l- عبور لینک های نمادین و اتصالات دایرکتوری n- فقط شماره نسخه فایل را نشان می دهد یکی از راه های استفاده از این ابزار این اسـت کـه فایـل هـای بدون نام را در دایرکتـوری Windows \ System۳۲ \ خـود بـا این دستور چک کنید:

ابزار شماره ۲۲	
	system۳۲ sigcheck -u -e c: \ windows \

ابزار Streams

ابزار شماره ۲۳	
نام ابزار	Streams
لینک دانلود	https://download.sysinternals.com/files/Streams.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	سیستم فایل NTFS برنامه های کاربردی را قادر می سازد جریان های داده های جایگزین اطلاعات را ایجاد کند .به طور پیش فرض، تمام داده ها در یک جریان اطلاعات بی نام اصلی فایل ذخیره می شوند، اما با استفاده از نحو "file:stream "، شما قادر به خواندن و نوشتن به متناوب هستید .همه برنامه ها برای دسترسی به جریان های متناوب نمی نویسند، اما شما می توانید جریان ها را به سادگی نشان دهید .ابتدا، خط فرمان را به یک دایرکتوری بر روی یک درایو NTFS تغییر دهید .بعد،

ابزار شماره ۲۳	
	"echo <hello> test: stream"را تایپ کنید .شما فقط یک جریان با نام 'stream ' ایجاد کرده اید که با فایل 'test' همراه است .توجه داشته باشید هنگامی که شما به اندازه test نگاه می کنید، آن را برابر با صفر گزارش می کنید، و فایل در هر ویرایشگر متن خالی دیده می شود .برای دیدن stream خود 'more < test:stream>' را وارد کنید.
نحوه ی استفاده از ابزار	streams [-s] [-d] <file or directory> -s زیر شاخه ها را بازسازی می کند. -d حذف جریان ها

ابزار Sync

ابزار شماره ۲۴	

ابزار شماره ۲۴	
نام ابزار	Sync
لینک دانلود	https://download.sysinternals.com/files/Sync.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	ابزار Sync ، در تمام نسخه های ویندوز کار می کند .هر زمان که بخواهید بدانید که فایل داده های اصلاح شده به صورت ایمن بر روی هارد دیسک ذخیره شده است، میتوان از آن استفاده کرد .متاسفانه، Syncنیاز به دسترسی مدیریت برای اجرا دارد .این نسخه همچنین به شما اجازه می دهد که درایوهای قابل جابجایی مانند درایوهای ZIP را از بین ببرید.
نحوه ی استفاده از ابزار	sync [-r] [-e] [drive letter list] r-درایوهای قابل جابجایی فلاش e-درایوهای قابل جابجایی را حذف می کند.

ابزار VolumeID

ابزار شماره ۲۵	
نام ابزار	VolumeID

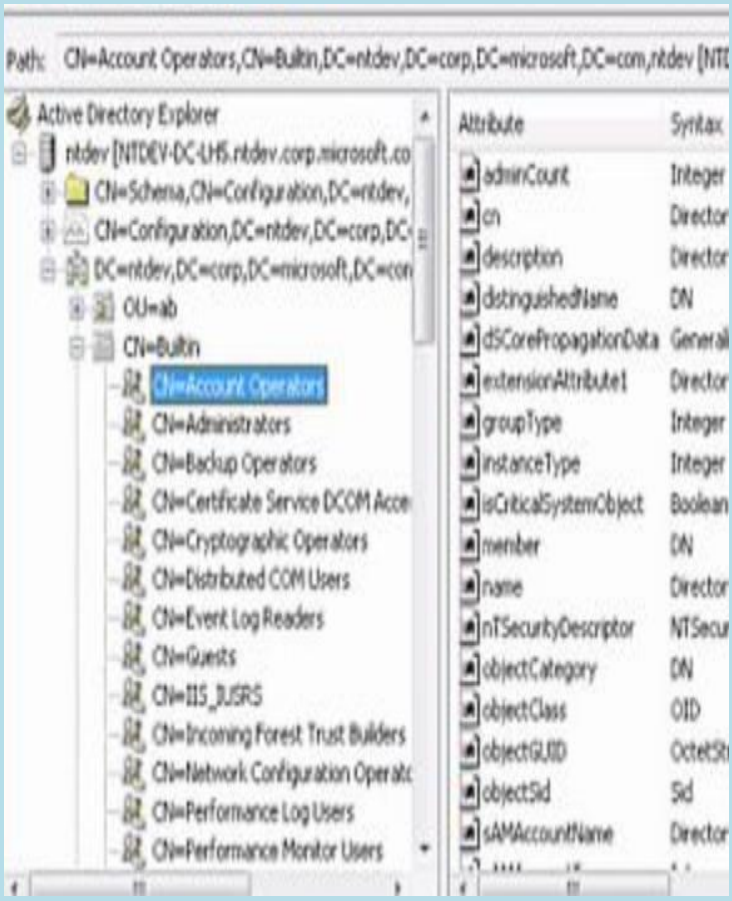
ابزار شماره ۲۵	
لینک دانلود	https://download.sysinternals.com/files/VolumeId.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	در حالی که ابزارهای Label ویندوز ۲۰۰۰ / NT و ویندوز ۹۵ و ۹۸ به شما اجازه می دهد تا برچسب های حجم دیسک را تغییر دهید، هیچ وسیله ای برای تغییر شناسه های ذخیره شده، ارائه نمی دهد. VolumeID، به شما امکان تغییر شناسه های FAT و NTFS دیسک ها (فلاپی ها یا هارد دیسک ها) را می دهد.
نحوه ی استفاده از ابزار	این برنامه خط فرمانی است و شما باید آن را در خط فرمان ویندوز اجرا کنید. توجه داشته باشید که تغییرات در حجم NTFS تا زمان راه اندازی مجدد بعدی قابل مشاهده نیست. علاوه بر این، قبل از تغییر یک شناسه حجم، هر برنامه ای را که پیش از آن اجرا کرده اید، تعطیل کنید.

دسته دوم Sysinternals Networking Utilities

معرفی ابزارهای موجود در دسته دوم

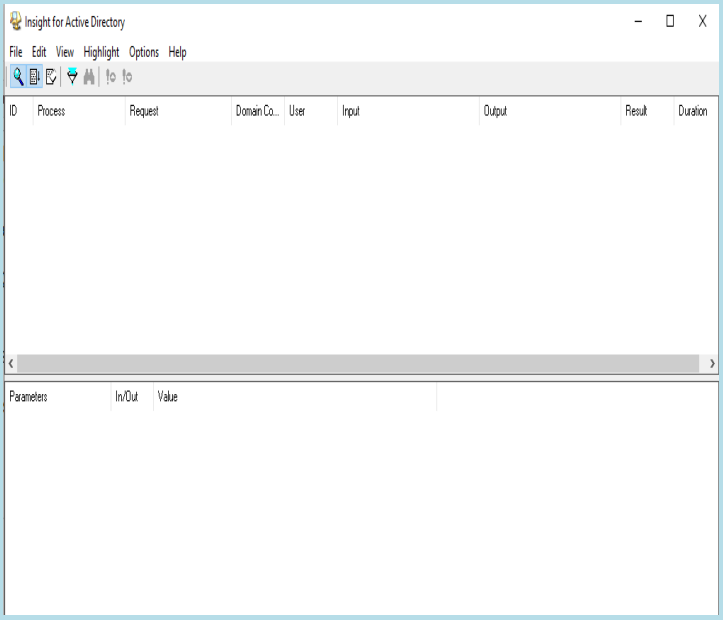
ابزار Active Directory Explorer

ابزار شماره ۱	
نام ابزار	AdExplorer
لینک دانلود	https://download.sysinternals.com/files/AdExplorer.zip
تاریخ انتشار	November ۱۵, ۲۰۱۲
معرفی این ابزار	AD Explorer یک دایرکتوری پیشرفته Active Directory (AD) و ویرایشگر است. شما می توانید از AD Explorer به راحتی به یک پایگاه داده AD بروید، مکان های مورد علاقه را مشخص کنید، خواسته ها و ویژگی های شیء را مشاهده کنید، بدون نیاز به باز کردن جعبه های محاوره ای، ویرایش مجوز ها، مشاهده اشیاء، و جستجو های پیشرفته ای که می توانید ذخیره کنید و مجددا اجرا کنید. AD Explorer همچنین شامل توانایی ذخیره عکس های فوری از پایگاه داده AD برای مشاهده و مقایسه خارج از خط است. هنگامی که یک فتوشاپ ذخیره شده را بارگذاری می کنید، می

ابزار شماره ۱	
	توانید آن را به همان شیوه پایگاه داده زنده مشاهده کنید و آن را کشف کنید. اگر شما دو عکس از یک پایگاه داده AD داشته باشید می توانید از قابلیت مقایسه AD Explorer استفاده کنید تا ببینید چه اشیاء، ویژگی ها و مجوزهای امنیتی بین آنها تغییر کرده است.
نحوه ی استفاده از ابزار	نرم افزار را از لینک داده شده دانلود کرده از حالت فشرده در بیاورید و به راحتی آن را نصب و اجرا کنید. 

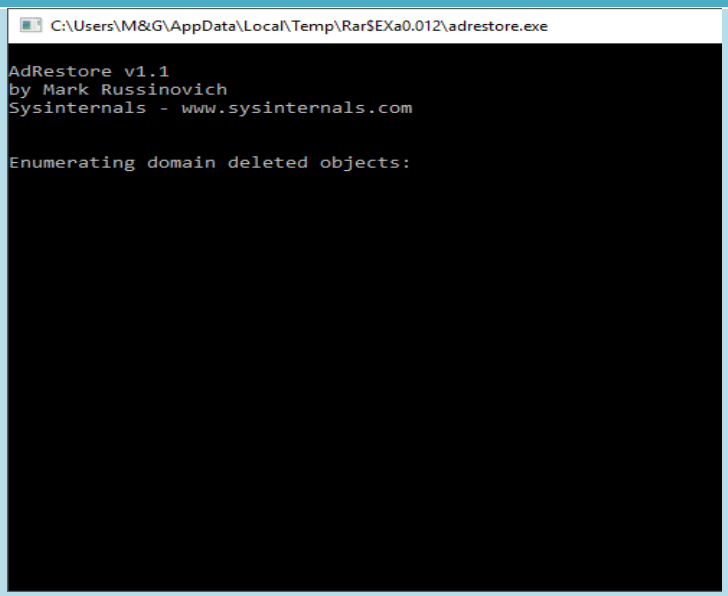
ابزار Insight for Active Directory

ابزار شماره ۲	
نام ابزار	AdInsight
لینک دانلود	https://download.sysinternals.com/files/AdInsight.zip
تاریخ انتشار	October ۲۶, ۲۰۱۵
معرفی این ابزار	AD Insight LDAP (پروتکل دسترسی آسان دیتابیس دسترسی به دیتابیس) ابزار مانیتورینگ برای رفع اشکال برنامه های کاربردی سرویس گیرنده Active Directory است. از ردیابی کاملی ارتباطات client-server Active Directory برای رفع شناسایی ویندوز، Exchange، DNS و سایر مشکلات استفاده کنید. ADInsight با استفاده از تکنیک های تزریق DLL به فراخوانی تماس هایی که برنامه ها در کتابخانه dll۳۲Wldap. هستند می پردازد، که کتابخانه استاندارد Active Directory API ها مانند ldap و ADSI است. بر خلاف ابزارهای نظارت بر شبکه، ADInsight تمامی API های سمت سرویس گیرنده را از بین می برد و تفسیر می کند، از جمله آنهایی که در نتیجه انتقال به

ابزار شماره ۲	
	یک سرور نیستند. ADInsight مانیتور هر فرآیندی را که می تواند آن را بارگذاری نماید، DLL ردیابی می کند، بدین معنا که مجوز نیاز ندارد، اما اگر با حقوق اداری اجرا شود، همچنین فرآیندهای سیستم، از جمله خدمات ویندوز را نظارت خواهد کرد.
نحوه ی استفاده از ابزار	نرم افزار را از لینک داده شده دانلود کرده از حالت فشرده در بیاورید و به راحتی فایل ADInsight.exe را اجرا کنید. 

ابزار AdRestore

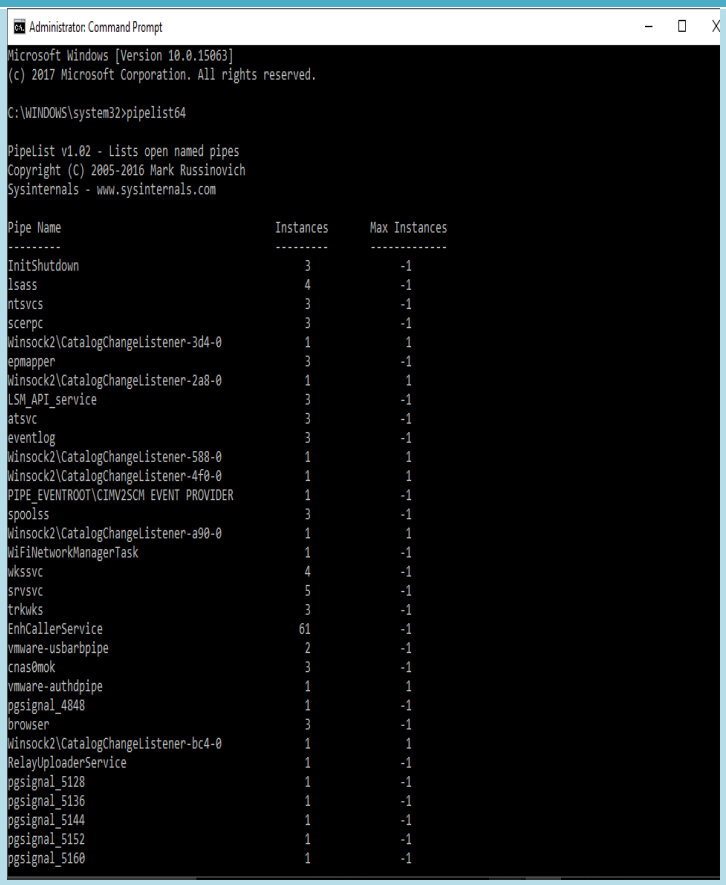
ابزار شماره ۳	
نام ابزار	ADRestore
لینک دانلود	https://download.sysinternals.com/files/ADRestore.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	ویندوز سرور ۲۰۰۳ توانایی بازگرداندن اشیاء پاک شده tombstoned را معرفی می کند. این ابزار ساده خط فرمان، اشیاء حذف شده در یک دامنه را شمارش می کند و به شما امکان بازگرداندن هر یک از آنها را می دهد. کد منبع بر اساس کد نمونه در Microsoft Platform SDK است.
نحوه ی استفاده از ابزار	نرم افزار را از لینک داده شده دانلود کرده از حالت فشرده در بیاورید و به راحتی فایل adrestore.exe را اجرا کنید.

