بسمه تعالی

گزارش در خصوص ابزارهای Sysinternals Suite

فهرست مطالب

معرفی Sysinternals Suite

Sysinternals Suite به صورت یک پک ارائه شده توسط شرکت ماکروسافت 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

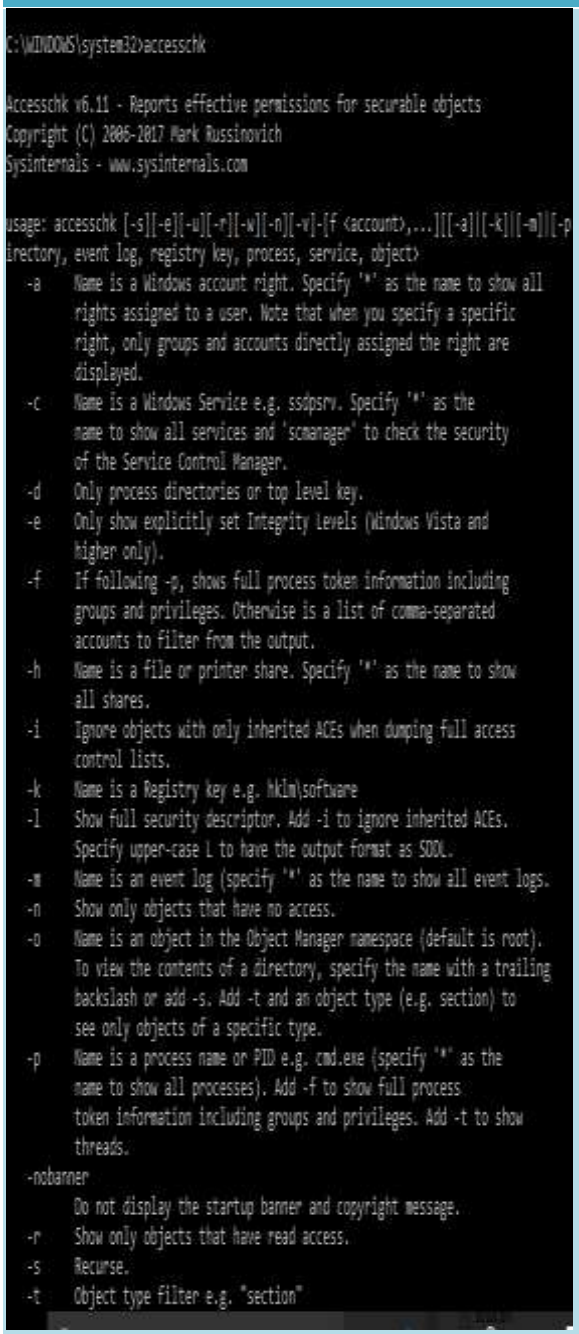
ابزار AccessChk

ابزار شماره ۱	
نام ابزار	AccessChk

ابزار شماره ۱	
لینک دانلود	https://download.sysinternals.com/files/AccessChk.zip
تاریخ انتشار	September 11, 2017
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.

ابزار شماره ۱	
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 AccessChk و اجرای ابزار دستورات کاربردی آن با توضیح نشان داده می شود. برای مثال ما ابزار AccessChk.exe را در مسیر windows\system32 کپی می کنیم با تایپ آن طبق شکل زیر برنامه اجرا می شود:

