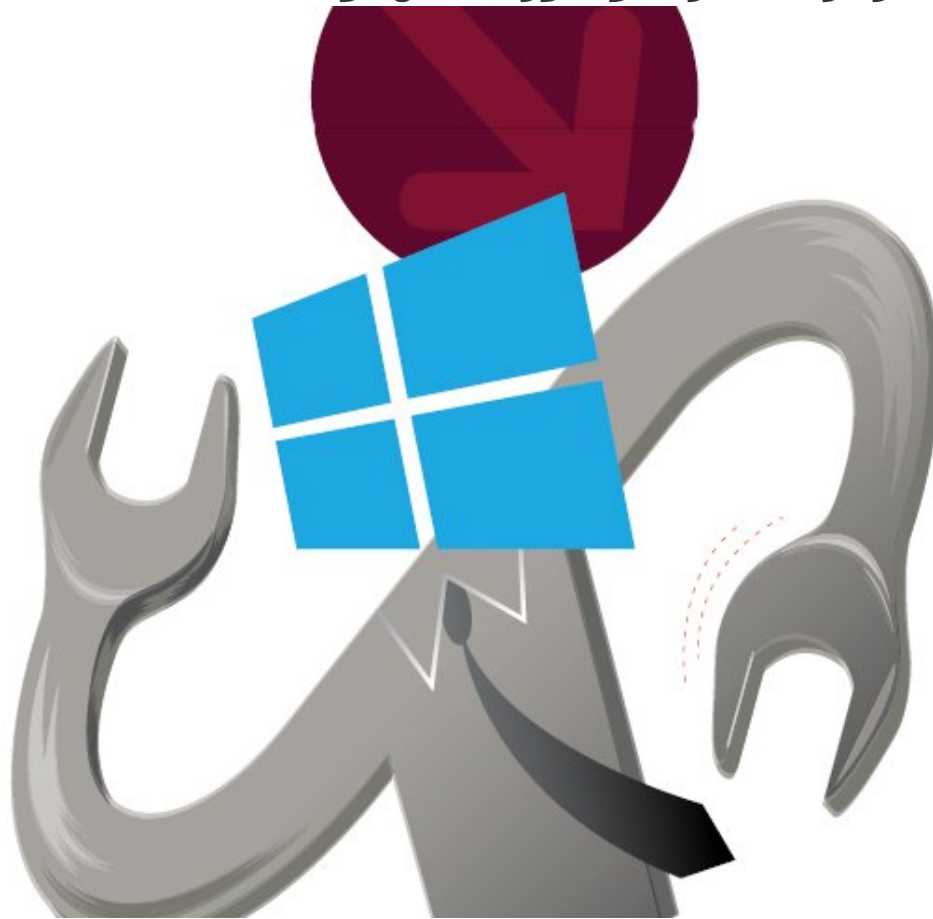
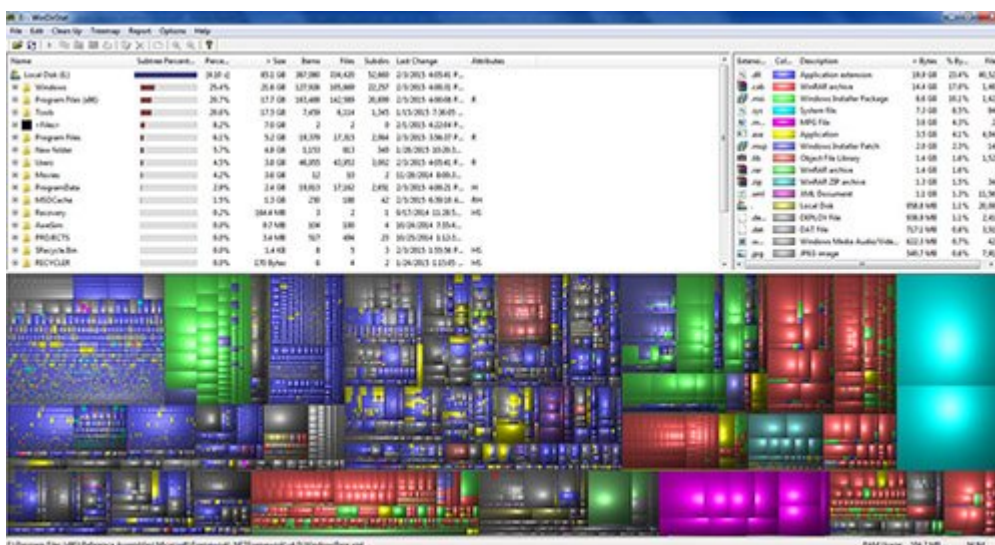