ابزار شماره ۳	
	

ابزار PipeList

ابزار شماره ۴	
نام ابزار	PipeList
لینک دانلود	https://download.sysinternals.com/files/PipeList.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	این امکان وجود ندارد که فهرست دایرکتوری از لوله های نامیده شده در سیستم را با استفاده از Win ۳۲API انجام دهید. به طور مستقیم با استفاده از NtQueryDirectoryFile، تابع بومی که بر روی API های Win۳۲ FindFile تکیه می کنند، امکان

ابزار شماره ۴	
	لیست کردن لوله ها وجود خواهد داشت.
نحوه ی استفاده از ابزار	این ابزار یک برنامه است که به صورت کنسول اجرا می شود. پس از دانلود این ابزار به command prompt در ویندوز می رویم و آدرس جایی را که این نرم افزار وجود دارد زده تا این ابزار اجرا شود سپس با تایپ pipelist۶۴ و اجرای ابزار دستورات کاربردی آن با توضیح نشان داده می شود. برای مثال ما ابزار pipelist۶۴.exeرا در مسیر windows\system۳۲ کپی می کنیم با تایپ آن طبق شکل زیر برنامه اجرا می شود:

ابزار شماره ۴


ابزار PsPing

ابزار شماره ۵

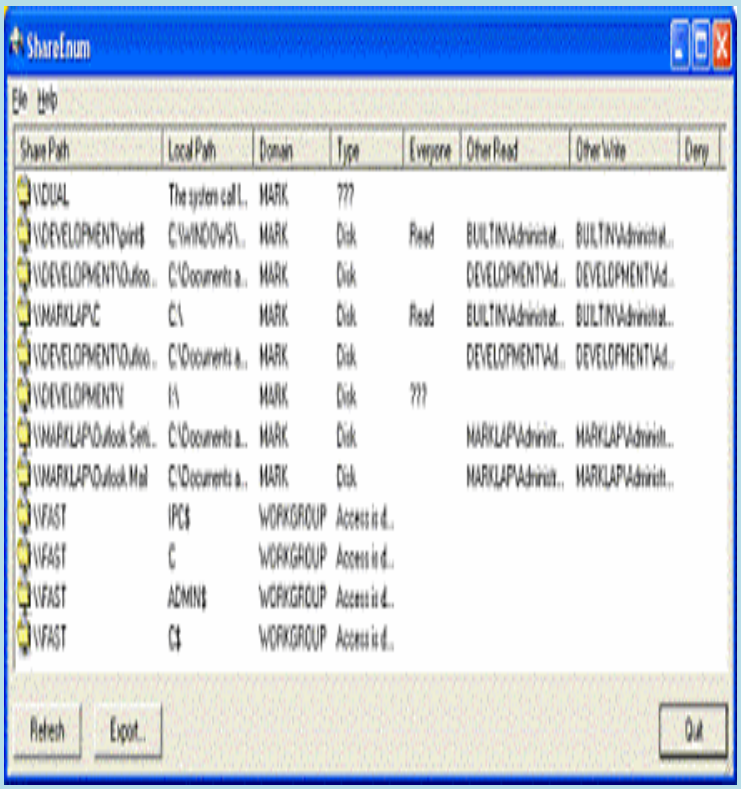
ابزار شماره ۵	
نام ابزار	PsPing
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	PsPing پیاده سازی قابلیت های Ping، پینگ TCP، اندازه گیری تاخیر و پهنای باند. از گزینه های خط فرمان زیر برای نشان دادن استفاده برای هر نوع آزمون استفاده کنید: **Usage: psping -? [i|t|l|b]** Parameter — Description -? I — Usage for ICMP ping. -? T — Usage for TCP ping. -? L — Usage for latency test. -? B — Usage for bandwidth test. ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و خروجی را به صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با سیستم های ویندوز NT و نسخه های بعدی سازگاری کامل دارند .این ابزارها هرچند قابلیت اجرا بر روی سیستم های

ابزار شماره ۵	
	ریموت را دارند ولی در مقابل قابلیت استفاده به صورت لوکال و در شبکه محلی را نیز دارند. مجموعه ابزار pstools نیاز به نصب ندارند. ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر انتخاب شده.

ابزار شماره ۵	
	PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

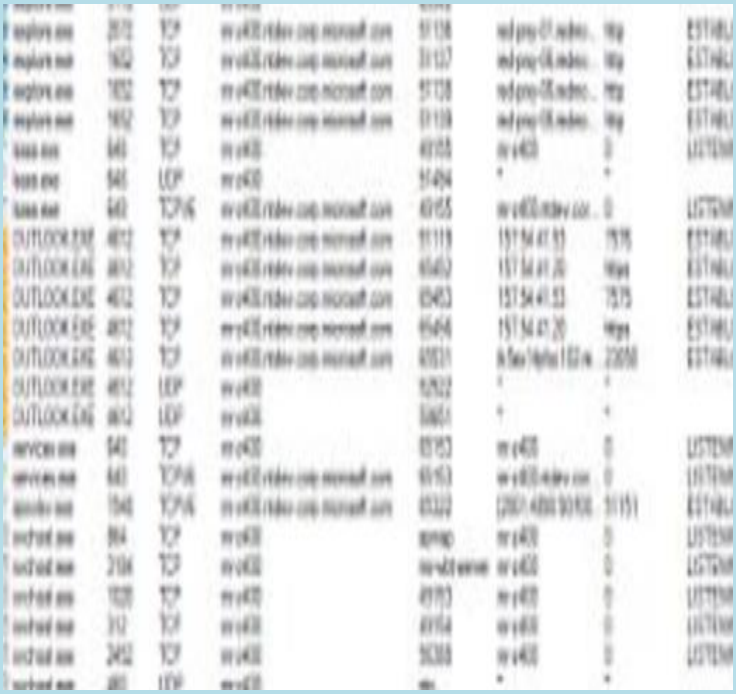
ابزار ShareEnum

ابزار شماره ۶	
نام ابزار	ShareEnum
لینک دانلود	https://download.sysinternals.com/files/ShareEnum.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	یک جنبه از امنیت شبکه ویندوز / XP ۲۰۰۰NT / که اغلب نادیده گرفته شده است، اشتراک فایل است. نقص امنیتی رایج هنگامی رخ می دهد که کاربران فایل ها را با امنیت پایین تنظیم می کنند، و اجازه می دهد تا کاربران غیر مجاز فایل های حساس را مشاهده کنند. هیچ ابزار ساخته شده برای لیست کردن Shareها قابل مشاهده بر روی شبکه و تنظیمات امنیتی آنها وجود ندارد، اما ShareEnum به شما اجازه می دهد که اشتراک فایل ها را در شبکه خود قفل کنید. هنگامی که شما ShareEnum را اجرا می کنید، از شمارهٔ NetBIOS استفاده می کند تا همه رایانه ها را در حوزه های قابل دسترسی برای آن اسکن کند، نشان دادن اشتراک فایل ها و چاپ ها و تنظیمات امنیتی آنها. از آنجائیکه تنها مدیر دامنه دارای توانایی مشاهده تمام منابع شبکه است، ShareEnum موثرتر از زمان اجرای آن از یک حساب کاربری مدیریت دامنه است.

ابزار شماره ۶	
نحوه ی استفاده از ابزار	ShareEnum با استفاده از WNetEnumResource برای ارزیابی دامنه ها و کامپیوترهای موجود در آنها و NetShareEnum بـرای شمارش Share ها در رایانه ها. 

ابزار TCPView

ابزار شماره ۷	
نام ابزار	TCPView
لینک دانلود	https://download.sysinternals.com/files/TCPView.zip
تاریخ انتشار	July ۲۵, ۲۰۱۱
معرفی این ابزار	TCPView یک برنامه ویندوز است که فهرست دقیق تمام نقطه های TCP و UDP در سیستم شما را شامل می شود، از جمله آدرس های محلی و از راه دور و وضعیت اتصالات. TCPView همچنین نام پروسه ای که دارای نقطه پایانی است را گزارش می دهد. TCPView یک زیرمجموعه اطلاعاتی است و به راحتی برنامه Netstat را ارائه می دهد که با ویندوز همراه است. دانلود TCPView شامل Tcpvcon، یک نسخه خط فرمان با همان قابلیت است.
نحوه ی استفاده از ابزار	هنگامی که TCPView را اجرا می کنید، تمام نقطه های پایانی TCP و UDP فعال را شناسایی می کند. شما می توانید از دکمه نوار ابزار یا آیتم های منو برای نمایش resolved names استفاده کنید. در سیستم های ویندوز XP، TCPView نام پروسه ای که هر نقطه پایانی را دارد، نشان می دهد. به طور پیش فرض، TCPView به طور مداوم در هرثانیه اسکن می کند، اما شما می توانید از گزینه Refresh Rate برای تغییر

ابزار شماره ۷	
	زمان آن استفاده کنید. اگر Endpoints از یک بروز رسانی به بعد تغییر وضعیت دهند، به رنگ زرد برجسته می شوند. کسانی که حذف شده اند قرمز نشان داده شده است، و نقاط انتهایی جدید با رنگ سبز نشان داده می شوند. با انتخاب File | Close Connections یا با کلیک راست روی یک اتصال و انتخاب بستن Connections از منوی زمینه نتیجه حاصل می توانید اتصالات TCP / IP برقرار شده (که با وضعیت ESTABLISHED برچسب گذاری شده اند) را ببندید. 

ابزار Whois

ابزار شماره ۸	
نام ابزار	WhoIs
لینک دانلود	https://download.sysinternals.com/files/WhoIs.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	Whois ثبت نام برای نام دامنه یا آدرس IP شما را مشخص می کند.
نحوه ی استفاده از ابزار	این ابزار یک برنامه است که به صورت کنسول اجرا می شود. پس از دانلود این ابزار به command prompt در ویندوز می رویم و آدرس جایی را که این نرم افزار وجود دارد زده تا این ابزار اجرا شود سپس با تایپ whois۶۴ و اجرای ابزار دستورات کاربردی آن با توضیح نشان داده می شود. برای مثال ما ابزار whois۶۴.exe را در مسیر windows\system۳۲ کپی می کنیم با تایپ آن طبق شکل زیر برنامه اجرا می شود:

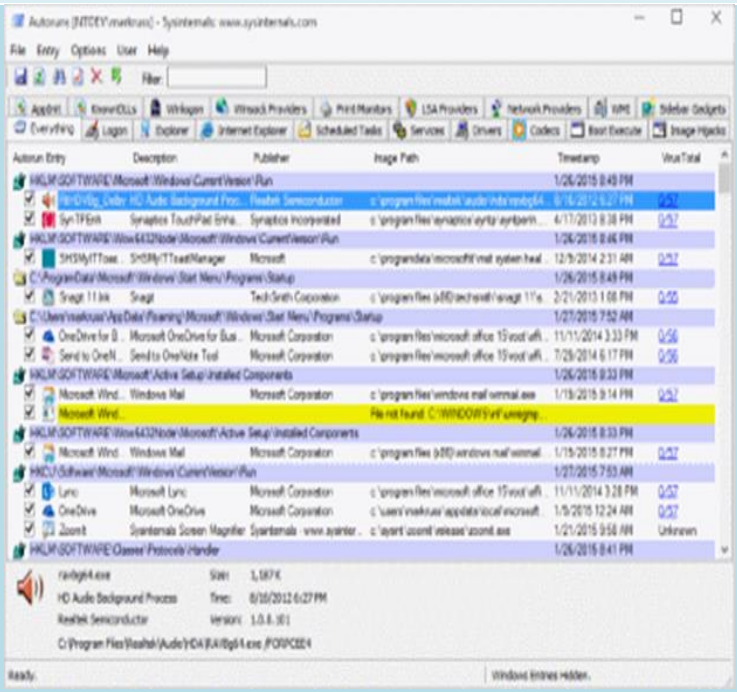
ابزار شماره ۸	
	Usage: whois [-v] domainname [whois.server] Parameter Description -v Print whois information for referrals

دسته سوم Sysinternals Process Utilities

معرفی ابزارهای موجود در دسته سوم

ابزار AutoRuns

ابزار شماره ۱	
نام ابزار	Autoruns
لینک دانلود	https://download.sysinternals.com/files/Autoruns.zip
تاریخ انتشار	September ۱۱, ۲۰۱۷
معرفی این ابزار	این ابزار، که دارای جامع ترین دانش از مکان های خودکار شروع هر مانیتور راه اندازی است، برنامه های پیکربندی شده برای اجرا در طول bootupسیستم و یا ورود به سیستم، و زمانی که شما شروع به اجرا برنامه های مختلف ساخته شده در ویندوز مانند اینترنت اکسپلورر، اکسپلورر و مدیا پلیر را نشان می دهد . این

ابزار شماره ۱	
	برنامه ها شامل مواردی هستند که در پوشه راه اندازی، Run، RunOnceو دیگر کلید های رجیستری قرار دارند . Autoruns ، پسوندهای پوسته اکسپلورر ، نوار ابزار، اشیاء کمکی مرورگر، اطلاعیهWinlogon ، خدمات خودکار شروع، و ... را گزارش میدهد. گزینه Autoruns Hide Signed Microsoft Entries به شما کمک می کند تا عکس های شخص ثالثی که به سیستم شما اضافه شده اند، بزرگتر شوید و از جستجوی خودکار عکس هایی که برای حساب های دیگر پیکربندی شده است در یک سیستم پشتیبانی میکند .همچنین در بسته دانلود شامل یک معادل خط فرمان می باشد که می تواند در قالبCSV ، تولید شود.
نحوه ی استفاده از ابزار	

ابزار شماره ۱	
	به سادگی Autoruns را اجرا کنید و به شما برنامه های شروع خودکار پیکربندی شده و همچنین لیست کامل مکان های رجیستری و فایل سیستمی که برای پیکربندی خودکار فعال شده را نشان می دهد . مکان های Autostart نمایش داده شده توسط Autoruns شامل ورودی های ورود به سیستم، افزودنی های اکسپلورر، افزودنی های اینترنت اکسپلورر از جمله Object Helper Browser (BHOs)، Appinit DLLهای، خسارت های تصویری، تصاویر بوت اجرا، DLLهای اطلاع رسانیWinlogon ، سرویس های ویندوز و Winsock ارائه دهندگان خدمات لایه، رسانه ها کدک ها و....است . زبانه ها را برای نمایش ایستگاه های خودکار از دسته های مختلف سوئیچ کنید. نحوه ی استفاده از نسخه خط فرمان: autorunsc [-a <*|bdeghiklmoprsw>] [-c|-ct] [-h] [-m] [-s] [-u] [-vt] [[-z] | [user]]] a- انتخاب ورودی *\ همه b اجرا بوت g اسباب بازی نوار ابزار (ویستا و بالاتر) i افزونه های اینترنت اکسپلورر. k DLL های شناخته شده

ابزار شماره ۱	
	l راه اندازی ورود به سیستم (پیش فرض). m ورودیWMI n پروتکل Winsock و ارائه دهندگان شبکه. P چاپگر DLL های مانیتور. Wورودی.Winlogon c-چاپ خروجی به عنوان.CSV ct-چاپ خروجی به عنوان مقادیر جدا شده با تب. h-نمایش هش های پرونده. m-مخفی کردن مقالات مایکروسافت(در صورت استفاده با v- نوشته های امضا شده را مخفی کنید) s-امضای دیجیتال را تأیید کنید. t-نشان دادن نشانگرهای زمانی در UTC معمولی (YYYYMMDD-hhmmss). u-اگر بررسی VirusTotal فعال باشد، نشان می دهد فایل های ناشناخته توسط VirusTotalیا تشخیص غیر صفر، در غیر این صورت فقط فایل های بدون امضا را نشان می دهد. x-چاپ خروجی به عنوان.XML vt-قبل از استفاده از ویژگی هایVirusTotal ، شما باید شرایط سرویس VirusTotal را بپذیرید .اگر شرایط را قبول نکردید و این گزینه را حذف می کنید، به صورت تعاملی از شما خواسته می شود.