ابزار شماره ۱	

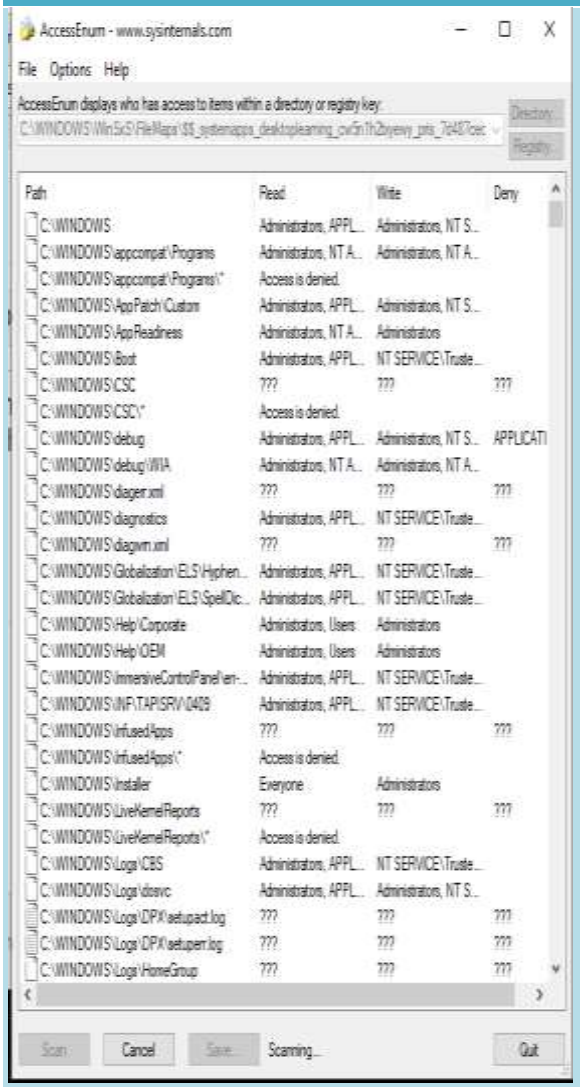


```
C:\WINDOWS\system32>accesschk

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

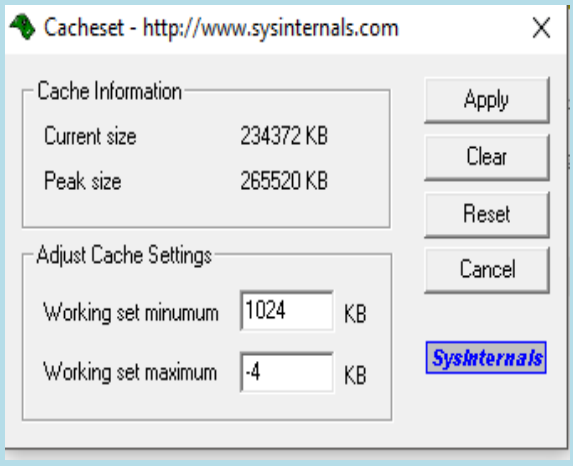
ابزار شماره ۲	
نام ابزار	AccessEnum
لینک دانلود	https://download.sysinternals.com/files/AccessEnum.zip
تاریخ انتشار	November 1, 2006
معرفی این ابزار	در حالی که مدل امنیتی قابل انعطاف با استفاده از سیستم های مبتنی بر ویندوز NT امکان کنترل کامل امنیت و مجوزهای فایل را فراهم می کند، مدیریت مجوز ها به طوری 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

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

ابزار شماره ۲	
	

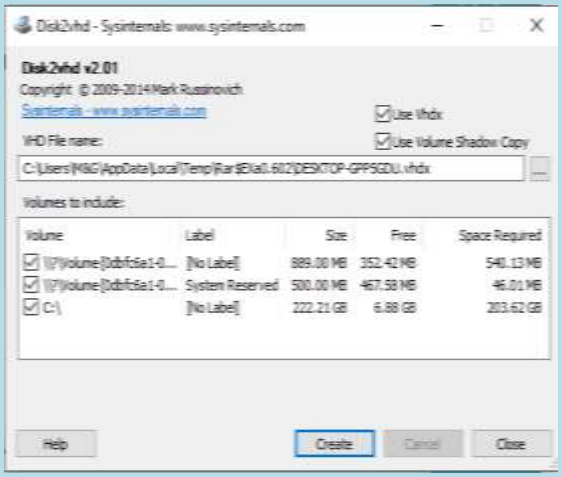
ابزار CacheSet

ابزار شماره ۳	
نام ابزار	CacheSet
لینک دانلود	https://download.sysinternals.com/files/CacheSet.zip
تاریخ انتشار	November 1, 2006
معرفی این ابزار	CacheSet به شما اجازه می دهد تا پارامترهای کار شده در حافظه فایل سیستم را دستکاری کنید. بر خلاف CacheMan، CacheSetبر روی تمام نسخه های NT اجرا می شود و بدون تغییر در نسخه های جدید Service Packکار 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

ابزار شماره ۳	
	حداقل نقطه شروع کنید. همچنین بر خلافCacheMan ، تغییرات ساخته شده با CacheSet تاثیر فوری بر اندازه Cacheدارند .