## ابزارهای منبع باز همراه ابزارهای مایکروسافت قدرت مضاعفی در اختیار مدیران قرار می‌دهند 15 ابزار منبع باز برای مدیران ویندوز - بخش اول



مدیران اغلب به دنبال ابزارهای اصلی و قدرتمند سمت سرور هستند که برای راهبری بهتر روی محصولاتی همچون ویندوز سرور، Exchange Server، SQL Server و شیرپوینت مورد استفاده قرار گیرند. برای آن‌ها که دید عمیق‌تری نسبت به این مسئله دارند یا در پی مجموعه‌ای از ابزارهایی هستند که توسط محصولات سرور مایکروسافت مورد پشتیبانی قرار گیرند، ابزارهای منبع باز مایکروسافت از طریق CodePlex و همچنین سازندگان ثالث وجود دارد. با توجه به رویکرد متفاوتی که از سوی مایکروسافت در سمت میزبانی و ارائه محصولاتی نظیر Office 365 و Azure به وجود آمده، انگیزه بیشتری در مدیران برای بررسی تحولات ابزارهای مدیریتی ویندوز پدید آمده است. در ادامه، فهرستی از ابزارهای منبع باز را معرفی می‌کنیم که هر مدیر ویندوز بهتر است از آن‌ها با خبر باشد.

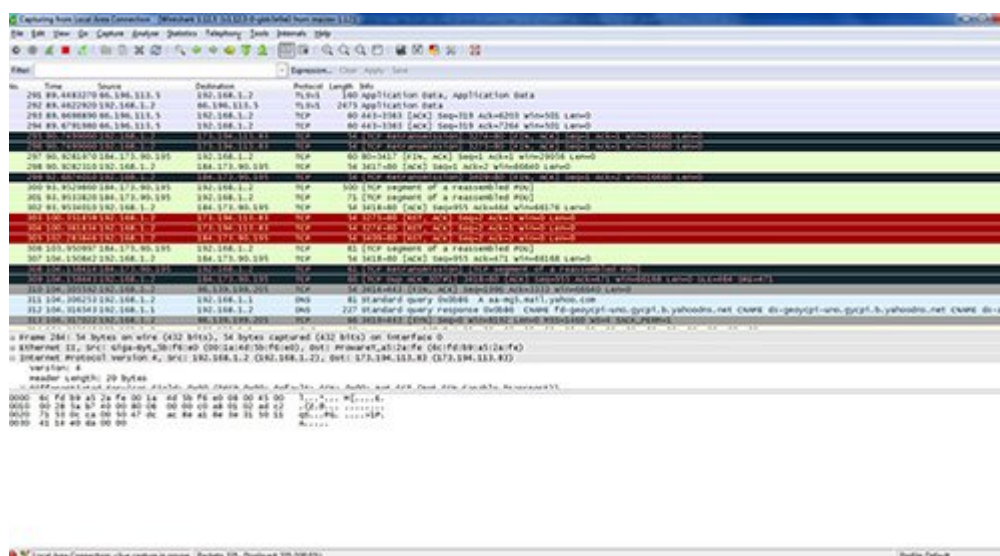
### WinDirStat



WinDirStat (سرنام Windows Directory Statistics) ابزاری است که نحوه استفاده از دیسک را مدیریت می‌کند.