ابزار شماره ۱	
	z- سیستم آفلاین ویندوز را برای اسکن تعیین می کند. userمشخص کننده نام حساب کاربری که موارد autorun نمایش داده خواهد شد .برای تشخیص تمام پروفایل های کاربری، '*' را انتخاب کنید.

ابزار Handle

ابزار شماره ۲	
نام ابزار	Handle
لینک دانلود	https://download.sysinternals.com/files/Handle.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	Handleیک ابزار است که اطلاعات مربوط به دسته های باز برای هر فرآیند در سیستم را نمایش می دهد .شما می توانید از آن برای دیدن برنامه هایی که دارای پرونده باز هستند و یا برای دیدن انواع و اسامی تمامی شیء های یک برنامه ،استفاده کنید.
نحوه ی استفاده از ابزار	Handle در جستجو برای منابع فایل باز است، بنابراین اگر شما هیچ پارامترهای خط فرمان را مشخص نکنید، مقادیر تمام دسته های سیستم را که به فایل های باز اشاره دارند و نام فایل ها را لیست می کند.

ابزار شماره ۲	
	handle [[-a] [-u] | [-c <handle> [-l] [-y]] | [-s]] [-p <processname>|<pid>> [name] a- اطلاعات در مورد انواع دسته ها، نه تنها کسانی که به فایل ها اشاره می کنند را از بین می برند .انواع دیگر شامل پورت ها، کلید های رجیستری، نخ ها و فرآیندها هستند. c- handle مشخص شده را تعطیل می کند . شما باید فرایند را با PID خودش مشخص کنید. l- اندازه بخش های پشتیبانی شده بر روی صفحه را از بین ببرید. y- تأیید برای بستن handle s- چاپ تعداد از هر نوع ،دسته های باز. u- نشانگر نام کاربر مالک هنگام جستجو برای دسته ها. p- به جای بررسی همه دسته ها در سیستم، این پارامتر اسکن دستی را به آن فرایندهایی که با نام فرایند شروع می شود محدود می کند .بدین ترتیب: handle -p exp فایلهای باز را برای تمام فرآیندهای که با «exp» شروع می شوند، شامل Explorer می شوند. name این پارامتر وجود دارد به طوری که شما می توانید

ابزار شماره ۲	
	Handleرا برای جستجو برای اشاره به یک شی با یک نام خاص هدایت کنید.

ابزار ListDLLs

ابزار شماره ۳	
نام ابزار	ListDLLs
لینک دانلود	https://download.sysinternals.com/files/ListDlls.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	ListDLLs یک ابزار است که DLL های بارگذاری شده در فرآیندها را گزارش میدهد. شما می توانید آن را برای لیست تمام DLL های بارگذاری شده در تمام فرآیندها، و یا یک فرایند خاص، یا لیست پروسه هایی که یک DLL خاص دارند بارگذاری کنید. ListDLLs همچنین می تواند اطلاعات نسخه کامل را برای DLL ها، از جمله امضای دیجیتال خود را نمایش دهد، و می تواند برای پردازش DLL های بدون امضا استفاده شوند.

ابزار شماره ۳	
نحوه ی استفاده از ابزار	listdlls [-r] [-v | -u] [processname|pid] listdlls [-r] [-v] [-d dllname] processname تخلیه DLL های لود شده توسط فرآیند. pid تخلیه DLL های مرتبط با شناسه پردازش مشخص شده. dllname فقط پروسه هایی را نشان می دهد که DLL مشخص شده را بارگذاری کرده اند. -r پرچم DLL که جابجا شده اند زیرا آنها در آدرس پایه خود بارگذاری نشده اند. -u تنها لیست DLL های بدون نام را لیست کنید. -v نمایش اطلاعات نسخه DLL.

ابزار Portmon

ابزار شماره ۴	
نام ابزار	portmon
لینک دانلود	https://download.sysinternals.com/files/ portmon.zip
تاریخ انتشار	January ۱۲, ۲۰۱۲

ابزار شماره ۴	
معرفی این ابزار	یک ابزار است که فعالیت های سریال و پورت موازی را در یک سیستم نظارت و نمایش می دهد. این قابلیت پیشرفته فیلتر کردن و جستجو را دارد که آن را ابزار قدرتمند برای بررسی نحوه کار ویندوز می داند، نحوه استفاده از برنامه ها از پورت ها یا ردیابی مشکلات در تنظیمات سیستم یا برنامه را توضیح می دهد.
نحوه ی استفاده از ابزار	به سادگی فایل برنامه Portmon (portmon.exe) را اجرا کنید و Portmon بلافاصله شروع به گرفتن خروجی اشکال زدایی می کند. برای اجرای Portmon در ویندوز ۹۵ شما بایستی WinSock۲ را از مایکروسافت دریافت کنید. توجه داشته باشید که اگر Portmon در ویندوز NT / ۲K اجرا شود، portmon.exe باید در یک درایو غیر شبکه قرار گیرد و شما باید دارای امتیاز مدیریتی باشید. منوها، کلید های hot-key یا دکمه های نوار ابزار می توانند برای پاک کردن پنجره، ذخیره داده های نظارت شده در یک فایل، جستجو خروجی، تغییر فونت پنجره و غیره استفاده شوند. کمک در خط شرح همه ویژگی های Portmon است. پورتمن تمام فرمان های I / O control I / O (IOCTLs) سریال و موازی را درک می کند و آنها را همراه با اطلاعات

ابزار شماره ۴	
	جالب در مورد پارامترهای مرتبط با آن نمایش می دهد. برای خواندن و نوشتن درخواست Portmon اولین چندین بایت بافر را نمایش می دهد، با استفاده از '.' برای نشان دادن کاراکترهای غیر قابل چاپ گزینه Show Hex به شما این امکان را می دهد که بین ASCII و خروجی شصت خالص داده های بافر را تغییر دهید.

ابزار Process Explorer

ابزار شماره ۶	
نام ابزار	Process Explorer
لینک دانلود	https://download.sysinternals.com/files/ Process Explorer.zip
تاریخ انتشار	May ۱۶, ۲۰۱۷
معرفی این ابزار	تا کنون فکر کرده اید که کدام یک فایل یا دایرکتوری خاص باز است؟ اکنون می توانید پیدا کنید Process Explorer به شما

ابزار شماره ۶	
	نشان می دهد که کدام دسته ها و فرآیندهای DLL باز یا بارگذاری شده اند. صفحه نمایش Process Explorer متشکل از دو زیر پنجره است. پنجره بالا همیشه یک لیست از فرآیندهای در حال حاضر فعال، از جمله نام حساب های خود را نشان می دهد، در حالی که اطلاعات نمایش داده شده در پنجره پایین، بستگی به حالت که Process Explorer در آن است: اگر در حالت دسته باشد، خواهید دید فرایند انتخاب شده در پنجره بالا باز می شود؛ اگر Process Explorer در حالت DLL باشد، DLL ها و فایل های mapped شده حافظه را که روند بارگذاری شده را مشاهده می کنید. فرآیند اکسپلورر نیز یک قابلیت جستجو قدرتمند است که به سرعت نشان می دهد که چه فرآیندهای خاص دستگیره های باز شده و یا DLL ها بارگذاری شده است. قابلیت های منحصر به فرد Process Explorer آن را برای ردیابی مشکلات نسخه DLL یا نشت نشتی ها مفید می سازد و بینش در مورد نحوه کار ویندوز و برنامه های کاربردی را ارائه می دهد.
نحوه ی استفاده از ابزار	به سادگی اجرای Process Explorer (procexp.exe) را اجرا

ابزار شماره ۶	
	کنید. فایل کمک توضیح می دهد عملیات و استفاده از پردازنده اکسپلورر. اگر مشکلی دارید یا سوالی دارید، لطفا از Sysinternals Process Explorer Forum دیدن کنید.

ابزار Process Monitor

ابزار شماره ۷	
نام ابزار	Process monitor
لینک دانلود	https://download.sysinternals.com/files/ Process monitor.zip
تاریخ انتشار	September ۱۲, ۲۰۱۷
معرفی این ابزار	فرآیند مانیتورینگ یک ابزار نظارت پیشرفته برای ویندوز است که زمان واقعی را که فایل های سیستمی، فعالیت های رجیستری و روند / نخی را نشان می دهد. این فرآیند ترکیبی از ویژگی های دو واحد داخلی سیستم با نام های Filemon و Regmon می باشد. این ابزار شامل یک لیست گسترده ای از

ابزار شماره ۷	
	برنامه های پیشرفته شامل فیلتر های غنی و غیر مخرب، رویداد های جامع مانند شناسه های جلسه و نام کاربری و ویژگی های آن ها، اطلاعات پردازشی قابل اعتماد، پشته های موضوعی کامل با پشتیبانی از نماد های یکپارچه برای هر عملیات، ویژگی ورود به سیستم به صورت همزمان و... است. ویژگی های منحصر به فرد این نرم افزار قدرتمند آن را به یک ابزار اصلی برای عیب یابی سیستم و شکار نرم افزارهای مخرب تبدیل کرده است. ویژگی های منحصر به فرد قدرتمند Process Monitor یک ابزار اصلی را در ابزارهای عیب یابی سیستم و شکار نرم افزارهای مخرب شما ایجاد می کند. نگاهی اجمالی به توانایی های فرآیند قدرتمند مانیتورینگ توانایی نظارت و فیلتر کردن، به عنوان نمونه این نرم افزار می تواند داده های بیشتری را برای پارامترهای ورودی و خروجی عملیات ها بگیرد. فیلترهای غیر مخرب به شما این امکان را می دهند که بدون دانستن اطلاعات، فیلتر کنید. ضبط مقاطع نخ برای هر عملیات در بسیاری از موارد امکان شناسایی علت اصلی عملیات را میسر می سازد.

ابزار شماره ۷	
	بدست آوردن اطلاعات قابل اطمینان از جزئیات روندها،به کمک این برنامه امکان پذیر است. به عنوان نمونه مسیرهای تصویر، خطوط فرمان، کاربر و شناسه جلسه از این طریق بدست می آید. قرار دادن ستون های قابل تنظیم و متحرک برای هر ویژگی فیلترها را می توان برای هر زمینه داده ای بکار برد به عنوان نمونه با کمک این برنامه فیلدها به عنوان ستون تنظیم نمی شوند. معماری پیشرفته ورود به سیستم می تواند ده ها میلیون کاربر و گیگابایت داده را ساپورت کند. ابزار درخت فرایند، رابطه بین تمامی فرآیندهای اشاره شده در ردیابی را نشان می دهد. فرمت ورودی و محلی تمامی داده ها را برای بارگیری در یک فرایند مانیتورینگ نمونه و متفاوت نگه می دارد. ابزار آسان و راهنمای تصویری و اطلاعات کامل در جهت برای مشاهده و استفاده آسان راهنمای ابزاری به همراه جزئیات مربوط به آن ها به شما امکان دسترسی آسان به داده های فرمت شده را می دهد. این امکان در ستون ها جا نمی شود. جستجوی لغو پذیر:

ابزار شماره ۷	
	در زمان بوت شدن تمامی ورودی های سیستم و تمامی عملیات ها تحت تاثیر قرار می گیرند. بهترین روش برای آشنا کردن با ویژگی های فرایند مانیتورینگ این است که از طریق فایل هلپ و کمک استفاده کرده و سپس هر یک از آیتم های منو و گزینه های آن را در یک سیستم زنده مشاهده کرده و امتحان کنید.

ابزار PsExec

ابزار شماره ۸	
نام ابزار	PsExec
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	

ابزار شماره ۸	
	نرم افزارهایی نظیر Telnet و برنامه های کنترل از راه دور مانند Symantec PC هرجا به شما اجازه اجرای برنامه ها در سیستم های از راه دور را می دهد، اما می توانید آنها را تنظیم کنید و نیاز به نصب نرم افزار کلاینت را در سیستم های راه دور که میخواهید به آن دسترسی پیدا کنید. PsExec یک جایگزین تلفنی با وزن سبک است که به شما امکان اجرای فرآیندها در سایر سیستم ها را میدهد، با تعامل کامل برای برنامه های کنسول، بدون نیاز به نصب دستی نرم افزار کلاینت. از مزایای قدرتمند PsExec عبارتند از راه اندازی دستورات تعاملی در سیستم های از راه دور و ابزارهای از راه دور مانند IpConfig که در غیر اینصورت توانایی نمایش اطلاعات مربوط به سیستم های از راه دور را ندارند. توجه: برخی از اسکنرهای ضد ویروس گزارش می دهند که یک یا چند ابزار با یک ویروس "remote admin" آلوده شده اند. هیچ یک از PsTools حاوی ویروس نیست، اما توسط ویروس ها مورد استفاده قرار گرفته است، به همین دلیل آنها باعث انتشار اطلاعیه های ویروس می شوند.
نحوه ی استفاده از ابزار	پردازنده های جداگانه که در آن برنامه می تواند با کاما اجرا شود در صورتی که CPU ۱ کمترین تعداد باشد. برای مثال، برای اجرای برنامه در CPU ۲ و CPU ۴، عبارت "۲- a،۴" را

ابزار شماره ۸	
	وارد کنید c- برنامه مشخص شده را به سیستم راه دور برای اجـرای کپـی کنید. اگر این گزینه را حذف کنید، برنامه باید در مسیر سیستم در سیستم راه دور باشد. d- منتظر فرآیند خاتمه دادن (غیر تعاملی) نباشید. e- نمایه حساب مشخص شده را بارگیری نمی کند. f- برنامه مشخص شده را حتی اگر فایل در سیستم از راه دور وجود داشته باشد کپی کنید. i- اجرای برنامه را به طوری که با دسکتاپ جلسه مشخص شده در سیستم راه دور تعامل داشته باشد. اگر هیچ جلسه مشخص نشده است، روند در جلسه کنسول اجرا می شود. h- اگر سیستم هدف ویستا یا بالاتر باشد، فرایند با علامت بالا حساب، اگر موجود باشد، اجرا می شود. l- اجرای فرایند به عنوان کاربر محدود (نوار گروه مدیران و اجازه می دهد تنها امتیازات اختصاص داده شده به گروه کاربران). در ویندوز ویستا این فرایند با Low Integrity اجرا می شود. n- زمان اتصال به رایانه های راه دور را تعیین می کند. p- رمز عبور اختیاری برای نام کاربری را مشخص می کند. اگر این را حذف کنید، از شما خواسته می شود تا یک رمز عبور

ابزار شماره ۸	
	پنهانی وارد کنید. -r نام سرویس راه دور را برای ایجاد یا تعامل با آن مشخص می کند. -s فرایند راه دور را در حساب سیستم اجرا کنید. -u نام کاربر اختیاری را برای ورود به کامپیوتر از راه دور مشخص می کند. -v فقط کپی فایل مشخص شده را در صورتی که شماره نسخه بالاتری داشته باشد یا جدیدتر از آن در سیستم راه دور باشد. -w تنظیم دایرکتوری کار فرآیند (نسبت به کامپیوتر از راه دور). -x نمایش UI در دسک تاپ امن Winlogon (فقط سیستم محلی). PsExec Direct برای اجرای برنامه بر روی کامپیوتر یا رایانه های مشخص شده تعیین شده است. اگر نام رایانه را حذف کنید، PsExec برنامه را بر روی سیستم محلی اجرا می کند، و اگر شما یک wildcard (\\ *) را مشخص کنید، PsExec این فرمان را بر روی تمام رایانه های موجود در دامنه فعلی اجرا می کند. PsExec file فرمان را بر روی هر یک از رایانه های ذکر شده در فایل اجرا خواهد کرد.