نحوه ی استفاده از ابزار	این ابزار بر روی Client: Windows Vistaو بالاتر . Server: Windows Server 2008 and 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 Disk2vhd

ابزار شماره 4	
نام ابزار	Disk2vhd
لینک دانلود	https://download.sysinternals.com/files/Disk2vhd.zip
تاریخ انتشار	January 21, 2014
معرفی این ابزار	Disk2vhd 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 Disk2vhd و دیگر ابزارهای مبدل هارد فیزیکی به

ابزار شماره 4	
	مجازی این است که شما می توانید Disk2vhd 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:  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.

ابزار شماره 4	
	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:Disk2vhd از تبدیل حجم دیسک با Bitlocker 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. Disk2vhd در ویندوز ویستا، ویندوز سرور ۲۰۰۸ و بالاتر از جمله سیستم های x64 اجرا می شود. در اینجا یک تصویر از کپی یک سیستم عامل ویندوز سرور ۲۰۰۸ R2 Hyper-V در یک ماشین مجازی در بالای سیستم آن ساخته شده است:

ابزار شماره 4	
	 استفاده از خط فرمان Disk2vhd شامل گزینه های خط فرمان است که شما را قادر به ایجاد کردن VHD ها می کند. Example: disk2vhd * c:\vhd\snapshot.vhd دستور کامل: disk2vhd <[drive: [drive:]...]|[*]> <vhdfile>

ابزار Contig

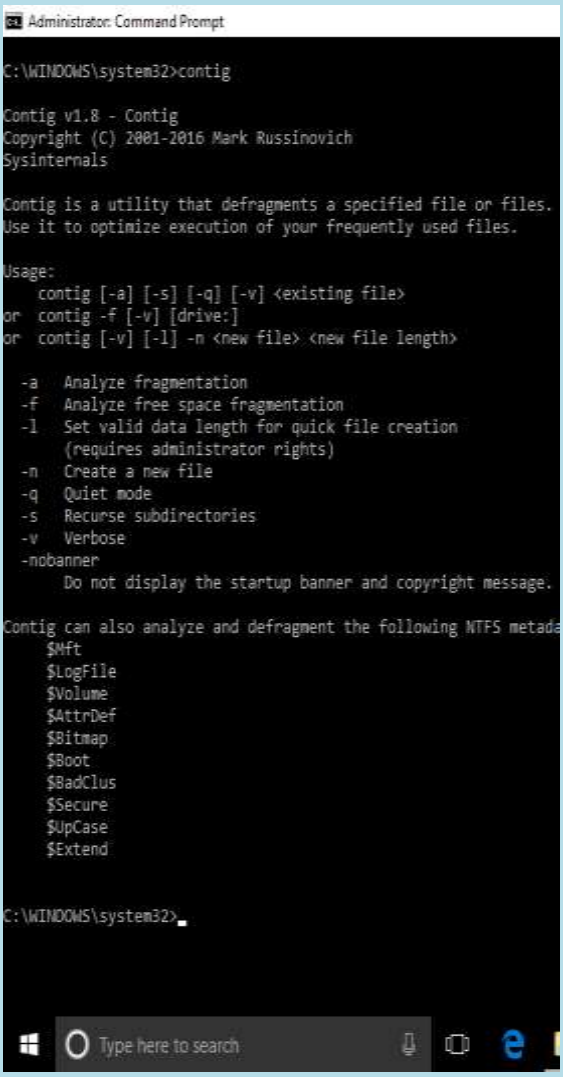
ابزار شماره 5	
نام ابزار	Contig
لینک	https://download.sysinternals.com/file

ابزار شماره 5	
دانلود	s/Contig.zip
