Ishare

KSR COLLEGE OF ARTS AND SCIENCE
INDIA
Knowledge is Power

Apr 2010

Issue #20

Ishare

Monthly Magazine

Ignite ur Ideas

Department of Computer Science & Applications

UG(BCA & B.Sc)

PG(MCA & M.Sc)

M.Phil(CS)

KSR College of Arts and science

EDITORIAL …

PARAM Padma is C-DAC's next generation high performance scalable computing cluster, currently with a peak computing power of One Teraflop. The hardware environment is powered by the Compute Nodes based on the state-of-the-art Power4 RISC processors, using Copper and SOI technology, in Symmetric Multiprocessor(SMP)configuration These nodes are connected through a primary high performance System Area Network, PARAMNet-II, designed and developed by C-DAC and a Gigabit Ethernet as a backup network. C-DAC's PARAM series of supercomputers have been deployed to address diverse applications in science and engineering, and business computing at various institutions in India. More useful and interesting informations in this edition of ISHARE....

Editorial Board

CONTENTS

Articles

Tech Zone

Social Network Analysis

Author

S.Sasikala,
Lecturer, CS

Article Title

Social Network Analysis

Article Description

This article gives information about Social Network Analysis and where it is used effectively.

Social network analysis [SNA] is the mapping and measuring of relationships and flows between people, groups, organizations, computers, URLs, and other connected information/knowledge entities. The nodes in the network are the people and groups while the links show relationships or flows between the nodes. SNA provides both a visual and a mathematical analysis of human relationships.

Management consultants use this methodology with their business clients and call it Organizational Network Analysis [ONA].

To understand networks and their participants, we evaluate the location of actors in the network. Measuring the network location is finding the centrality of a node. These measures give us insight into the various roles and groupings in a network -- who are the connectors, mavens, leaders, bridges, isolates, where are the clusters and who is in them, who is in the core of the network, and who is on the periphery.

We look at a social network -- the "Kite Network" above -- developed by David Krackhardt, a leading researcher in social networks. Two nodes are connected if they regularly talk to each other, or interact in some way. Andre regularly interacts with Carol, but not with Ike. Therefore Andre and Carol are connected, but there is no link drawn between Andre and Ike. This network effectively shows the distinction between the three most popular individual centrality measures: Degree Centrality, Betweenness Centrality, and Closeness Centrality.

Degree Centrality

Social network researchers measure network activity for a node by using the concept of degrees -- the number of direct connections a node has. In the kite network above, Diane has the most direct connections in the network, making hers the most active node in the network. She is a 'connector' or 'hub' in this network. Common wisdom in personal networks is "the more connections, the better." This is not always so. What really matters is where those connections lead to -- and how they connect the otherwise unconnected! Here Diane has connections only to others in her immediate cluster -- her clique. She connects only those who are already connected to each other.

Betweenness Centrality

While Diane has many direct ties, Heather has few direct connections -- fewer than the average in the network. Yet, in may ways, she has one of the best locations in the network -- she is between two important constituencies. She plays a 'broker' role in the network. The good news is that she plays a powerful role in the network, the bad news is that she is a single point of failure. Without her, Ike and Jane would be cut off from information and knowledge in Diane's cluster. A node with high betweenness has great influence over what flows -- and does not -- in the network. Heather may control the outcomes in a network. That is why I say, "**As in Real Estate, the golden rule of networks is: Location, Location, Location**."

Closeness Centrality

Fernando and Garth have fewer connections than Diane, yet the pattern of their direct and indirect ties allow them to access all the nodes in the network more quickly than anyone else. They have the shortest paths to all others -- they are close to everyone else. They are in an excellent position to monitor the information flow in the network -- they have the best visibility into what is happening in the network.

Network Centralization

Individual network centralities provide insight into the individual's location in the network. The relationship between the centralities of all nodes can reveal much about the overall network structure.

A very centralized network is dominated by one or a few very central nodes. If these nodes are removed or damaged, the network quickly fragments into unconnected sub-networks. A highly central node can become a single point of failure. A network centralized around a well connected hub can fail abruptly if that hub is disabled or removed. Hubs are nodes with high degree and betweeness centrality.