ابزار شماره ۸	
	cmd نام برنامه برای اجرای. استدلال Arguments to pass (توجه داشته باشید که مسیر فایل باید مسیر مطلق در سیستم هدف باشد).

ابزار PsGetSid

ابزار شماره ۹	
نام ابزار	PsGetside
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	PsGetsid به شما اجازه می دهد تا SID ها را به نام نمایش

ابزار شماره ۹	
	دهنده خود ببرید و بالعکس. این در حساب های داخلی، حساب های دامنه و حساب های محلی کار می کند.
نحوه ی استفاده از ابزار	Usage: psgetsid [\\computer [, computer[...] | @file\] [-u username [-p password]]] [account|SID] -u نام کاربر اختیاری را برای ورود به کامپیوتر از راه دور مشخص می کند. -p رمز عبور اختیاری برای نام کاربری را مشخص می کند. اگر این را حذف کنید، از شما خواسته می شود تا یک رمز عبور پنهانی وارد کنید. PsGetSid SID account را برای حساب کاربری مشخص شده به جای کامپیوتر گزارش می دهد. PsGetSid SID حساب برای SID مشخص شده را گزارش می دهد. computer مستقیم PsGetSid برای اجرای دستور بر روی کامپیوتر یا رایانه های مشخص شده مشخص شده است. اگر نام رایانه را حذف کنید، PsGetSid فرمان را در سیستم محلی اجرا می کند، و اگر شما یک wildcard (\\ *) را مشخص کنید، PsGetSid دستور را روی تمام رایانه های موجود در دامنه فعلی

ابزار شماره ۹	
	اجرا می کند. @file PsGetSid فرمان را بر روی هر یک از رایانه های ذکر شده در فایل اجرا خواهد کرد.

ابزار PsKill

ابزار شماره ۱۰	
نام ابزار	pskill
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	

ابزار شماره ۱۰	
	ویندوز ۲۰۰۰ / NT با ابزار خط فرمان 'kill' نمی آید. شما می توانید یکی را در کیت منابع ویندوز NT یا Win۲K دریافت کنید، اما ابزار کیت تنها می تواند فرایندهای بر روی کامپیوتر محلی را خاتمه دهد. PsKill یک ابزار kill است که نه تنها نسخه کیت Resource Kit را انجام می دهد بلکه می تواند فرآیندهای را در سیستم های از راه دور kill کند. شما حتی نباید یک مشتری را در رایانه مقصد نصب کنید تا از PsKill برای پایان دادن به یک فرایند از راه دور استفاده کنید.
نحوه ی استفاده از ابزار	Usage: pskill [-] [-t] [\\computer [-u username] [-p password]] <process name | process id> - گزینه های پشتیبانی شده را نمایش می دهد. -ت فرایند و فرزندانش را از بین ببر \\ رایانه رایانه ای را مشخص می کند که در آن فرایندی که می خواهید پایان دهید، اجرا می شود. کامپیوتر از راه دور باید از طریق محله شبکه NT قابل دسترسی باشد. -u username اگر میخواهید یک فرایند را در یک سیستم از راه دور kill کنید و حساب کاربری که در آن اجرا می کنید دارای امتیازات اداری در سیستم راه دور نیست، پس باید به عنوان یک مدیر با استفاده از این گزینه خط فرمان وارد شوید..

ابزار شماره ۱۰	
	-p password این گزینه به شما اجازه می دهد رمز ورود را در خط فرمان مشخص کنید تا بتوانید از PsList از فایل های دسته ای استفاده کنید. اگر نام یک حساب کاربری را مشخص کرده اید و گزینه -p را حذف کنید PsList شما را به صورت تعاملی برای رمز عبور راهنمایی می کند. process id شناسه فرایند فرایندی را که می خواهید killشود را مشخص کنید مشخص می کند. نام فرآیند نام فرآیند فرآیند یا پردازشهایی را که میخواهید killکنید مشخص می کند.

ابزار PsList

ابزار شماره ۱۱	
نام ابزار	PsList
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶

ابزار شماره ۱۱	
معرفی این ابزار	کلید اختصاری حافظه تمام مقادیر حافظه در KB نمایش داده می شود. Pri: اولویت Thd: تعداد موضوعات Hnd: تعداد دستگیره ها VM: حافظه مجازی WS: مجموعه کار Priv: حافظه مجازی خصوصی Priv Pk: پیک مجازی حافظه مجازی Faults: گسل های صفحه NonP: استخر غیر اختصاصی Page : Pooled Paged Cswtch: کلید های متن PsList بخشی از یک مجموعه رو به رشد از ابزار خط فرمان Sysinternals است که به مدیریت سیستم های محلی و از راه دور به نام PsTools کمک می کند. ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و خروجی را به

ابزار شماره ۱۱	
	صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با سیستم های ویندوز NT و نسخه های بعدی سازگاری کامل دارند .این ابزارها هرچند قابلیت اجرا بر روی سیستم های ریموت را دارند ولی در مقابل قابلیت استفاده به صورت لوکال و در شبکه محلی را نیز دارند. مجموعه ابزار pstools نیاز به نصب ندارند. ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری

ابزار شماره ۱۱	
	PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر انتخاب شده. PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

ابزار PsService

ابزار شماره ۱۲	
نام ابزار	PsService
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip

ابزار شماره ۱۲	
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	PsServiceبخشی از یک مجموعه رو به رشد از ابزار خط فرمان Sysinternalsاست که به مدیریت سیستم های محلی و از راه دور به نام PsTools کمک می کند PsService یک مرورگر سرویس و کنترل کننده برای ویندوز است. PsService همانند ابزار SC که در کیت منابع Windows NT و Windows ۲۰۰۰ موجود است، وضعیت، پیکربندی و وابستگی یک سرویس را نمایش می دهد و به شما این را امکان می دهد تا آنها را شروع، متوقف، مکث، و راه اندازی مجدد کنید. بر خلاف ابزار SC، PsService شما را قادر می سازد تا به یک سیستم از راه دور با استفاده از یک حساب کاربری دیگر، برای مواردی که حساب کاربری که شما آن را اجرا می کنید مجوز های لازم را در سیستم از راه دور ندارد، وارد شوید. PsService شامل یک سرویس جستجوی منحصر بفردی است که نمونه های فعال سرویس را در شبکه شما شناسایی می کند. شما می توانید از ویژگی جستجو استفاده کنید. ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و

ابزار شماره ۱۲	
	خروجی را به صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با سیستم های ویندوز NT و نسخه های بعدی سازگاری کامل دارند .این ابزارها هرچند قابلیت اجرا بر روی سیستم های ریموت را دارند ولی در مقابل قابلیت استفاده به صورت لوکال و در شبکه محلی را نیز دارند. مجموعه ابزار pstoolsنیاز به نصب ندارند. ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری

ابزار شماره ۱۲	
	PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر انتخاب شده. PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

ابزار PsSuspend

ابزار شماره ۱۳	
نام ابزار	PsSuspend

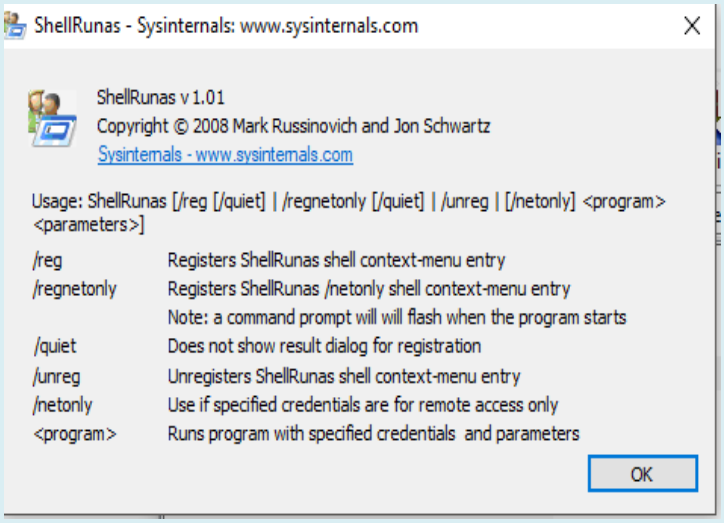
ابزار شماره ۱۳	
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	PsSuspend به شما اجازه می دهد تا پروسه ها را در سیستم محلی یا از راه دور متوقف کنید، که در مواردی که فرایند یک منبع (مثلا شبکه، پردازنده یا دیسک) را مصرف می کند، مطلوب است که می خواهید از پردازش های مختلف استفاده کنید. به جای از بین بردن فرآیند که منابع را مصرف می کند،فرآیند را به حالت تعلیق در می آورد تا آن را در برخی موارد بعد از مدتی ادامه دهد. ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و خروجی را به صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با سیستم های ویندوز NT و نسخه های بعدی سازگاری کامل دارند .این ابزارها هرچند قابلیت اجرا بر روی سیستم های ریموت را دارند ولی در مقابل قابلیت استفاده به صورت لوکال و در شبکه محلی را نیز دارند. مجموعه ابزار pstools نیاز به نصب ندارند.

ابزار شماره ۱۳	
	ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر انتخاب شده. PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است

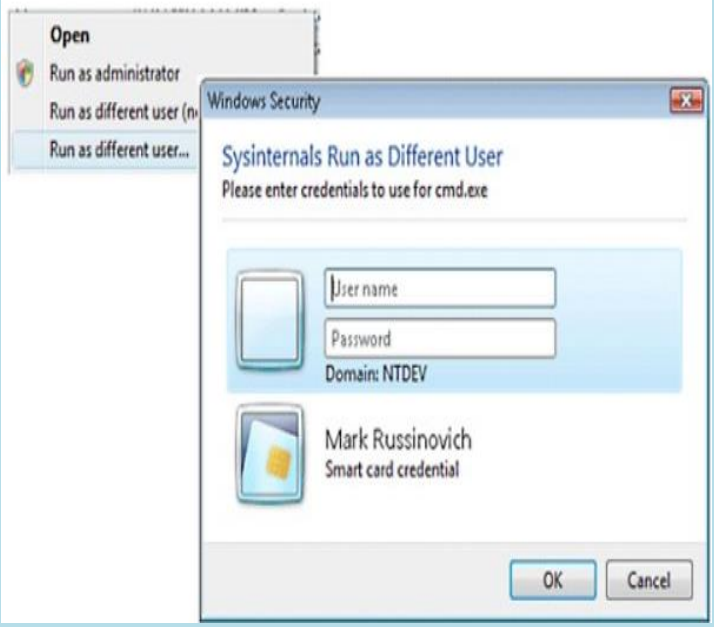
ابزار شماره ۱۳	
نحوه ی استفاده از ابزار	اجرای PsSuspend با یک شناسه فرآیند، آن را هدایت می کند تا فرایند آن شناسه را در رایانه محلی متوقف کند یا آن را ادامه دهد. اگر نام یک فرایند را مشخص می کنید، PsSuspend متوقف خواهد شد و یا تمام پروسه هایی را که دارای نام آن هستند، از سر می گیرند. هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

ابزار ShellRunas

ابزار شماره ۱۴	

ابزار شماره ۱۴	
نام ابزار	ShellRunas
لینک دانلود	https://download.sysinternals.com/files/ShellRunas.zip
تاریخ انتشار	February ۲۸, ۲۰۰۸
معرفی این ابزار	ابزار command-line مناسب برای راه اندازی برنامه های تحت حساب های مختلف است، اما اگر شما یک کاربر اکسپلورر هستید، مناسب نیست. ShellRunas عملکرد مشابهی با Runes فراهم می کند تا برنامه ها را به عنوان کاربر دیگری از طریق یک ورودیcontext-menu مناسب اجرا کند. 
نحوه ی استفاده از ابزار	به صورت شکل زیر برنامه را اجرا کرده و از شکل دستورات زیر استفتده کنید

ابزار شماره ۱۴	

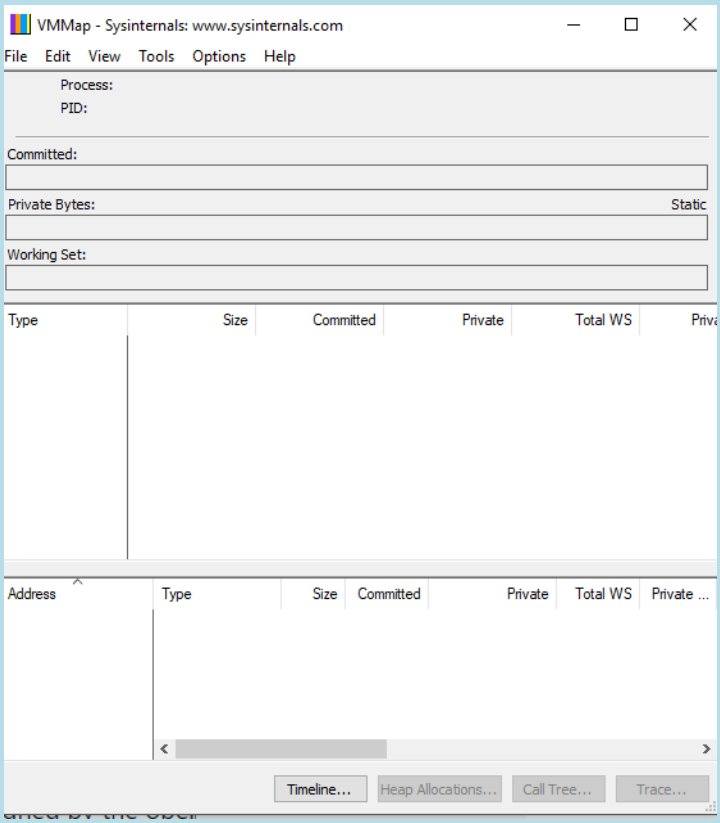


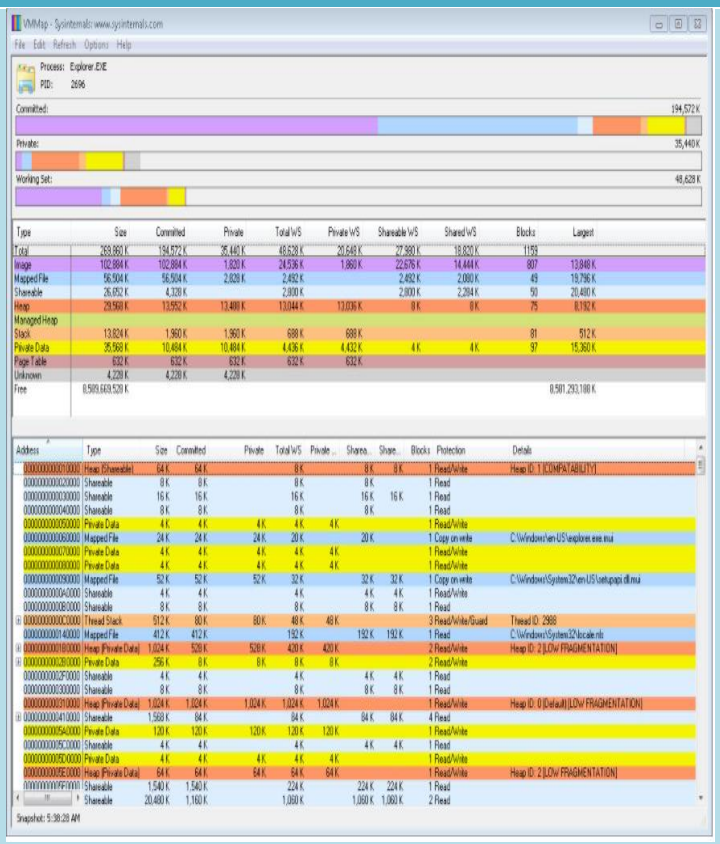
دستورات کاربردی

Parameter	Description
/reg	Registers ShellRunas shell context-menu entry
/regnetonly	Registers Shell /netonly context-menu entry **Note:** a command prompt will flash when the program starts
/unreg	Unregisters ShellRunas shell context-menu entry
/quiet	Register or unregisters ShellRunas shell context-menu entry without result dialog
/netonly	Use if specified credentials are for remote access only
<program>	Runs program with specified credentials and parameters