تاریخ انتشار	July 4, 2016
معرفی این ابزار	Contigبرای 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 ابزار Defragmenterساخته شده در 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 defragmentedشود: برای مثال contig -s C: \ * همه فایل ها را بر روی هارد دیسک C

ابزار شماره 5	
	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: • \$Mft • \$LogFile • \$Volume • \$AttrDef • \$Bitmap • \$Boot • \$BadClus • \$Secure • \$UpCase

ابزار شماره 5	
	• \$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. برای مثال ما ابزار Conig.exe را در مسیر windows\system32 کپی می کنیم با تایپ آن طبق شکل زیر برنامه اجرا می

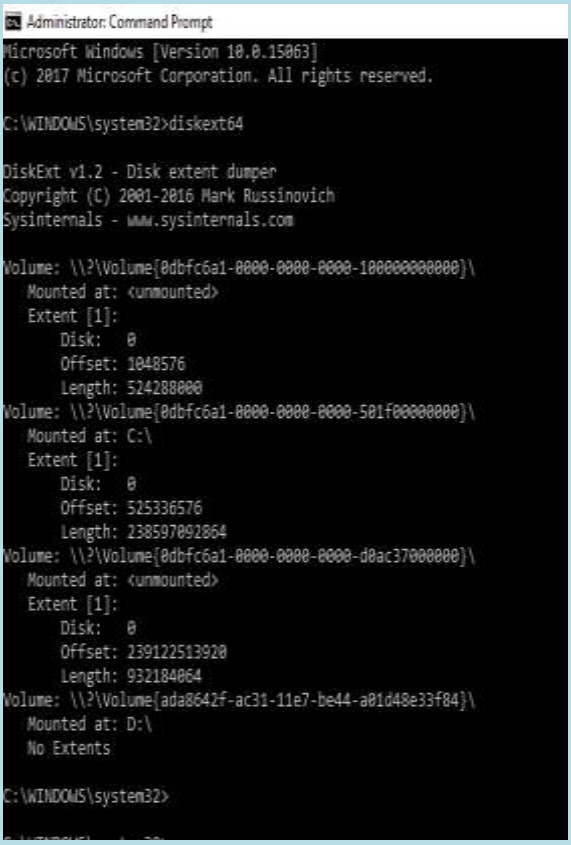
ابزار شماره 5	
	شود:



ابزار DiskExt

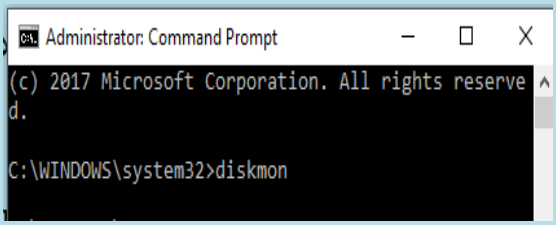
ابزار شماره 6	
نام ابزار	DiskExt
لینک دانلود	https://download.sysinternals.com/files/DiskExt.zip
تاریخ انتشار	July 4, 2016
معرفی این ابزار	DiskExt استفاده از فرمان IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS را که اطلاعاتی درباره دیسک هایی که پارتیشن های یک جلد در آن قرار گرفته اند نشان می دهد (دیسک های چند 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

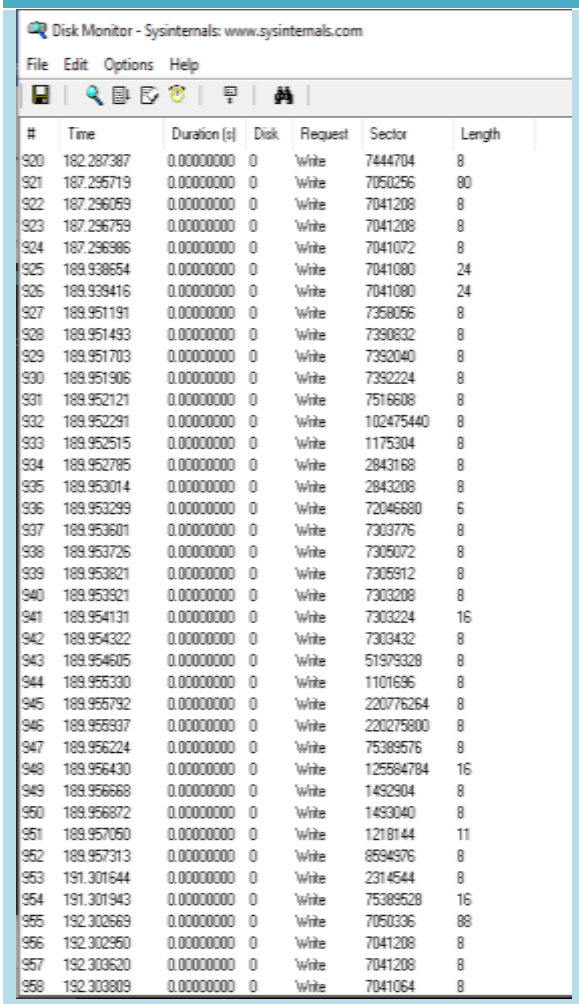
ابزار شماره 6	
	داده می شود. برای مثال ما ابزار DiskExt.exe را در مسیر windows\system32 کپی می کنیم با تایپ آن طبق شکل زیر برنامه اجرا می شود