A less centralized network has no single points of failure. It is resilient in the face of many intentional attacks or random failures -- many nodes or links can fail while allowing the remaining nodes to still reach each other over other network paths. Networks of low centralization fail gracefully.

Network Reach

Not all network paths are created equal. More and more research shows that the shorter paths in the network are more important. Noah Friedkin, Ron Burt and other researchers have shown that networks have horizons over which we cannot see, nor influence. They propose that the key paths in networks are 1 and 2 steps and on rare occasions, three steps. The "small world" in which we live is not one of "six degrees of separation" but of direct and indirect connections < 3 steps away. Therefore, it is important to know: who is in your network neighborhood? Who are you aware of, and who can you reach?

In the network above, who is the only person that can reach everyone else in two steps or less?

Boundary Spanners

Nodes that connect their group to others usually end up with high network metrics. Boundary spanners such as Fernando, Garth, and Heather are more central in the overall network than their immediate neighbors whose connections are only local, within their immediate cluster. You can be a boundary spanner via your bridging connections to other clusters or via your concurrent membership in overlappping groups.

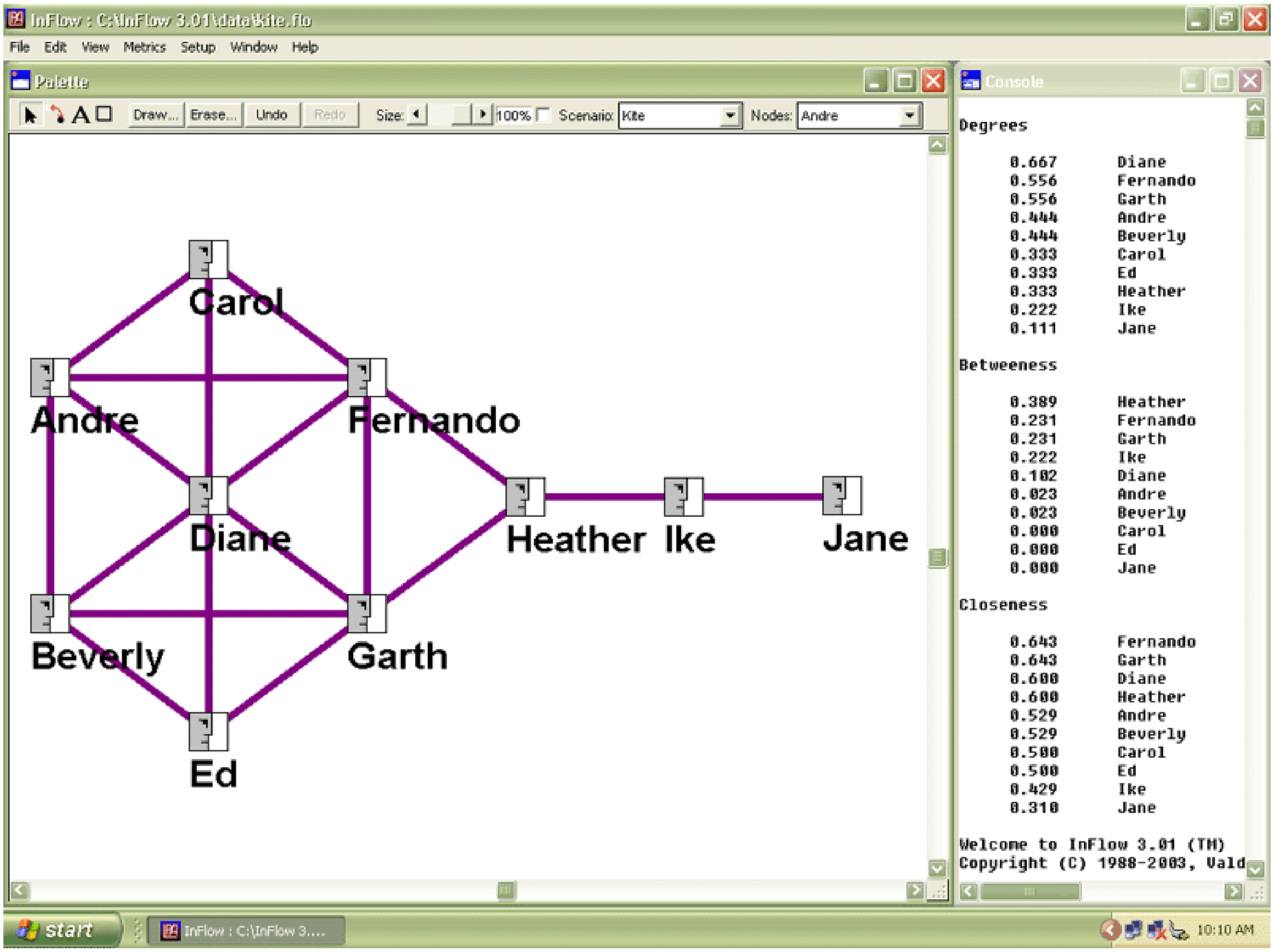
Boundary spanners are well-positioned to be innovators, since they have access to ideas and information flowing in other clusters. They are in a position to combine different ideas and knowledge, found in various places, into new products and services.