ابزار VMMap

ابزار شماره ۱۵	
نام ابزار	VMMap
لینک دانلود	https://download.sysinternals.com/files/VMMap.zip
تاریخ انتشار	July ۲۰, ۲۰۱۵
معرفی این ابزار	VMMap یک ابزار تجزیه و تحلیل حافظه مجازی و فیزیکی است. این نشان می دهد که تقسیم یک نوع حافظه مجازی متعهد فرآیند و همچنین مقدار حافظه فیزیکی (مجموعه کار) تعیین شده توسط سیستم عامل به آن نوع است. علاوه بر نمایشگرهای گرافیکی استفاده از حافظه، VMMap همچنین اطلاعات خلاصه و یک نقشه حافظه پردازش دقیق را نشان می دهد. قابلیت های قدرتمند فیلتر کردن و تازه سازی به شما این امکان را می دهد که منابع استفاده از حافظه فرایند و هزینه حافظه از ویژگی های برنامه را شناسایی کنید. VMMap علاوه بر نمایش های انعطاف پذیر برای تجزیه و تحلیل فرآیندهای زنده، از داده ها در قالب های مختلف پشتیبانی می کند، از جمله یک فرمت بومی که تمام اطلاعات را حفظ می کند تا شما بتوانید آن را بارگذاری کنید. همچنین شامل گزینه های خط فرمان است که سناریوهای اسکریپتی را فعال می کنند. VMMap ابزار ایده آل برای توسعه دهندگان است که مایل به

ابزار شماره ۱۵	
	درک و بهینه سازی استفاده از منابع حافظه برنامه خود هستند.
نحوه ی استفاده از ابزار	نرم افزار را از لینک داده شده دانلود کنید و سپس از حالت فرشده در بیارید و فایل exe آن را اجرا کنید 

ابزار شماره ۱۵	
	

دسته چهارم Sysinternals Security Utilities

معرفی ابزارهای موجود در دسته چهارم

ابزار Autologon

ابزار شماره ۱	
نام ابزار	AutoLogon
لینک دانلود	https://download.sysinternals.com/files/AutoLogon.zip
تاریخ انتشار	August ۲۹, ۲۰۱۶
معرفی این ابزار	Autologon شما را قادر می سازد به راحتی مکانیزم Autologon ساخته شده در ویندوز را پیکربندی کنید. به جای انتظار یک کاربر برای وارد کردن نام و رمز عبور خود، ویندوز با استفاده از اعتبارهایی که با Autologon وارد می کنید، که در رجیستری رمزگذاری شده اند، برای وارد کردن کاربر مشخص شده به صورت خودکار انجام می پزیرد.
نحوه ی استفاده از ابزار	Autologon برای استفاده بسیار آسان است. فقط autologon.exe را اجرا کنید، گفتگو را پر کنید و روی Enable کلیک کنید. برای غیرفعال کردن ورود خودکار، ضربه غیرفعال را فشار دهید. همچنین، اگر کلید shift قبل از اینکه یک سیستم Autologon را اجرا کند پایین نگه دارد، Autologon برای آن

ابزار شماره ۱	
	logon غیرفعال خواهد شد. شما همچنین می توانید نام کاربری، دامنه و رمز عبور را به عنوان استدلال خط فرمان ارسال کنید.

ابزار LogonSessions

ابزار شماره ۲	

ابزار شماره ۲	
نام ابزار	logonSessions
لینک دانلود	https://download.sysinternals.com/files/logonSessions.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	اگر فکر می کنید زمانی که شما به یک سیستم وارد می شوید، تنها یک جلسه ورود به سیستم وجود دارد، این ابزار شما را متعجب خواهد کرد. این فهرست جلسات ورود به سیستم فعال است و اگر شما گزینه -p را مشخص کنید، فرایندهای در حال اجرا در هر جلسه را نمایش خواهد داد.
نحوه ی استفاده از ابزار	این ابزار به صورت خط فرمان اجرا می شود و می توانیم از هر یک ازین دستورات استفاده کنیم.

Parameter	Description
-c	Print output as CSV.
-ct	Print output as tab-delimited values.
-p	List processes running in logon session.

ابزار شماره ۲	

```
C:\\&gt;logonsessions -p
…
\[13\] Logon session 00000000:6a6d6160:
    User name:    NTDEV\markruss
    Auth package: Kerberos
    Logon type:   RemoteInteractive
    Session:      1
    Sid:          S-1-5-21-397955417-626881126-188441444-3615555
    Logon time:   7/2/2015 6:05:31 PM
    Logon server: NTDEV-99
    DNS Domain:   NTDEV.CORP.MICROSOFT.COM
    UPN:          markruss@ntdev.microsoft.com
    15368: ProcExp.exe
    17528: ProcExp64.exe
    13116: cmd.exe
    17100: conhost.exe
     6716: logonsessions.exe
```

ابزار NewSID

ابزار شماره ۳	
نام ابزار	NewSID
لینک دانلود	NewSID قدیمی شده است و دیگر برای دانلود در دسترس نیست
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	NewSID برنامه ای است که ما برای تغییر SID رایانه ای توسعه دادیم. ابتدا یک SID تصادفی برای کامپیوتر تولید می کند و به منظور به روز رسانی نمونه هایی از SID رایانه موجود در رجیستری و در توصیف های امنیتی فایل، جایگزین رخدادهای با SID جدید می شود. NewSID نیاز به امتیازات اداری برای اجرا دارد. این دو عملکرد دارد: تغییر SID و تغییر نام کامپیوتر.
نحوه ی استفاده از ابزار	دستور: newsid /a [newname] NewSID را بدون prompting انجام داده و نام رایانه را به newnameتغییر دهید و اگر همه چیز درست باشد، کامپیوتر را دوباره راه اندازی کنید. NewSID با خواندن SID کامپیوتر موجود آغاز می شود. SID

ابزار شماره ۳	
	کـامپیوتر در SECURITY \ SAM \ Domains \ Account ذخیره می شود. این کلید دارای یک مقدار با نام F و یـک مقـدار با نام .Vمقدار V یک مقدار باینری است کـه SID کـامپیوتر در آن در انتهای داده هـای خـود جاسـازی شـده اسـت. NewSID تضمین می کند که این SID در فرمت استاندارد (۳ زیربنای ۳۲ بیتی پیش از سه فیلد اختیاری ۳۲ بیتی است).

ابزار PsLoggedOn

ابزار شماره ۴	
نام ابزار	PsLoggedOn
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	PsLoggedOn بخشی از یک مجموعه رو بـه رشـد از ابـزار خـط فرمان Sysinternals است که به مدیریت سیستم هـای محلـی و از راه دور به نام PsTools کمک می کند. با دستور ("session net") شما می توانید تعیین کنید که چه کسی از منابع خـود در رایانـه محلی استفاده می کند، اما هیچ راه درونی برای تعیین اینکه چـه کسی از منابع کامپیوتر از راه دور استفاده می کند وجـود نـدارد. علاوه بر این، NT بدون ابزار برای دیدن افرادی که بـه کـامپیوتر وارد شده اند، به صورت محلی یا از راه دور استفاده می شود. اگـر نام کاربری را به جای یک رایانه مشـخص کنیـد، PsLoggedOn کامپیوترها را در محدوده شبکه جستجو می کند و بـه شـما مـی گوید که آیا کاربر در حال ورود به سیستم است یا خیر. تعریف PsLoggedOn از یک کاربر به صـورت محلـی وارد شـده است که پروفایل خود را به رجیستری بارگیری می کند، بنابراین PsLoggedOn تعیین می کند که چه کسی وارد سیسـتم شـده است، با اسکن کلیدی زیر کلید .HKEY_USERSبرای هر کلید

ابزار شماره ۴	
	که نامی است که کاربر) SIDشناسه امنیتی) است، PsLoggedOn نام کاربری مربوطه را نمایش می دهد و آن را نمایش می دهد. PsLoggedOn با استفاده از API NetSessionEnum برای تعیین اینکه چه کسی از طریق اشتراک منابع به یک کامپیوتر وارد شده است. توجه داشته باشید که PsLoggedOn شما را به عنوان از طریق اشتراک منابع به کامپیوترهای راه دور که شما پرس و جو پرس و جو از طریق به اشتراک گذاشته شده است به دلیل ورود به سیستم برای PsLoggedOn برای دسترسی به رجیستری سیستم از راه دور. ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و خروجی را به صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با سیستم های ویندوز NT و نسخه های بعدی سازگاری کامل دارند .این ابزارها هرچند قابلیت اجرا بر روی سیستم های ریموت را دارند ولی در مقابل قابلیت استفاده به صورت لوکال و در شبکه محلی را نیز دارند. مجموعه ابزار pstools نیاز به نصب ندارند.

ابزار شماره ۴	
	ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر انتخاب شده. PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است

ابزار شماره ۴	
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

ابزار PsLogList

ابزار شماره ۵	
نام ابزار	PsLogList
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	PsLogList مانند EventViewer ساخته شده در ویندوز NT / K۲ و elogdump کیت منابع است، از API Event Log استفاده می کند که در Windows Platform SDK مستند شده است. PsLogList ماژول های منبع پیام را در سیستم ذخیره می کند که در آن ورودی رویداد مشاهده می شود و به طور صحیح نمایش پیام های رویداد را نمایش می دهد. PsLogList بخشی از یک مجموعه رو به رشد از ابزار خط فرمان Sysinternals است که به مدیریت سیستم های محلی و از راه دور به نام PsTools کمک می کند. ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و خروجی را به صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با سیستم های ویندوز NT و نسخه های بعدی سازگاری

ابزار شماره ۵	
	کامل دارند .این ابزارها هرچند قابلیت اجرا بر روی سیستم های ریموت را دارند ولی در مقابل قابلیت استفاده به صورت لوکال و در شبکه محلی را نیز دارند. مجموعه ابزار pstools نیاز به نصب ندارند. ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر

ابزار شماره ۵	
	انتخاب شده. PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

ابزار RootkitRevealer

ابزار شماره ۶	
نام ابزار	RootkitRevealer
لینک دانلود	https://download.sysinternals.com/files/RootkitRevealer.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	RootkitRevealer یک ابزار پیشرفته ریشه زایی است. این پروتکل بر روی ویندوز ۳۲XP بیتی و ویندوز سرور ۲۰۰۳ (۳۲ بیتی) اجرا می شود و خروجی آن لیست اختلالات API رجیستری و پرونده های سیستم است که ممکن است یک حالت کاربر یا rootkit حالت kernel را نشان دهد. RootkitRevealer با موفقیت بسیاری از روت کیت های پایدار از جمله AFX، Vanquish و HackerDefender را شناسایی می کند (توجه داشته باشید: RootkitRevealer برای شناسایی روت کیت هایی مانند Fu نیست). دلیل دیگری که نسخه خط فرمان دیگر وجود ندارد این است که نویسندگان بدافزار با هدف استفاده از اسکن RootkitRevealer با استفاده از نام اجرایی خود شروع کرده اند. بنابراین ما RootkitRevealer را به روز کردیم تا اسکن آن را از یک کپی از خود به صورت تصادفی که به عنوان یک سرویس ویندوز اجرا می شود اجرا کنیم. این نوع اعدام برای یک رابط خط فرمان مفید نیست. توجه داشته باشید که می توانید از گزینه های خط فرمان

ابزار شماره ۶	
	برای اجرای یک اسکن خودکار با نتایج ورود به یک فایل استفاده کنید که معادل رفتار نسخه خط فرمان است.
نحوه ی استفاده از ابزار	از آنجایی که روت کیت های پایدار با تغییر API ها کار می کنند به طوری که مشاهده سیستم با استفاده از API ها از دیدگاه واقعی در ذخیره سازی متفاوت است، RootkitRevealer نتایج اسکن سیستم را در بالاترین سطح با آن در پایین ترین سطح مقایسه می کند. بالاترین سطح API ویندوز است و پایین ترین سطح محتویات خام یک حجم فایل سیستم یا پرونده رجیستری است. دستورات راه اندازی اسکن خودکار: Parameter — Description -a — Automatically scan and exit when done. -c — Format output as CSV. -m — Show NTFS metadata files. -r — Don't scan the Registry.

ابزار Sysmon

ابزار شماره ۷	
نام ابزار	Sysmon
لینک دانلود	https://download.sysinternals.com/files/Sysmon.zip
تاریخ انتشار	September ۱۱, ۲۰۱۷
معرفی این ابزار	مانیتور سیستم Sysmon سرویس ویندوز دستگاه است که پس از نصب بر روی یک سیستم، در سیستم راه اندازی مجدد برای نظارت و ثبت فعالیت سیستم و ورود به سیستم و رویداد ویندوز باقی می ماند. این اطلاعات دقیق در مورد فرایند، اتصالات شبکه و تغییرات در زمان ایجاد فایل فراهم میشود و با جمع آوری حوادث آن با استفاده از مجموعه رویداد ویندوز یا عوامل SIEM تولید می شود و سپس آنها را تجزیه و تحلیل می کند، می توانید فعالیت های مخرب یا غیرعادی را شناسایی کنید و بدانید که چگونه مزاحمان و بدافزار در شبکه شما کار می کنند. توجه داشته باشید که Sysmon تجزیه و تحلیل رویدادهایی که تولید می کند را ارائه نمی دهد و همچنین تلاش نمی کند که خود را از مهاجمان محافظت کند یا پنهان کند.

ابزار شماره ۷	

Sysmon شامل قابلیت های زیر است:

ایجاد فرآیند با خط فرمان کامل برای هر دو فرآیند فعلی و والدین ایجاد می کند.

فایل های تصویر فرایند را با استفاده از ۱SHA (به طور پیش فرض)، ۵MD، ۲۵۶SHA یا IMPHASH ضبط می کند.

هش ها چندگانه را می توان در یک زمان استفاده کرد.

شامل فرآیند GUID در فرآیند ایجاد حوادث برای اجازه همبستگی حوادث حتی زمانی که ویندوز مجدد استفاده از شناسه فرایند.

ابزار شماره ۷	
	شامل یک GUID جلسه در هر رویداد برای اجازه دادن به همبستگی حوادث در یک جلسه Logon مشابه. بارگیری رانندگان یا DLL ها را با امضاهای و هشهای خود وارد می کند. اختیاری logs اتصالات شبکه، از جمله روند منبع هر اتصال، آدرس های IP، شماره های پورت، نام های میزبان و نام های پورت. تغییرات در زمان ایجاد فایل را تشخیص می دهد تا زمانی که یک فایل واقعا ایجاد شود. اصلاح فایل ایجاد زمانبندی ها یک تکنیک است که معمولا توسط نرم افزارهای مخرب برای پوشش آهنگ هایش استفاده می شود. در صورت تغییر در رجیستری، پیکربندی مجدد را به طور خودکار بارگذاری کنید. فیلتر فیلترینگ برای اضافه کردن یا حذف رویدادهای خاص به صورت پویا رویدادها را از ابتدای فرآیند بوت ایجاد می کند تا فعالیت های ناشی از پیچیده ترین نرم افزارهای مخرب kernel mode را ضبط کند.
نحوه ی استفاده از ابزار	دستورات کاربردی زیر برای نصب uninstall و....استفاده می شود

ابزار شماره ۷	

که برای هر دستور توضیح لازم آورده شده است.