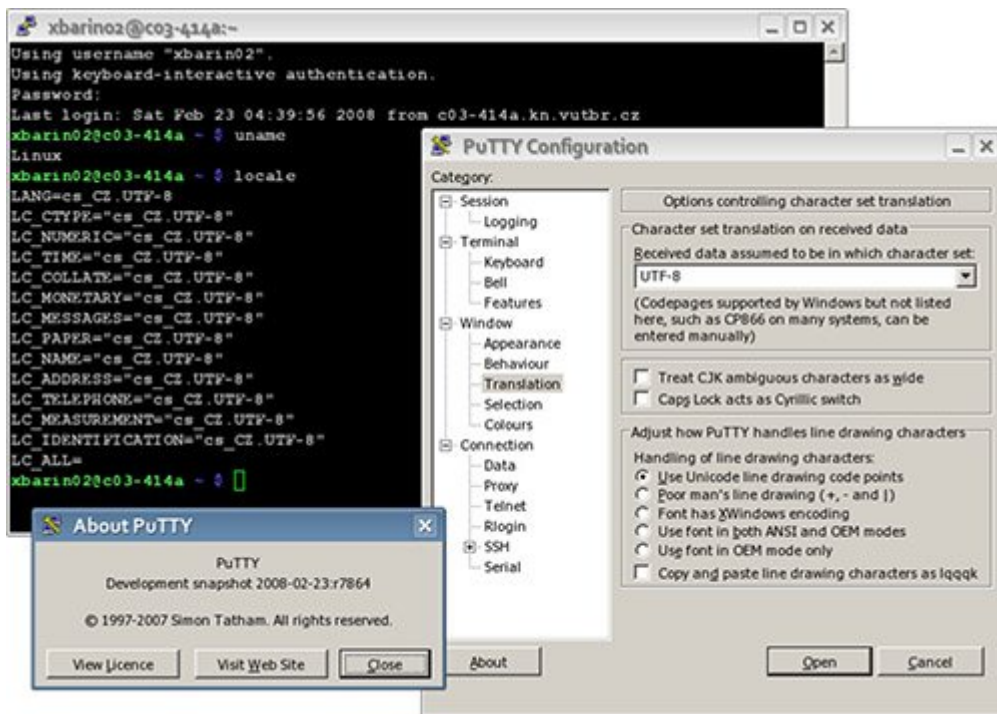
این ابزار نمایش‌های آماری مختلفی از اطلاعات ارائه می‌دهد. از این اطلاعات برای تجزیه و تحلیل این‌که چگونه دیسک مورد استفاده قرار گرفته است، می‌توان بهره برد. هر مدیر شبکه بارها تجربه برخورد با مشکلاتی در رابطه با فضای دیسک را تجربه کرده است. مشکلاتی از قبیل این‌که آیا از سیستم کاربر پشتیبانی کرده یا زمانی که نرم‌افزاری برای نظارت مورد استفاده قرار می‌گیرد، در زمان بروز مشکلات بحرانی برای سرور پیغام هشدار اعلام کرده است یا نه. اغلب زمانی که فضای دیسک مورد استفاده قرار گرفته و سیستم دچار مشکل می‌شود، می‌توان از این موضوع اطلاع پیدا کرد. اما در شرایطی که این آگاهی به‌وضوح مشخص نیست یا زمان کافی وجود نداشته نباشد، WinDirStat به کمک شما می‌آید. مدیران سیستم‌عامل‌های لینوکس می‌توانند از ابزار KDirStat و سیستم‌عامل‌های X MacOS X، Disk Inventory یا GrandPerspective استفاده کنند. این نرم‌افزار توانایی بازرسی و نظارت روی یک درایو، همه درایوها یا یک پوشه خاص را دارد. همان‌گونه که در شکل بالا مشاهده می‌کنید، این نرم‌افزار اطلاعات جامع و مفصلی درباره فایل‌ها، برنامه‌ها و انواع آن‌ها نشان می‌دهد. نکته جالب توجهی که درباره این نرم‌افزار باید به آن اشاره کرد، به شکل‌هایی که در بخش پایین پنجره نرم‌افزار قرار دارند، مرتبط می‌شود. اگر اشاره‌گر ماوس روی هر یک از پیکسل‌های درون این پنجره قرار بگیرد، فایل و مسیر متناظر به فایل نشان داده می‌شود.

## WireShark



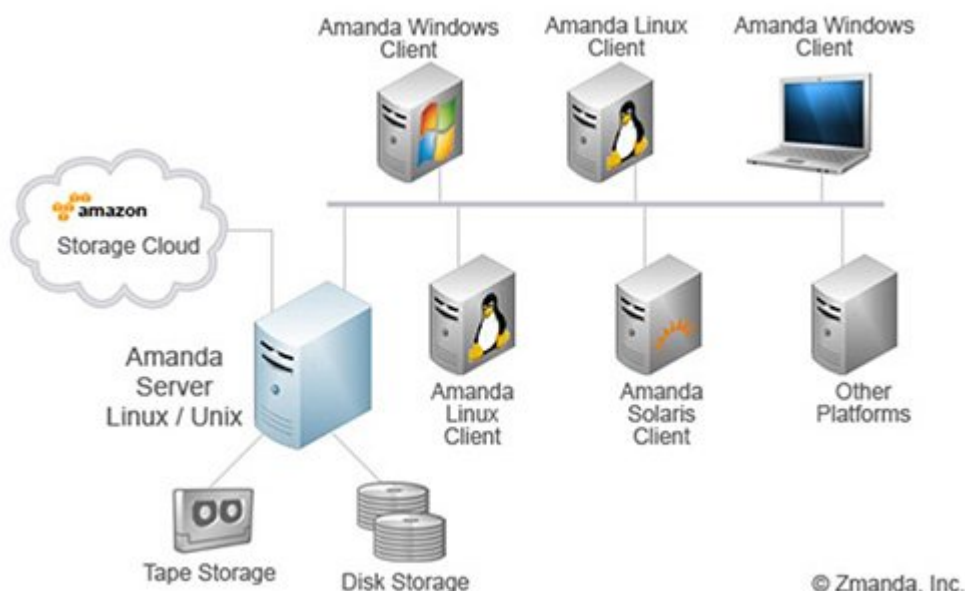
تجزیه و تحلیل بسته‌های شبکه و خطایابی آن‌ها به‌راستی یک هنر واقعی است و اغلب نیازمند سال‌ها تجربه و آموزش است. اما به لطف قابلیت‌های قدرتمند و ایرشارک این منحنی یادگیری به‌سرعت تکمیل می‌شود. و ایرشارک یک نرم‌افزار متن باز چندپلتفرمی بوده که برای عیب‌یابی، تجزیه و تحلیل نرم‌افزارها و توسعه پروتکل‌های ارتباطی و آموزشی مورد استفاده قرار می‌گیرد.