Peripheral Players

Most people would view the nodes on the periphery of a network as not being very important. In fact, Ike and Jane receive very low centrality scores for this network. Since individuals' networks overlap, peripheral nodes are connected to networks that are not currently mapped. Ike and Jane may be contractors or vendors that have their own network outside of the company -- making them very important resources for fresh information not available inside the company!

This is a list of real-time operating systems

. An RTOS is an operating system in which the maximum time from an input stimulus to an output response can be definitely determined.



```
Degrees

      0.667        Diane
      0.556        Fernando
      0.556        Garth
      0.444        Andre
      0.444        Beverly
      0.333        Carol
      0.333        Ed
      0.333        Heather
      0.222        Ike
      0.111        Jane

Betweeness

      0.389        Heather
      0.231        Fernando
      0.231        Garth
      0.222        Ike
      0.102        Diane
      0.023        Andre
      0.023        Beverly
      0.000        Carol
      0.000        Ed
      0.000        Jane

Closeness

      0.643        Fernando
      0.643        Garth
      0.600        Diane
      0.600        Heather
      0.529        Andre
      0.529        Beverly
      0.500        Carol
      0.500        Ed
      0.429        Ike
      0.310        Jane

Welcome to InFlow 3.01 (TM)
Copyright (C) 1988-2003, Vald
```

List of Computer Viruses

Author

G. Manigandaprabhu
II B.Sc(CS) 'B'

Article Title

List of Computer Viruses

Article Description

This article gives list of computer viruses developed from 1980s to 2008.

List of Computer Viruses Developed in 1980s

Elk Cloner Computer Virus - 1982

Among some of the earliest computer viruses this one is believed to be the first to go outside the computer system on which it was developed, which is why it is the first in our computer virus list. Elk Cloner was created by **Richard Skrenta**, a 15-year-old high school student, who made the virus for **Apple II** systems somewhere around 1982. The virus was able to spread by infecting the operating system on Apple II, which was stored on floppy disks. Just like the majority of the first computer viruses, the damaged caused by Elk Cloner were not high, but it did annoy a lot of users with the display of a poem that appeared on every 50th booting. It read:

- Elk Cloner: The program with a personality
- It will get on all your disks
- It will infiltrate your chips
- Yes it's Cloner!
- It will stick to you like glue
- It will modify ram too
- Send in the Cloner!

The Brain Computer Virus - 1986

The Brain virus plague started in 1986. It was the **first IBM PC computer virus** and was able to infect 360KB diskettes, thus spreading worldwide very fast.

The virus managed to infect a lot of computers simply because people were unprepared for computer viruses. The Brain was developed in Pakistan by two brothers: Basit and Amjad Farooq Alvi. Both worked as software vendors, and their goal was to learn about the degree of piracy in their country, but they were unaware that their program could spread outside Pakistan. It is worth mentioning that the Brain computer virus is considered to be the **first stealth virus**, and it comes second in our computer virus list.