Parameter	Description
-c	Update configuration of an installed Sysmon driver or dump the current configuration if no other argument is provided. Optionally take a configuration file.
-h	Specify the hash algorithms used for image identification (default is SHA1). It supports multiple algorithms at the same time. Configuration entry: HashAlgorithms.
-i	Install service and driver. Optionally take a configuration file.
-l	Log loading of modules. Optionally take a list of processes to track.
-m	Install the event manifest (done on service install as well).
-n	Log network connections. Optionally take a list of processes to track.
-r	Check for signature certificate revocation. Configuration entry: CheckRevocation.
-s	Print configuration schema definition.
-u	Uninstall service and driver.

دسته پنجم Sysinternals System Information Utilities

معرفی ابزارهای موجود در دسته پنجم

ابزار Coreinfo

۲ابزار شماره	
نام ابزار	Coreinfo
لینک دانلود	https://download.sysinternals.com/files/Coreinfo.zip
تاریخ انتشار	August ۱۸, ۲۰۱۴
معرفی این ابزار	یک ابزار خط فرمانی است که پردازنده منطقی را به پردازنده فیزیکی نگاشت میکند. گره NUMA و سوکت که در آن هستند، و همچنین حافظه پنهان اختصاص داده شده به هر پردازنده منطقی. این سیستم از تابع GetLogicalProcessorInformation ویندوز برای به دست آوردن این اطلاعات استفاده می کند و آن را روی صفحه نمایش می دهد و یک نگاشت را به یک پردازنده منطقی با ستاره نمایش می دهد، به عنوان مثال'*' Coreinfo برای به دست آوردن اطلاعات درمورد پردازنده و توپولوژی cach در سیستم مفید است.
نحوه ی استفاده از ابزار	برای هر منبع، یک نقشه از پردازنده های قابل مشاهده OS را که

۲ابزار شماره	
	با منابع مشخص شده مطابقت دارند نشان می دهد، '*' نشان دهنده پردازنده های قابل اجرا است. coreinfo [-c] [-f] [-g] [-l] [-n] [-s] [-m] [-v] انواع پارامترها ** c-**: تخلیه اطلاعات در هسته ها. f-: تخلیه ویژگی اطلاعات هسته g-: تخلیه اطلاعات گروه ها. ** L- ** تخلیه اطلاعات پیمایش در cach ها. n- اطلاعات مربوط به گره NUMA را بارگیری کنید. s- تخلیه اطلاعات سوکت. m- تخلیه هزینه دسترسی NUMA. v- فقط ویژگی های مرتبط با مجازی سازی را از جمله پشتیبانی از ترجمه آدرس سطح دوم را تخلیه میکند (در سیستم های اینتل نیاز به دسترسی مدیر وجود دارد). تمام گزینه های غیر از v- به طور پیش فرض انتخاب می شوند. خروجی Coreinfo به صورت XML است.

ابزار LiveKd

۳ابزار شماره	
نام ابزار	LiveKd
لینک دانلود	https://download.sysinternals.com/files/LiveKD.zip
تاریخ انتشار	May ۱۶, ۲۰۱۷
معرفی این ابزار	به کارگیری Microsoft kernel debugger برای مطالعه سیستم های فعال این ابزار اجازه می دهد تا KD و Windbg debugers کرنل مایکروسافت را که بخشی از بسته های Debugging Tools Windows هستند را به صورت محلی بر روی سیستم عامل فعال اجرا کنید. تمام فرمان های دیباگر را که بر روی فایل های خراب داخل سیستم کار میکنند ، اجرا کنید. در حالی که آخرین نسخه های Windbg و Kd دارای قابلیت مشابه در ویندوز ویستا و سرور ۲۰۰۸ هستند، LiveKD قابلیت های بیشتری از قبیل مشاهده پشته های موضوع با دستور thread را فراهم می کند.
نحوه ی استفاده از ابزار	-hv مشخص کننده نام یا GUID Hyper-V VM برای اشکالزدایی است. -hvd شامل صفحاتHypervisor (ویندوز ۸.۱ و بالاتر) -hvl نام و GUID ها را برای اجرای VM های Hyper-V لیست می کند. -k مسیر کامل و نام فایل تصویر اشکال زدا برای اجرا را مشخص می کند -m یک دامنه ی آینه ایجاد می کند که یک دیدگاه سازگار از حافظه ی

۳ابزار شماره	
	هسته است. فقط حافظه حالت هسته ای در دسترس خواهد بود و این گزینه ممکن است به مقدار قابل توجهی از حافظه فیزیکی موجود نیاز داشته باشد. ml-تولید مجدد زنده با استفاده از پشتیبانی بومی (ویندوز ۸.۱ و بالاتر). mp-مشخص کننده یک فرایند واحد است که محتویات حافظه حالت کاربر باید شامل یک dump انعکاس دهنده باشد. که تنها با گزینه m- موثر است. o-ذخیره فایل memory.dmp به جای راه اندازی debugger دیسک. p-هدف VM Hyper-V را متوقف می کند در حالی که LiveKd فعال است (برای استفاده با o- توصیه می شود) نام یا GUID Hyper-V VM را برای debug مشخص می کند. hvl-نام و GUID ها را برای اجرای VM های Hyper-V لیست می کند. vsym-اطلاعات اشکال زدایی طولانی مربوط به عملیات نماد load را نمایش می دهد. توجه: از Ctrl-Break برای خاتمه دادن و راه اندازی مجدد debug استفاده کنید.. به طور پیش فرض LiveKd kd.exe را اجرا می کند.

ابزار LoadOrder

۴ابزار شماره	
نام ابزار	LoadOrder
لینک دانلود	https://download.sysinternals.com/files/LoadOrder.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	سیستم لود درایور های دستگاه را در سیستم ویندوز NT یا ویندوز ۲۰۰۰ نشان می دهد. توجه داشته باشید که در درایورهای پلاگین و بازی ویندوز ۲۰۰۰ ممکن است در یک دستورالعمل متفاوت از یک محاسبه شده بارگذاری شود، زیرا درایورهای پلاگین و بازی در هنگام تشخیص و شمارش دستگاه بارگیری می شوند.
نحوه ی استفاده از ابزار	

ابزار ProcFeatures

۵ابزار شماره	
نام ابزار	ProcFeatures
لینک دانلود	——
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	ProcFeatures از کار افتاده است شده است، زیرا آخرین نسخه Coreinfo این ابزار را منسوخ کرده است. Coreinfo v۳ در حال حاضر ویژگی های پردازنده پشتیبانی شده توسط پردازنده های سیستم را نشان می دهد.
نحوه ی استفاده از ابزار	ProcFeatures از کار افتاده شده است، زیرا آخرین نسخه Coreinfo این ابزار را منسوخ کرده است. Coreinfo v۳ در حال حاضر ویژگی های پردازنده پشتیبانی شده توسط پردازنده های سیستم را نشان می دهد.

ابزار PsInfo

ابزار شماره۶	
نام ابزار	PsInfo
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	PsInfo با استفاده از API رجیستری از راه دور برای خواندن اطلاعات سیستم از رجیستری سیستم و WMI برای تعیین اینکه آیا نصب ویندوز XP فعال شده است یا خیر. PsInfo یک ابزار خط فرمان است که جمع آوری اطلاعات کلیدی در مورد سیستم ویندوز / ۲۰۰۰NT محلی یا راه دور شامل نوع نصب، ساخت هسته، سازمان ثبت شده و مالک، تعداد پردازنده ها و نوع آنها، میزان حافظه فیزیکی، نصب تاریخ سیستم می باشد. c:>> psinfo \\\\development -h -d PsInfo v1.6 - local and remote system information vi Copyright (C) 2001-2004 Mark Russinovich Sysinternals - www.sysinternals.com System information for \\\\DEVELOPMENT: Uptime: 28 days, 0 hours, 15 minutes, 12 seconds Kernel version: Microsoft Windows XP, Multiproce Product type Professional Product version: 5.1 Service pack: 0 Kernel build number: 2600

ابزار شماره۶	

```
Registered organization: Sysinternals
Registered owner: Mark Russinovich
Install date: 1/2/2002, 5:29:21 PM
Activation status: Activated
IE version: 6.0000
System root: C:\\WINDOWS
Processors: 2
Processor speed: 1.0 GHz
Processor type: Intel Pentium III
Physical memory: 1024 MB
Volume Type Format Label Size Free Free
A: Removable 0%
C: Fixed NTFS WINXP 7.8 GB 1.3 GB 16%
D: Fixed NTFS DEV 10.7 GB 809.7 MB 7%
```

```
D: Fixed NTFS DEV 10.7 GB 809.7 MB 7%
E: Fixed NTFS SRC 4.5 GB 1.8 GB 41%
F: Fixed NTFS MSDN 2.4 GB 587.5 MB 24%
G: Fixed NTFS GAMES 8.0 GB 1.0 GB 13%
H: CD-ROM CDFS JEDIOUTCAST 633.6 MB 0%
I: CD-ROM 0% Q: Remote 0%
T: Fixed NTFS Test 502.0 MB 496.7 MB 99%
OS Hot Fix Installed
Q147222 1/2/2002
Q309521 1/4/2002
Q311889 1/4/2002
Q313484 1/4/2002
Q314147 3/6/2002
Q314862 3/13/2002
```

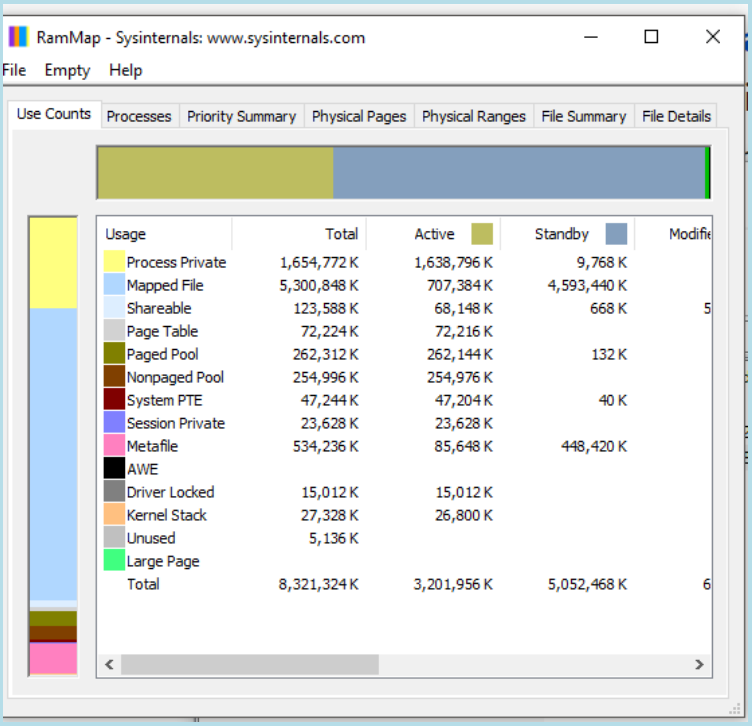
ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و خروجی را به صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با سیستم های ویندوز NT و نسخه های بعدی سازگاری کامل دارند . این ابزارها هرچند قابلیت اجرا بر روی سیستم های ریموت را دارند ولی در مقابل قابلیت استفاده به صورت لوکال و در شبکه محلی را

۶ابزار شماره	
	نیز دارند. مجموعه ابزار pstools نیاز به نصب ندارند. ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر انتخاب شده. PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی

۶ابزار شماره	
	آن چه مدت در حال اجرا بوده است
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

ابزار RAMMap

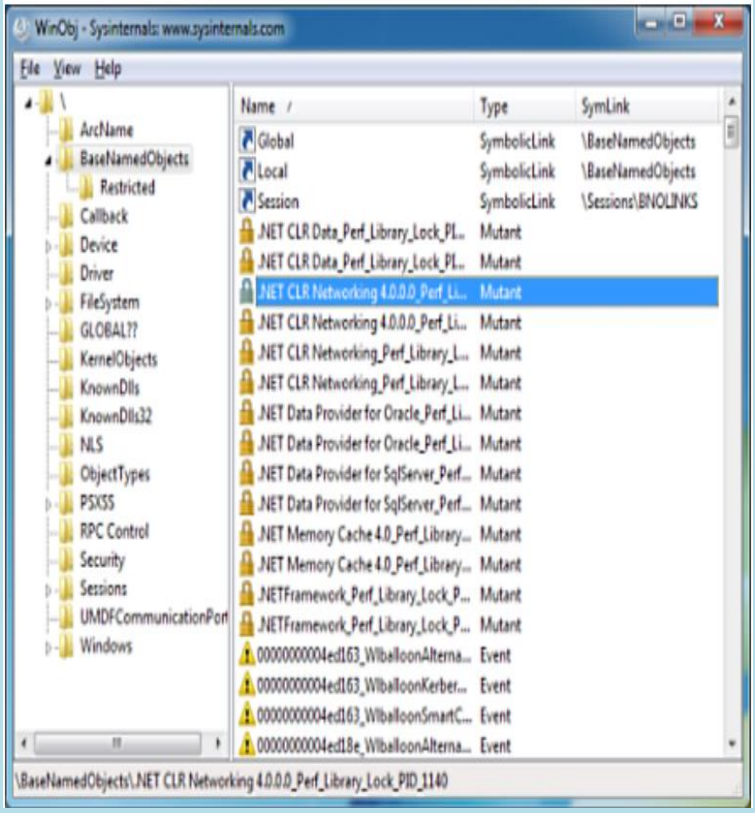
۷ابزار شماره	
نام ابزار	RAMMap
لینک دانلود	https://download.sysinternals.com/files/RAMMap.zip
تاریخ انتشار	February ۲, ۲۰۱۶
معرفی این ابزار	آیا تا کنون فکر کرده اید دقیقا چگونه اختصاص حافظه فیزیکی، اطلاعات ذخیره شده در حافظه رم و یا مقدار رم در هسته و درایور دستگاه استفاده می شود؟ RAMMap پاسخ به این سوالات را آسان می کند. RAMMap ابزار پیشرفته استفاده از حافظه فیزیکی برای ویندوز ویستا و بالاتر است. این اطلاعات استفاده را به شیوه های مختلف در چند زبانه مختلف ارائه می کند: Use Counts: خلاصه استفاده بر اساس نوع و لیست صفحات Processes: حجم کار اندازه پردازش Priority Summary: اندازه فهرست های آماده به کار اولویت بندی شده است Physical Pages: استفاده از هر صفحه برای تمام حافظه فیزیکی Physical Ranges: آدرس های حافظه فیزیکی File Summary: داده فایل در RAM توسط فایل File Details: صفحات فیزیکی فردی توسط فایل
نحوه ی استفاده از	نرم افزار را از لینک داده شده دانلود کنید سپس از حالت فشرده در

ابزار شماره ۷	
ابزار	بیاورید و فایل exe. آن را اجرا کنید 

ابزار WinObj

ابزار شماره ۸	

۸ابزار شماره	
نام ابزار	WinObj
لینک دانلود	https://download.sysinternals.com/files/WinObj.zip
تاریخ انتشار	February ۱۴, ۲۰۱۱
معرفی این ابزار	WinObj یک ابزار ضروری است اگر شما مدیر سیستم مربوط به امنیت، هستید این نرم افزار برای شما بسیار مفید است. WinObj بسیاری از object types را درک می کند. سرانجام، نسخه ۲.۰ WinObj دارای پیشرفت های در رابط کاربر است، می داند که چگونه object دستگاه را باز کند، و به شما اجازه می دهد اطلاعات مربوط به امنیت object را با استفاده از ویراستاران امنیت ملی NT مشاهده و تغییر دهید.
نحوه ی استفاده از ابزار	کامپوننت راننده دستگاه برای WinObj وجود ندارد، بنابراین شما می توانید آن را مانند هر برنامه ۳۲Win اجرا کنید.