## PuTTY



هیچ فهرست ابزار متن بازی که مدیران مورد استفاده قرار می‌دهند، بدون اشاره به PuTTY کامل نخواهد بود. PuTTY یکی از پرکاربردترین ابزارهای شبیه‌ساز ترمینال است. خواه شما نیازمند یک ارتباط سریال برای سوئیچ کردن به Telnet، SSH، SCP یا rlogin باشید، PuTTY به‌خوبی از عهده اداره کردن این فرآیند برمی‌آید. این ابزار از اواخر دهه 1990 میلادی تا به امروز وجود داشته و ده‌ها نرم‌افزار از آن الگو گرفته‌اند. اما هیچ کدام به اندازه نسخه اصلی محبوب نبودند.

## [AMANDA Network Backup](#)



مدیرانی که همیشه از فرآیند پشتیبان‌گیری در سیستم‌های مجهز به ویندوز رنج می‌برند، بهتر است ابزار AMANDA را مورد بررسی قرار دهند. AMANDA (سرنام Advanced Maryland Automatic Network Disk Archiver) قابلیت در اختیار یک مدیر قرار می‌دهد که یک سرور پشتیبان‌گیر مجزا که توانایی پشتیبانی از ویندوزهای دسکتاپ و سرور روی یک شبکه را دارد، ایجاد می‌کند. همچنین، از انواع مختلفی از ابزارهای ذخیره‌سازی همچون نوارهای مغناطیسی، دیسک‌ها یا رسانه‌های نوری پشتیبانی می‌کند که از پارتیشن‌بندی NTFS استفاده می‌کنند. ZMANDA به‌راحتی و آسانی از AMANDA پشتیبانی می‌کند. ZMANDA Recovery Manager برای بانک اطلاعاتی MySQL

طراحی شده است که فرآیند تهیه نسخه پشتیبان و بازیابی آسان و در عین حال انعطاف‌پذیر و قدرتمند را در اختیار یک مدیر بانک اطلاعاتی می‌گذارد. همچنین، خدمات شبکه و پشتیبان‌گیری ابری را به صورت تجاری عرضه می‌کند.

## Nmap

```
31337
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc    Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Nmap یک ابزار عالی نگاشت شبکه است که برای آگاهی از میزبان‌ها و سرویس‌هایی که به شبکه متصل هستند مورد استفاده قرار می‌گیرد. در حالی که Nmap بیشتر در زمینه بررسی امنیت به‌ویژه برای شناسایی پورت‌های باز و رخنه‌ها مورد استفاده قرار می‌گیرد، بیشتر مدیران سیستم‌ها از آن به‌عنوان ابزاری که به‌سادگی برای اطلاع از این‌که چه عملیاتی روی شبکه آن‌ها در حال وقوع است، آن را مورد استفاده قرار می‌دهند. شناسایی سیستم‌عامل و نشانی‌های سخت‌افزاری میزبان‌های مختلف از جمله این فعالیت‌ها به‌شمار می‌رود. Nmap توانایی تشخیص نسخه برنامه‌ها و خدمات، بررسی میزبان یا مدت زمان تخمینی در دسترس بودن سرویس و حضور دیوار آتش را دارد.

منبع:

---

نشانی منبع: <https://www.shabakeh-mag.com/workshop/426>