The Vienna virus - 1987

In 1987 users witnessed the appearance of "Vienna" computer virus. It is the **first direct action virus**, which means that it instantaneously downloads into memory, shortly after that it infects other files, and afterwards the virus unloads itself. **Ralph Burger** was the one to receive a copy of the Vienna virus. He disassembled it, and then published his findings in his book entitled "Computer Viruses: a High-tech Disease". In his book, the author stated about the idea of developing computer viruses popular. Burger explained how to make viruses, thus, unintentionally leading to the creation of thousands of computer viruses that were developed by his readers.

The Jerusalem virus - 1987

In the Fall of 1987 the **Jerusalem University** was struck by a computer virus, which was ultimately dubbed the Jerusalem virus. This computer virus is preset in our computer virus list because it is considered to be one of the **first MS-DOS viruses** that led to a real pandemic. Computers worldwide were infected, including those from Europe, the United States and the Middle East. The Jerusalem virus was able to infect .COM, .EXE, .SYS, .BIN, and .PIF files.

Morris Virus - 1988

Until the appearance of this computer virus, other viruses spread on a somewhat smaller scale. Morris is present in our computer virus list because it is the first Internet computer virus that truly spread across the world. It was developed by a **Cornell University** graduate student, who also appeared to be the son of a top government computer-security specialist. This computer virus managed to infect around 6000 university and military machines, including the computers of **NASA research Institute** where it completely paralyzed the machines' work.

Datacrime virus - 1989

For the first time this computer virus was spotted in 1989. It led to a real hysteria at that time, but in the end it caused very little harm. The Datacrime virus overwrote parts of the HDD and displayed the following message: **"DATACRIME VIRUS' 'RELEASED: 1 MARCH 1989"**. Afterwards the virus formatted the first 9 tracks of the HDD.

The Fu Manchu virus - 1989

Tthis computer virus represented as modification of Jerusalem virus. The Fu Manchu Virus represents a computer virus able to infect .COM, .EXE and overlay files. After an infected program had been executer, the virus loaded into computer's memory and then struck the machine's runtime operation, damaging overlay files.

In 1980s there were some other viruses developed. Below you can find a small list of computer viruses that were also created during this period of time:

- - Vacsina;
- - Yankee;
- - Cascade;

- - Stoned;
- - Yale;
- - PingPong;
- - Lehigh;
- - "Suriv-1" a.k.a. "April1st";
- - Suriv-2;
- - Suriv-3.

List of Computer Viruses Developed in 1990s

The 1990s marked a great evolution of **computer viruses**, especially those that were created to infect Windows OS files. Below you will find a computer virus list that includes viruses created during the 1990s.

Chameleon polymorphic computer virus - 1991

First in the computer virus list are the first polymorphic viruses that appeared at the beginning of the last decade of the 20th century. The world faced a true problem associated with these viruses in April 1991. A real epidemic around the globe was caused in particular by the Tequila virus. Another popular polymorphic virus was the Chameleon. This computer virus was also known as V2P1, V2P2, and V2P6. After its appearance the developers of **anti-virus programs** were forced to search for other methods of virus detection. Here are some of the polymorphic viruses that appeared in this period: Bootache, CivilWar, Crusher, Dudley, Fly, Freddy, Ginger, Grog, Haifa, Moctezuma, MVF, Necros, Nukehard, PcFly, Predator, Satanbug, Sandra, Shoker, Todor, Tremor, Trigger and Uruguay.

Dedicated computer virus - 1992

The Dedicated virus appeared in 1992 and represented an encrypted computer virus that takes advantage of stealth techniques in order to avoid being spotted. It infected .COM files and that includes command. Com. As soon as the computer virus is loaded into memory (whenever an infected program is executed) it causes damage to the machine's runtime operation and affects program files.

Shifter, SrcVir and OneHalf - 1994

These three computer viruses appeared in 1994. The first one was the Shifter, computer virus that was able to infect object modules (OBJ files). In April the world witnessed the appearance of SrcVir that infected program source code (C and Pascal). June 1994 saw the introduction of OneHalf, considered to be one of the most dangerous computer viruses in Russia.