ابزار DiskMon

ابزار شماره ۷	
نام ابزار	DiskMon
لینک دانلود	https://download.sysinternals.com/files/DiskMon.zip
تاریخ انتشار	November 1, 2006
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 در event tracing استفاده می کند. SDK پلتفرم مایکروسافت مستند شده

ابزار شماره ۷	
	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\system32 بریزید سپس در حالت admin به cmd رفته و کلمه ی DiskMon را تایپ می کنیم.سپس برنامه به صورت گرافیکی برای شما اجرا خواهد شد. 

ابزار شماره ۷	
	

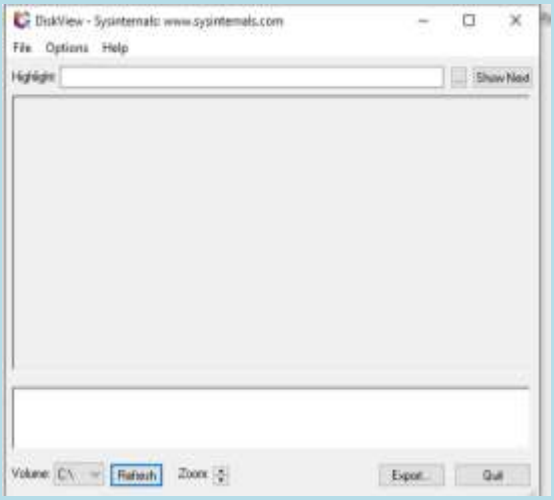
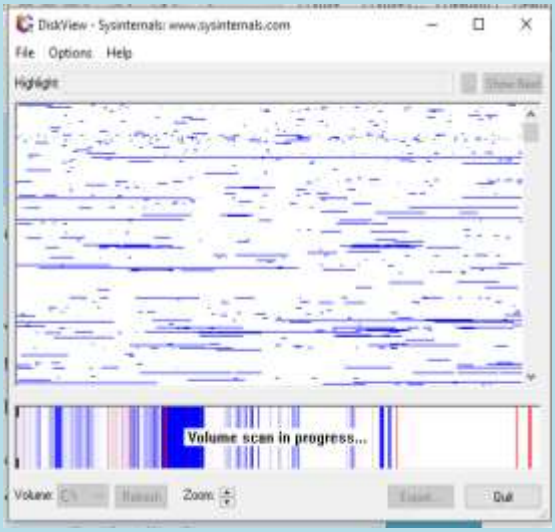
Disk Monitor - Sysinternals: www.sysinternals.com

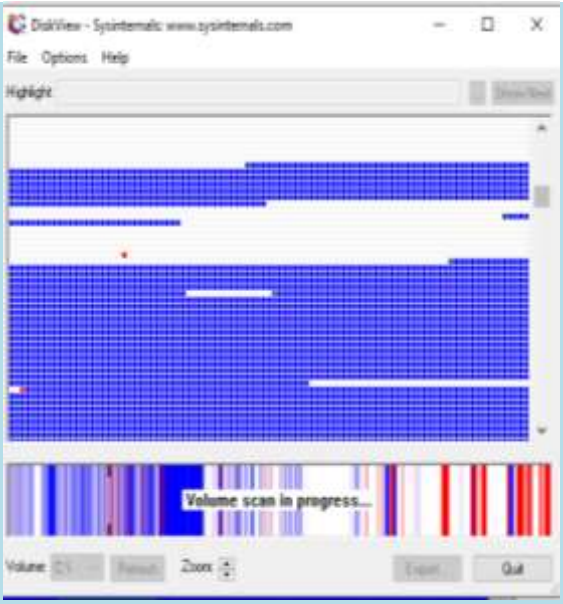
File Edit Options Help

#	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	189.956937	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 25, 2010
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.

ابزار شماره ۸	
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 Disk Usage

ابزار شماره ۹	
نام ابزار	Disk Usage
لینک دانلود	https://download.sysinternals.com/files/DU.zip
تاریخ انتشار	July 4, 2016
معرفی این ابزار	مشاهده disk usage توسط دایرکتوری. 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.

ابزار شماره ۹	
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