۸ابزار شماره	
	

دسته ششم Sysinternals Miscellaneous Utilities

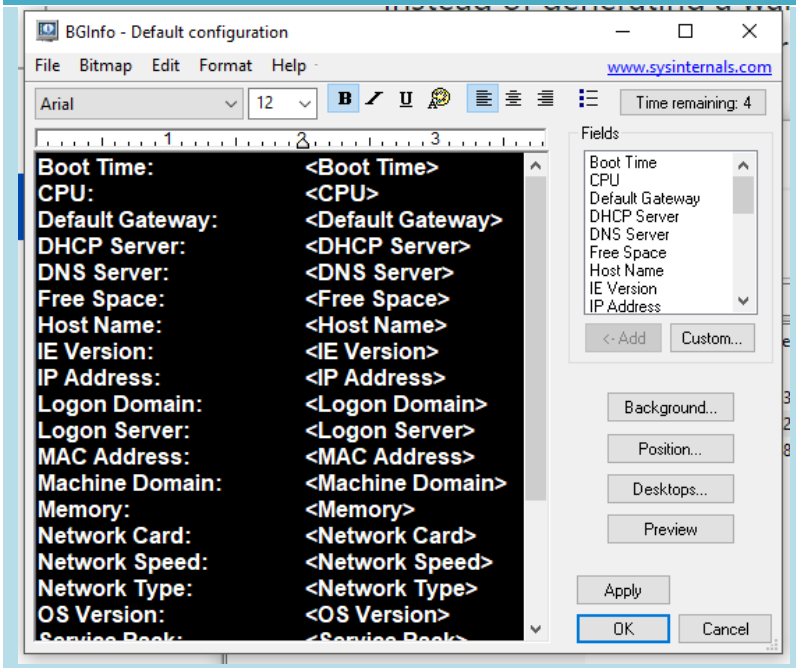
معرفی ابزارهای موجود در دسته ششم

ابزار BgInfo

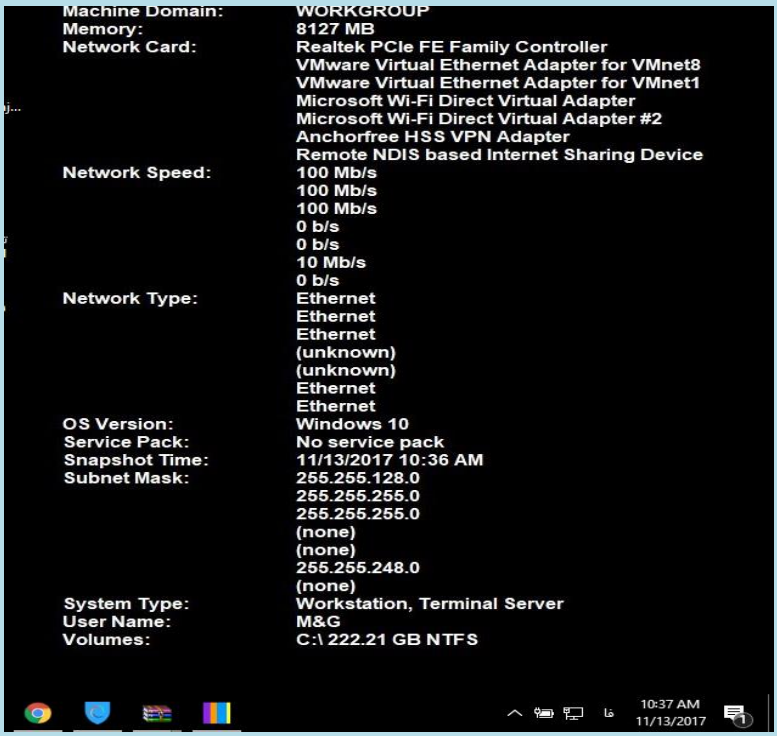
ابزار شماره ۱	

ابزار شماره ۱	
نام ابزار	BGInfo
لینک دانلود	https://download.sysinternals.com/files/BGInfo.zip
تاریخ انتشار	May ۱۶, ۲۰۱۷
معرفی این ابزار	جنبه های مهمی از پیکربندی سیستم، مانند نام، آدرس IP یا نسخه سیستم عامل، را نمایش می دهد.اگر شما چندین رایانه را مدیریت میکنید، احتمالا به BGInfo نیاز دارید. این به طور خودکار اطلاعات مربوط به یک کامپیوتر ویندوز را در پسزمینه دسک تاپ مانند نام رایانه، آدرس IP، نسخه سرویس بسته و غیره نمایش می دهد. شما می توانید هر زمینه و همچنین رنگ فونت و پس زمینه را ویرایش کنید و می توانید آن را در پوشه راه اندازی خود قرار دهید یا حتی آن را پیکربندی کنید تا به عنوان پس زمینه برای صفحه ورود به سیستم نمایش داده شود.
نحوه ی استفاده از ابزار	نرم افزار را از لینک داده شده دانلود کنید و از حالت فشرده در بیاورید آنگاه فایل exe. را اجرا کنید سپس با شکل زیر مواجه خواهید شد.

ابزار شماره ۱	



بازدن دکمه یokاطلاعات سیتسم شما را روی صفحه ی نمایش مانیوتر نمایش خواهد داد



ابزار BlueScreen Screen Saver

ابزار شماره ۲	
نام ابزار	BlueScreen
لینک دانلود	https://download.sysinternals.com/files/BlueScreen.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	یکی از رنگ های ترسناک در جهان NT آبی است. صفحه نمایش آبی صفحه مرگ BSOD است در هر زمان که چیزی به اشتباه رخ داده است، بر روی سیستم NT ظاهر می شود. Bluescreen محافظ صفحه ای است که نه تنها به درستی BSOD را تقلید می کند، بلکه صفحه های راه اندازی را که در طول بوت سیستم دیده می شود، شبیه سازی می کند. در نصب NT ۴.۰، chkdsk از درایوهای دیسک با اشتباهات شبیه سازی می شود! در ویندوز ۲۰۰۰، ویندوز ۹۵ و ویندوز ۹۸ این صفحه نمایش پلاگین راه اندازی ویندوز ۲۰۰۰ را به همراه باند پیشرفت چرخشی و به روز رسانی کنترل پیشرفت ارائه می دهد! در ویندوز ایکس پی و ویندوز سرور ۲۰۰۳ ویندوز ایکس پی / سرور ۲۰۰۳ صفحه نمایش چلپ چلوپ شدن با نوار پیشرفت را ارائه می دهد!

ابزار شماره ۲	
نحوه ی استفاده از ابزار	توجه داشته باشید: قبل از اینکه بتوانید Bluescreen را روی ویندوز ۹۵ یا ۹۸ اجرا کنید، باید \ system \ ntoskrnl.exe ۳۲winnt را از یک سیستم ویندوز ۲۰۰۰ به دایرکتوری Windows خود کپی کنید. به سادگی BLUESCRN.SCR Sysinternals را در دایرکتوری ۳۲system خود در صورتی که در K۲Windows NT و یا System Windows است دایرکتوری در ویندوز ۹۵ یا ۹۸ کپی کنید، روی دسکتاپ راست کلیک کنید تا محاورهای تنظیمات نمایش داده شود و سپس Screen Saver برگه از لیست کشویی برای پیدا کردن Sysinternals Bluescreen استفاده کنید و آن را به عنوان محافظ صفحه نمایش جدید خود اعمال کنید. دکمه "تنظیمات" را برای فعال کردن فعالیت دیسک جعلی انتخاب کنید،

ابزار Ctrl۲Cap

ابزار شماره ۳	
نام ابزار	Ctrl۲Cap
لینک دانلود	https://download.sysinternals.com/files/Ctrl۲Cap.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	cap۲Ctrl یک driver دستگاه kernel-mode است که class driver کلید صفحه سیستم را فیلتر می کند تا کارکترهای caps-lock را به کاراکترهای کنترل تبدیل کند. برای افرادی که به NT از یونیکس مهاجرت می کنند استفاده می شود. کلید کنترل در جایی که کلید caps-lockبر روی صفحه کلید کامپیوتر استاندارد است، استفاده می شود، بنابراین یک ابزار مانند این برای بهبود وضعیت ضروری است.
نحوه ی استفاده از ابزار	cap۲Ctrl را اجرا کنید و دستور install۲ctrl / cap را از دایرکتوری که فایلهای cap۲Ctrl را از حالت فشرده خارج کرده اید، نصب کنید. برای حذف ابزار از دستور (uninstall / cap۲ctrl)استفاده کنید.

ابزار DebugView

ابزار شماره ۴	
نام ابزار	DebugView
لینک دانلود	https://download.sysinternals.com/files/DebugView.zip
تاریخ انتشار	December ۴, ۲۰۱۲
معرفی این ابزار	رهگیری DbgPrint device drivers و .OutputDebugString این برنامه به شما اجازه می دهد تا بـه مشـاهده و ضـبط output debug session بر روی کامپیوتر های محلی و یا اینترنت(بدون debuggerفعال)بپردازید. DebugView یک برنامـه کـاربردی اسـت کـه بـر روی خروجـی اشکال زدایی(debug) در سیستم محلی خود یا هـر رایانـه ای کـه می توانید از طریق TCP / IP به آن دسترسی پیدا کنیـد، نظـارت کنید. این قابلیت نمایش درهر دو حالت mode هسته و خروجـی اشکال زدایی Win۳۲ وجوددارد، بنابراین شما نیـاز بـه debugger برای گرفتن خروجی debug برنامه های خود یـا درایـور دسـتگاه ندارید، همچنین نیازی به تغییر برنامه های خـود و یـا درایـور هـا برای استفاده از debug غیر استاندارد API های خروجی ندارید. DebugView دارای مجموعه قدرتمند ، از ویژگی ها برای کنتـرل و مدیریت خروجی debugl است. ویژگی های جدید نسخه ۴.۶ پشتیبانی از ویندوزویستا۳۲ و ۶۴ بیتی

ابزار شماره ۴	
نحوه ی استفاده از ابزار	به سادگی فایل برنامهDebugView (dbgview.exe)را اجرا کنید DebugView بلافاصله شروع به تولید خروجی debug میکند. توجه داشته باشید که اگر DebugView را در ویندوز ۲۰۰۰ / XP اجرا کنید، باید برای نمایش حالت خطای هسته-حالت، مجوز ادمین داشته باشید. منوها، کلید های hot-key یا دکمه های نوار ابزار می توانند برای پاک کردن پنجره، ذخیره داده های تحت نظارت به یک فایل، جستجو خروجی، تغییر فونت پنجره و غیره استفاده شوند.

ابزار Hex۲dec

ابزار شماره ۵	
نام ابزار	Hex۲Dec
لینک دانلود	https://download.sysinternals.com/files/Hex۲Dec.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	تبدیل هگزادسیمال به دهدهی و برعکس با این خط فرمان ساده میتوان هگزادسیمال را به دهدهی و بالعکس تبدیل نمود
نحوه ی استفاده از ابزار	نحوه استفاده: hex۲dec [hex|decimal] x یا ۰x به عنوان پیشوند شماره برای تعیین مقدار هگزادسیمال وارد کنید. به عنوان مثال، برای ترجمه ۱۲۳۳ دهدهی به هگزادسیمال: hex۲dec ۱۲۳۳ به عنوان مثال، برای ترجمه x۱۲۳۳۰ هگزادسیمال به دهدهی: hex۲dec ۰x۱۲۳۳

ابزار Desktops

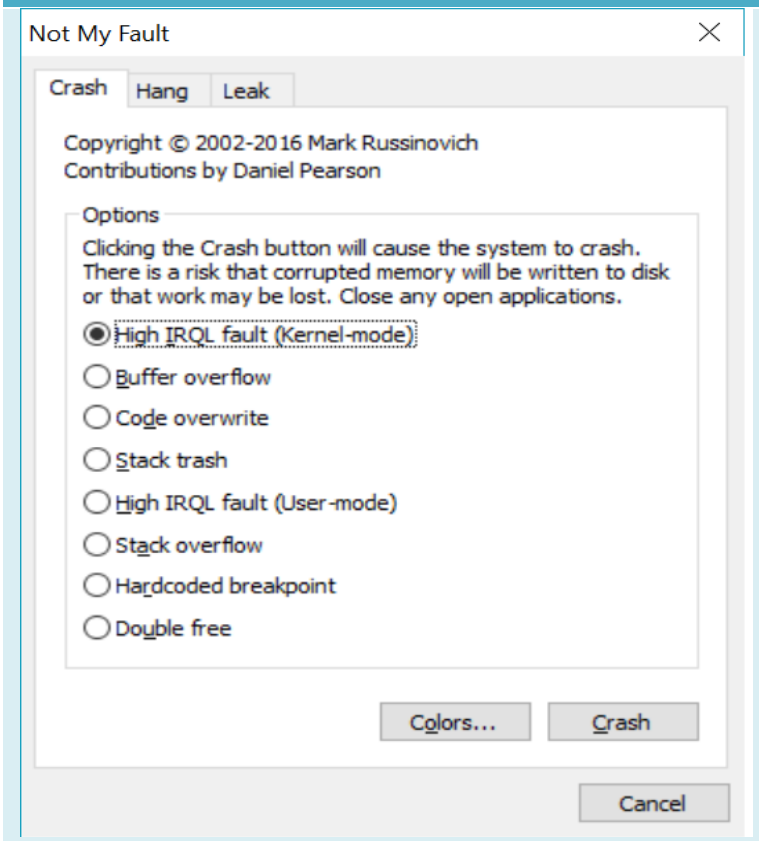
ابزار شماره ۶	
نام ابزار	Desktops
لینک دانلود	https://download.sysinternals.com/files/Desktops.zip
تاریخ انتشار	October ۱۷, ۲۰۱۲
معرفی این ابزار	Desktops به شما اجازه می دهد تا برنامه های خود را بر روی چهار میزکار مجازی سازماندهی کنید. بدون بهم ریختگی پنجره هایی که استفاده نمی کنید، ایمیل را در یکی بخوانید، وب را دردومی مرور کنید و در سومی کار خود در نرم افزار بهره وری را انجام دهید، پس از تنظیم کلید های hotkeys برای تعویض دسکتاپ، می توانید دسکتاپ را با کلیک کردن بر روی آیکون سینی مانند، ایجادکرده ویا تغییر دهید تا دسکتاپ ، پیش نمایش و تعویض پنجره یا استفاده از کلید های میانبر را باز کنید.
نحوه ی استفاده از ابزار	بر خلاف سایر ابزارهای دسکتاپ مجازی که از طریق نمایش پنجره هایی که در دسکتاپ فعال هستند و پنهان کردن بقیه اجرا می شوند، دسکتاپ های Sysinternals از یک دسکتاپ ویندوز برای هر دسکتاپ استفاده می کنند. پنجره های کاربردی هنگامی که ایجاد می شوند، به یک شیء دسکتاپ محدود می شوند، بنابراین ویندوز ارتباط بین خودش و دسکتاپ را حفظ می کند و اطلاع دارد که چه زمانی دسکتاپ را عوض می کنید. این نحوه ساختن Sysinternals رومیزیباعث میشود بسیار سبک وزن و

ابزار شماره ۶	
	بدون اشکال باشد .رویکرد دیگر مستلزم جایی است که دید آنها از پنجره های فعال با پنجره های قابل مشاهده متناقض می شود. Desktops به اشیاء دسکتاپ ویندوز متکی است، به این معنا که نمیتواند بعضی از قابلیتهای سایر ابزارهای دسکتاپ مجازی را فراهم کند. به عنوان مثال، ویندوز یک راه را برای حرکت یک پنجره از یک شیء دسکتاپ به یکی دیگر فراهم نمی کند و چون یک فرایند اکسپلورر جداگانه باید بر روی هر دسکتاپ اجرا شود تا یک نوار وظیفه و منوی شروع را اجرا کند، اکثر برنامه های tray تنها روی دسکتاپ اول قابل مشاهده هستند . علاوه بر این، هیچ راهی برای حذف شیء دسکتاپ وجود ندارد، به همین ترتیب Desktops راهی برای بستن آن فراهم نمی کند، زیرا این امر منجر به پنجره ها و فرآیندهای بدون والد می شود. بنابراین راه توصیه شده برای خروج از Desktops، این است که logoffکنید.