The Concept Virus - 1995

For the first time Concept was identified in August 1995, when Microsoft launched its popular operating system Windows 95. The computer virus was able to infect Word files and as long as the user used Microsoft Office application, the virus would work on an IBM PC or a Macintosh. The appearance of the Concept virus marked a turning point in the history of computer viruses and anti-viruses since it was the first "alive" virus for MS Word. In just a few month the computer virus infected a high number of machines around the globe that had MS Word installed.

Laroux computer virus - 1996

This virus was spotted in August 1996. It infected Microsoft Excel spreadsheets and just like in the case of the Concept, described previously in our computer virus list, the Laroux virus was identified almost simultaneously by a number of companies. The Laroux computer virus affected the files of Excel 5 and Excel for Microsoft's Windows 95.

Win.Tentacle - 1996

This computer virus caused the first Windows 3.x virus epidemic. It managed to infect a computer network in a hospital and in a number of other institutions located in France. The virus infected Windows 16 bit executable files. After staying in memory for some time it infected other Windows files. It was also noticed that the virus infected files with GIF extension.

W32.HLLP.DeTroie - 1998

Just like most of viruses described in our computer virus list, this one led to a real epidemic. Besides being able to infect Windows32 executed files, W32.HLLP.DeTroie could also convey to its "owner" the data stored on the infected machine. Due to the fact that the virus and some of its variants employed particular libraries that were attached only to the French version of Windows, only computers of the French speaking nations were affected. The virus was written in Delphi and it also had a backdoor capability, allowing the "owner" to access the infected system.

Happy99 computer virus – 1999

January of 1999 marked the beginning of the global epidemic of the Happy99 computer virus. As a matter of fact, Happy99 represented the first worm as we know it today, thus leading to a new chapter in the history of malware evolution. The virus used MS Outlook, which by that time had already been widely used by both European and American users. Although the virus appeared ten years ago, till nowadays it is considered to be one of the most widespread dangerous programs.

You can find more information on computer viruses here at www.InfoNIAC.com, please consider checking the links at the bottom of the story.

New computer viruses with highly unusual methods of infection

During the 1990s, a lot of new computer viruses started using highly unusual methods of infecting various files, loading into the computer system and more. Some of them include: PMBS, Strange (aka Hmm), Shadowgard, Carbunkle, Emmie, Metallica, Bomber, Uruguay and Cruncher.

Our computer virus list ends with several other viruses developed during the 1990s, these are:

- **1990:** Murphy, Nomenclatura, Beast;
- **1991:** Dir_II, Tequila;
- **1992:** Win.Vir_1_4, Michelangelo (a.k.a. March6);
- **1994:** SMEG.Pathogen, SMEG.Queeg;
- **1995:** NightFall, Nostardamus, Nutcracker, ByWay, DieHard2;
- **1996:** Win95.Punch, Laroux, OS2.AEP, Zhengxi, Win95.Boza;
- **1997:** Esperanto, Homer, ShareFun, Linux.Bliss;
- **1998:** Win95.CIH, RedTeam, Cross, AccessiV, Win95.HPS, Win95.Marburg, Excel4.Paix;
- **1999:** GaLaDRieL, ExploreZip, Toadie (a.k.a. Termite), Bubbleboy, KakWorm, FunLove, Vecna.

List of Computer Viruses from 2000 Onward

In the 21st century the number of computer viruses considerably increased. Our computer virus list features descriptions of a large number of dangerous **computer viruses**, worms and Trojans that appeared starting with 2000 and till this day.

Inta - 2000

This computer virus was released by the members of an underground group called 29 A. As soon as the virus was released, it attacked Windows 2000 files even before the software giant, Microsoft, managed to announce the commercial version of its OS. Inta was the first computer virus to infect Windows 2000.

LoveLetter - 2000

This script virus caused a real pandemic on May 5, 2000. Most users were unaware of the fact that VBS and TXT files could cause harm, but they did, being infected with this dangerous virus. As soon as the virus is uploaded, it destroys numerous files and then sends itself to everyone in the MS Outlook contact list.

Timofonica - first cellular virus - 2000

For the first time the Timofonica virus was spotted on June 6, 2000. It was the first mobile phone virus. Besides being able to spread through email, the virus also sent messages to different mobile phones that were in the MoviStar cellular network, owned by Telefonica, global telecommunications giant.