ابزار شماره ۶	

ابزار NotMyFault

ابزار شماره ۷	
نام ابزار	NotMyFault
لینک دانلود	https://download.sysinternals.com/files/NotMyFault.zip
تاریخ انتشار	November ۱۸, ۲۰۱۶
معرفی این ابزار	Notmyfault ابزاری است که می توانید از آن برایcrash ، hangو نابودی حافظه kernel در سیستم ویندوز خود استفاده کنید. برای یادگیری نحوه شناسایی و تشخیص مشکلات داریور دستگاه و سخت افزار، مفید است و همچنین می توانید از آن برای تولید فایل های خراب آبی روی سیستم های خرابکار استفاده کنید. فایل دانلود شامل نسخه های ۳۲ بیتی و ۶۴ بیتی و همچنین نسخه خط فرمانی است که در Nano Server کار می کند. فصل ۷ در ویندوز داخلی از Notmyfault برای نشان دادن عیب یابی نشت مخزن استفاده می کند و فصل ۱۴ آن را برای نمونه های تحلیل تجزیه و تحلیل استفاده می شود

ابزار شماره ۷	
	
نحوه ی استفاده از ابزار	نحوه استفاده notmyfaultc.exe crash crash_type_num

ابزار PsPasswd

ابزار شماره ۸	
نام ابزار	PsPasswd
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	June ۲۹, ۲۰۱۶
معرفی این ابزار	مدیران سیستم که حسابهای اداری محلی را در چندین کامپیوتر مدیریت میکنند، به طور منظم بایستی گذرواژه حساب را بهعنوان بخشی از شیوههای امنیتی استاندارد تغییر دهند. PsPasswd یک ابزار است که به شما اجازه می دهد رمز عبور حساب کاربری خود را در سیستم های محلی یا راه دور تغییر دهید، PsPasswd از API های بازنشانی گذرواژه ویندوز استفاده می کند، بنابراین رمزهای عبور بر روی شبکه را به صورت روشن ارسال نمی کند. PsPasswd بخشی از یک مجموعه رو به رشد از ابزار خط فرمان Sysinternals است که به مدیریت سیستم های محلی و از راه دور به نام PsTools کمک می کند. ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و خروجی را به صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با

ابزار شماره ۸	
	سیستم های ویندوز NT و نسخه های بعدی سازگاری کامل دارند. این ابزارها هرچند قابلیت اجـرا بـر روی سیسـتم هـای ریمـوت را دارند ولی در مقابل قابلیت استفاده به صـورت لوکـال و در شـبکه محلی را نیز دارند. مجموعه ابزار pstools نیاز به نصب ندارند. ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر

ابزار شماره ۸	
	انتخاب شده. PsSuspend - فرآیندها را متوقف می کند PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید.

ابزار PsShutdown

ابزار شماره ۹	

ابزار شماره ۹	
نام ابزار	PsShutdown
لینک دانلود	https://download.sysinternals.com/files/PSTools.zip
تاریخ انتشار	December ۴, ۲۰۰۶
معرفی این ابزار	PsShutdown یک ابزار خط فرمانی است که مشابه برنامه خاتمه دهنده از کیت Resource Kit ویندوز ۲۰۰۰ است اما با توانایی بسیار بیشتری کار می کند. علاوه بر پشتیبانی از گزینه های مشابه برای خاموش کردن یا راه اندازی مجدد کامپیوتر یا کامپیوتر از راه دور، PsShutdown می تواند کنسول را قفل کند (قفل کردن نیاز به ویندوز ۲۰۰۰ یا بالاتر دارد). PsShutdown نیاز به نصب دستی نرم افزار مشتری ندارد. PsShutdown بخشی از یک مجموعه رو به رشد از ابزار خط فرمان Sysinternals است که به مدیریت سیستم های محلی و از راه دور به نام PsTools کمک می کند. ابزار pstools مجموعه ای از ابزارها می باشد که توسط Mark Russinovichطراحی شده است. این ابزارها مبتنی بر خط فرمان ویندوز می باشند و شما را قادر می سازند تا فرایندهایی را به صورت ریموت بر روی سیستم اجرا کنید و خروجی را به صورت لوکال در حال اجرا مشاهده کنید. همه این ابزارهای خاص با سیستم های ویندوز NT و نسخه های بعدی سازگاری کامل دارند .این ابزارها هرچند قابلیت اجرا بر روی سیستم های ریموت

ابزار شماره ۹	
	را دارند ولی در مقابل قابلیت استفاده به صورت لوکال و در شبکه محلی را نیز دارند. مجموعه ابزار pstools نیاز به نصب ندارند. ابزارهای موجود در مجموعه PsTools که به عنوان یک بسته قابل دانلود می باشند عبارتند از: PsExec - اجرای فرآیندهای از راه دور PsFile - نمایش فایل های باز شده از راه دور PsGetSid - نمایش SID یک رایانه یا یک کاربر PsInfo - لیست اطلاعات مربوط به یک سیستم PsPing - اندازه گیری عملکرد شبکه PsKill - فرآیندها را با نام یا ID فرآیند حذف کنید PsList - لیست اطلاعات دقیق در مورد فرآیندها PsLoggedOn - ببینید که چه کسی به صورت محلی و یا از طریق اشتراک منابع وارد شده PsLogList - نسخه برداری پرونده های ثبت وقایع(log) PsPasswd - تغییر رمز عبور حساب کاربری PsService - خدمات مشاهده و کنترل PsShutdown - خاموش کردن و را اندازی مجدد کامپیوتر انتخاب شده. PsSuspend - فرآیندها را متوقف می کند

ابزار شماره ۹	
	PsUptime - نشان می دهد که سیستم از زمان آخرین راه اندازی آن چه مدت در حال اجرا بوده است
نحوه ی استفاده از ابزار	هیچ یک از ابزارها نیازی به نصب خاصی ندارند .حتی نیازی به نصب نرم افزار در رایانه هایی که شما آنها را هدف قرار داده اید نیست . این ابزارها برای دسترسی به صورت ریموت، نیازمند نام کاربری و رمز عبور سیستم هدف می باشند. و دقت داشته باشید که خط فرمان را با دسترسی ریموت اجرا کنید. برای نمایش راهنمایی بیشتر، دستور "-؟" را اجرا کنید

ابزار RegDelNull

ابزار شماره ۱۰	

ابزار شماره ۱۰	
نام ابزار	Regdelnull
لینک دانلود	https://download.sysinternals.com/files/Regdelnull.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	این ابزار خط فرمان را جستجو می کند و به شما اجازه می دهد کلید های رجیستری را که حاوی کاراکترهای جاسازی شده و null هستند حذف کنید و با استفاده از ابزارهای ویرایش رجیستری استاندارد، قابل بازگرداندن هستند. توجه داشته باشید: حذف کلید های رجیستری ممکن است برنامه های مرتبط با آنها را مختل کند.
نحوه ی استفاده از ابزار	در اینجا یک مثال از RegDelNull در هنگام استفاده از یک سیستم که در برنامه نمونه RegHide یک کلید جاسازی شده را ایجاد کرده است آورده ایم: Shell Copy C:\>regdelnull hklm -sRegDelNull v1.10 - Delete Registry keys with embedded N Copyright (C) 2005-2006 Mark Russinovich Sysinternals - www.sysinternals.com Null-embedded key (Nulls are replaced by '*'): HKLM\SOFTWARE\Systems Internals\Can't touch me!* Delete (y/n) y Scan complete.

ابزار Registry Usage

ابزار شماره ۱۱	
نام ابزار	RU
لینک دانلود	https://download.sysinternals.com/files/RU.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	ابزار Ruگزارش استفاده از فضای رجیستری را برای کلید رجیستری مشخص می کند .به طور پیش فـرض، کلیـد هـای فرعـی را بـرای نشان دادن کل اندازه کلید و کلید های فرعی آن به عنوان خروجی میدهد.
نحوه ی استفاده از ابزار	ru [-c[t]] [-l <levels> | -n | -v] [-q] <absolute path> ru [-c[t]] [-l <levels> | -n | -v] [-q] -h <hive file> [relative path] -c چاپ خروجی به عنوان CSV. مشخصه ct- برای خروجی به صورت زبانه است -h فایل پرونده مشخص را بار گذاری کنید، محاسبات اندازه انجام دهید، سپس آن را بارگیری و فشرده سازی کنید. -l عمق اطلاعات کلید فرعی را مشخص کنید (به طور پیش فرض یک سطح است). -n تجدید نکنید(بدون بازگشت) -Q آرام و بی سرو صدا (بدون بنر) -v نمایش اندازه تمام کلید های فرعی.

ابزار شماره ۱۱	

ابزار Reghide

ابزار شماره ۱۲	
نام ابزار	RegHide
لینک دانلود	https://download.sysinternals.com/files/RegHide.zip
تاریخ انتشار	November ۱, ۲۰۰۶
معرفی این ابزار	تفاوت ظریف اما معنی داری بین API Win۳۲ و API بومی (Native) در توصیف نام ها وجود دارد. در API Win۳۲ رشته ها به صورت پایان یافته با NULL (انتهای رشته با NULL مشخص میشود)، ANSI(۸ بیتی) یا رشته ای گسترده (۱۶ بیتی) توصیف میشوند . درAPI محلی نام ها ،به صورت رشته های Unicode (۱۶ بیتی) توصیف می شوند. در حالی که این تمایز معمولا مهم نیست، یک وضعیت جالب را باز می کند: یک کلاس از نام هایی است که می تواند با استفاده از

ابزار شماره ۱۲	
	APIبومی ارجاع شود، اما نمی تـوان آن را بـا اسـتفاده از Win۳۲ APIتوصیف کرد.
نحوه ی استفاده از ابزار	

ابزار RegJump

ابزار شماره ۱۳	
نام ابزار	RegJump
لینک دانلود	https://download.sysinternals.com/files/RegJump.zip
تاریخ انتشار	April ۲۰, ۲۰۱۵
معرفی این ابزار	این اپلت خط فرمان کوچک ، یک مسـیر رجیسـتری را مـی گیـرد وباعث میشود Regedit آن مسیر را باز کند. آن کلید های ریشه را در استاندارد (مثلا HKEY_LOCAL_MACHINE)و فرم اختصاری (به عنوان مثال HKLM) می پذیرد.
نحوه ی استفاده از	regjump <<path>|-c> -c مسیر از کلیپ بورد کپی می شود

ابزار شماره ۱۳	
ابزار	مثال : regjump HKLM\Software\Microsoft\Windows

ابزار Strings

ابزار شماره ۱۴	
نام ابزار	Strings
لینک دانلود	https://download.sysinternals.com/files/Strings.zip
تاریخ انتشار	July ۴, ۲۰۱۶
معرفی این ابزار	کار بر روی NT و Win۲K به این معنی است که فایل های اجرایی و شیء چندین بار با رشته های UNICODE تعبیه خواهد شد، که شما به راحتی با یک رشته استاندارد ASCIIیا برنامه grep نمی توانید ببینید . Strings فقط پرونده ی رمز گذاری شده با رشته های UNICODE یا (ASCII)را با طول ۳ یا بیشتر UNICODEیا(ASCII) اسکن می کند . توجه داشته باشید که تحت ویندوز ۹۵ نیز کار می کند.
نحوه ی استفاده از	strings [-a] [-f offset] [-b bytes] [-n length] [-o] [-q] [-s]

ابزار شماره ۱۴	
ابزار	[-u] <file or directory> a- فقط جستجوی Ascii (به طور پیش فرض Unicode وAscii) b- بایت فایل برای اسکن f-ابتدای فایل برای شروع اسکن. o- رشته در چه مکانی از فایل واقع شده است n- حداقل طول رشته (به طور پیش فرض ۳ است) Q- بی سرو صدا (بدون بنر) s- زیر شاخه ها را بازسازی می کند u- فقط جستجوی Unicode (به طور پیش فرض Unicode و Ascii) برای جستجوی یک یا چند فایل برای حضور یک رشته خاص با استفاده از strings ، از دستور زیر استفاده کنید: TextToSearchFor strings * | findstr /i

ابزار ZoomIt

ابزار شماره ۱۵	
نام ابزار	ZoomIt

ابزار شماره ۱۵	
لینک دانلود	https://download.sysinternals.com/files/ZoomIt.zip
تاریخ انتشار	June ۲۰, ۲۰۱۳
معرفی این ابزار	ZoomItیک زوم روی صفحه و ابزار حاشیه نویسی برای ارائه هـای فنـی اسـت کـه شـامل تظـاهرات کـاربردی اسـت ZoomIt بـدون محدودیت اجرا می شود و با کلید های قابل تنظیم تنظیم می شود تا روی یک منطقه از روی صفحه نمایش بزرگنمایی کند، در حـالی که با زوم حرکت می کند، و بر روی تصـویر بزرگنمـایی مـی کنـد. ZoomItرا متناسب با نیازها نوشته اند و از آن در سخنرانی ها مـی توان استفاده کرد. ZoomItدر تمام نسخه های ویندوز کار می کند و شما می توانید از ورود قلم برای طراحی ZoomIt در رایانه ها استفاده کنید.
نحوه ی استفاده از ابزار	اولـین بـار کـه ZoomIt را اجـرا مـی کنیـد، آن یـک محـاوره ی تنظیمات را نشان می دهد که رفتار ZoomIt را نشان می دهد، بـه شما اجازه داده می شود که کلید های متناوب را برای بزرگنمایی و برای ورود به حالت رسم بدون زوم، و سفارشی کردن رنگ و انـدازه رسـم قلـم اسـتفاده کنیـد. از گزینـه draw-without-zoom بـرای مخفی کردن صفحه در رزولوشن بـومی خـود اسـتفاده مـی کنـیم. ZoomIt همچنین شامل یک ویژگی تایمر استراق سمع فعال است حتی زمانی که از پنجره تایمر دور می شود و به شما اجازه می دهد

ابزار شماره ۱۵	
	تا با کلیک روی آیکون Tray ZoomIt به پنجره تایمر بازگردید.