Liberty virus - 2000

This computer virus was identified in August. It is considered to be the first Trojan to be able to affect PalmOS of Palm Pilot, which is why it was included in our computer virus list. When the virus was installed on the machine, it deleted files. However, the good news is that the virus could not replicate itself.

Mandragore - 2001

The year 2001 was the one in which instant messaging services registered a significant increase in popularity. Some of them were ICQ and MS Instant Messenger, thus they served as guinea pigs for spreading malicious code. The Internet worm Mandragore used these services to install into the system and copy itself to Windows CurrentUser startup directory as "Gspot.exe" file. Because it was placed in the Startup folder, the worm was automatically run by the operating system on the next Windows startup. Then it ran two background processes, while remaining in Windows memory. The threads displayed two messages: "I'm Gnutella node, and here is file you are looking for." and "the filename you are looking for" with ".exe" extension, and with worm code in it."

Ramen - 2001

This computer virus managed to affect numerous corporate networks in just a few days. It penetrated NASA, A&M University as well as the Taiwanese hardware vendor Supermicro. Shortly after the launch of the virus, a lot of clones appeared along with a large number of new Linux worms. Ramen was a 300K multi-component worm that included 26 files and is the first known computer virus to infect RedHat Linux systems. You can find more information about

Klez - 2002

The Klez worm-virus managed to cause serious trouble in 2002. Initially detected on October 26 it continued to be considered one the most dangerous malware for the next two years. By the end of 2002, about 60 percent of all infections were the result of the Klez virus. Written in Microsoft Visual C++, it spread through the Internet, being attached to emails.

Slapper – 2002

This Internet worm was able to infect computers that run on Linux. The virus' source was about 68.4KB in size. Not only did it infect computer, it also managed to spread further, being able to act as a backdoor on the infected machine. Thus it made possible for the attacker to run different commands and start Denial-of-Service attacks by taking advantage of a distributed network maintained between the infected computers.

Lentin (aka Yaha) - 2002

Just like Klez this computer virus spread over the Internet being attacked to infected emails. It represents a mass-mailing worm that initially looks for emails in Windows Address Book, MSN, .NET messenger cache folders as well as HTM(L) files. It was able to spread with the help of a 'VALENTIN.SCR' file attached to a message that read:

- Subject 1:
- Melt the Heart of your Valentine with this beautiful Screen saver
- Body 1:
- This e-mail is never sent unsolicited. If you need to unsubscribe, follow the instructions at the bottom of the message.

Slammer - 2003

This Internet worm features in our computer virus list because it is the first fileless worm. Slammer was able to spread by taking advantage of the vulnerability found in the SQL Server. It fully showed the abilities of a flash-worm. The worm caused a denial of service on several Internet hosts and considerably slowed down the overall Internet traffic. The computer virus managed to infect about 75,000 computers in just 10 minutes.

Lovesan – 2003

This computer worm for the first time appeared in August 2003, showing the vulnerability of Windows. Lovesan took advantage of the vulnerability of the operating system in order to replicate itself - a technique similar that used by the Slammer. The virus downloads and the tries to run a file called msblast.exe. In addition, the user receives the following message:

- "I just want to say LOVE YOU SAN!!
- billy gates why do you make this possible? Stop making money and fix your software!!"

Mimail - 2003

This computer worm used the newest vulnerability in Internet Explorer in order to activate itself. It is worth mentioning that the vulnerability made it possible for the worm to extract the binary code from HTML files and the execute it. For the first time Minmail was used in Russia.

Zotob - 2005

This computer virus was launched on August 14, 2005. It used the Plug and Play (PnP) vulnerabilities, thus making big problems on the system. When Zotob infects a machine, it slows it down, causing the computer to repeatedly crash and reboot. Infected computers running Windows 2000 were left exposed to additional attacks, while those that run Windows XP only spread the worms.

Strorm - 2007

This computer virus holds a special place in our computer virus list. For the first time Storm was spotted at the beginning of 2007. It hid in email attachments that had the following title line: "230 dead as storm batters Europe." Users that opened the attachment let the virus in and their machines joined an ever-growing botnet. Security experts spread in opinions regarding the number of computers that were infected with this computer virus: some say that the number reached 10 million, while others claim that between a few thousand and about 1 million computers were infected. Computers infected with Storm virus could be used to launch millions of spam emails that would advertise Web links, and if someone clicked those links, they would download the computer virus on their machine. The Storm botnet was able to attack the online operations carried out by security vendors and analysts who tried to investigate the computer virus. The United States Federal Bureau of Investigation believes that Storm represents a major treat to increased bank fraud, identity theft, and a number of other cybercrimes.

The Conficker - 2008

This is a computer worm that for the first time was spotted in November 2008. Besides infecting the user's computer, the worm spreads to other machines throughout the network automatically. It managed to affects the computers of the French Navy, UK Ministry of Defense, Sheffield Hospital, German Bundeswehr as well as Norwegian Police. Microsoft decided to give away $250,000 for valuable information that could help capture the developer of Conficker.

W32.Dozer - 2009

Detected this year, the computer worm can load malicious files onto the infected machine. It was developed to delete information on infected computers and prevent them from being rebooted.

Other viruses that appeared during this period of time include:

2000: Dilber,CIH, SK, Bolzano, Jer, Stream, Fable, Pirus, Hybris;

2001: CodeRed, Nimda, Aliz, BadtransII, Magistr, SirCam, California.IBM, Girl Thing;

2002: LFM, Donut, Tanatos (aka Bugbear), Thus, TheSecond, Marker, Flop, Elkern, CIH, FunLove, Spaces;

2003: Ganda, Avron, Sobig, Tanatos.b, I-Worm.Swen, Backdoor.Agobot, Afcore;

2004: Witty worm, Nuclear RAT, Vundo, Bitfrost, Santy, Stratio-Zip, Netsky-D and MyDoom-O;

2005: Samy XSS, Zlob Trojan, Bandook;

2006: OSX/Leap-A, Stration (a.k.a. Warezov);

2008: MacSweeper, Sinowal (a.k.a. Mebroot), The Koobface.

Freeware

Author

M. Mohammad arif , *II B.Sc(CS) B*

<u>Article Title</u>

Freeware

<u>Article Description</u>

This article gives information about different types of freeware and it's technical details.

Nero Lite 9.4.12.708b

Nero Inc - 31.64MB (Freeware)

Nero Free, is the easy-to-use yet powerful multimedia suite, gives you the freedom to create, rip, copy, burn, edit, share, and upload online. Whatever you want – music, video, photo, and data –

share and enjoy with family and friends anytime, anywhere.

Title:	Nero Lite 9.4.12.708b
Filename:	Nero-9.4.12.708b_lite.exe
File size:	31.64MB (33,177,736 bytes)
Requirements:	Windows XP / 2003 / Vista / Windows7 / XP64 / Vista64 / Windows7 64
Languages:	en-US
License:	Freeware
Date added:	March 29, 2010

CCleaner 2.30.1130

Piriform - 3.22MB (Freeware)

CCleaner is a freeware system optimization, privacy and cleaning tool. It removes unused files from your system - allowing Windows to run faster and freeing up valuable hard disk space. It also cleans traces of your online activities such as your Internet history. Additionally it contains a fully featured registry cleaner. But the best part is that it's fast (normally taking less than a second to run) and contains NO Spyware or Adware! :)

Cleans the following:

- Internet Explorer
- Firefox
- Google Chrome
- Opera
- Safari
- Windows - Recycle Bin, Recent Documents, Temporary files and Log files.
- Registry cleaner
- Third-party applications
- 100% Spyware FREE

Title:	CCleaner 2.30.1130
Filename:	ccsetup230.exe
File size:	3.22MB (3,376,656 bytes)
Requirements:	Windows (All Versions)

Languages:	en-US, es-ES, ja-JP, pl-PL
License:	Freeware
Author:	Piriform

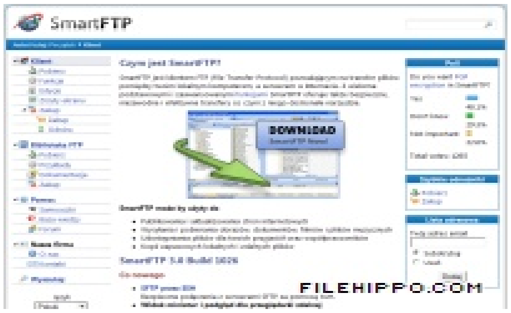
SmartFTP 4.0.1092.0

SmartFTP - *12.93MB(Commercial Trial)*

SmartFTP is an FTP (File Transfer Protocol) client which allows you to transfer files between your local computer and a server on the Internet. With its many basic and advanced features SmartFTP also offers secure, reliable and efficient transfers that make it a powerful tool.

SmartFTP can be used for:

- Web site publishing and maintenance
- Upload and download of images, documents, movie and music files
- Share your files with your friends and coworkers
- Backups of local or remote files



SmartFTP offers these features:

- Quickly rename multiple files.
- Search your hard drive in the Local Browser (Windows Vista and higher)

Title:	SmartFTP 4.0.1092.0
Filename:	SFTPMSI.exe
File size:	12.93MB (13,557,376 bytes)
Requirements:	Windows 2000 / XP / 2003 / Vista / Windows7 / XP64 / Vista64 / Windows7 64
Languages:	en-US
License:	Commercial Trial

Thunderbird 3.0.4

Mozilla Organization - 8.61MB (Open Source)

Thunderbird is a great email client from the same people who brought you the Firefox browser.

Thunderbird gives you IMAP/POP support, a built-in RSS reader, support for HTML mail, powerful quick search, saved search folders, advanced message filtering, message grouping, labels, return receipts, smart address book LDAP address completion, import tools, and the ability to manage multiple e-mail and newsgroup accounts.

- Tabbed email
- An Archive feature similar to the one in GMail
- Lightning fast search
- Smart folders

Mozilla's Thunderbird 2 email application is more powerful than ever.

Title:	Thunderbird 3.0.4
Filename:	Thunderbird Setup 3.0.4.exe
File size:	8.61MB (9,028,040 bytes)
Requirements:	Windows (All Versions)
Languages:	en-US
License:	Open Source
Author:	Mozilla Organization

SuperAntiSpyware 4.35.1002

SUPERAntiSpyware - 7.53MB (Freeware)

SUPERAntiSpyware Professional features our highly advanced Real-Time Protection to ensure protection from installation or re-installation of potential threats as you surf the Internet. Used in conjunction with our First Chance Prevention and Registry Protection, your computer is protected from thousands of threats that attempt to infect and infiltrate your system at startup or while shutting down your system.

Advanced Detection and Removal

- Detect and Remove Spyware, Adware, Malware, Trojans, Dialers, Worms, KeyLoggers, HiJackers, Parasites, Rootkits, Rogue Security Products and many other types of threats.
- Light on System Resources and won't slow down your computer like many other anti-spyware products. Won't conflict with your existing anti-spyware or anti-virus solution!

Real-Time Protection

- Real-Time Blocking of threats! Prevent potentially harmful software from installing or re-installing!
- First Chance Prevention examines over 50 critical points of your system each time your system starts up and shuts down to eliminate threats before they have a chance to infect and infiltrate your system.
- Schedule either Quick, Complete or Custom Scans Daily or Weekly to ensure your computer is free from harmful software.

Title:	SuperAntiSpyware 4.35.1002
Filename:	SUPERAntiSpyware.exe
File size:	7.53MB (7,899,168 bytes)
Requirements:	Windows (All Versions)
Languages:	en-US, es-ES, pl-PL
License:	Freeware
Author:	SUPERAnti Spyware

SuperAntiSpyware 4.35.1002

SUPERAntiSpyware - 7.53MB (Freeware)

SUPERAntiSpyware Professional features our highly advanced Real-Time Protection to ensure protection from installation or re-installation of potential threats as you surf the Internet. Used in conjunction with our First Chance Prevention and Registry Protection, your computer is protected from thousands of threats that attempt to infect and infiltrate your system at startup or while shutting down your system.

Advanced Detection and Removal

- Detect and Remove Spyware, Adware, Malware, Trojans, Dialers, Worms, KeyLoggers, HiJackers, Parasites, Rootkits, Rogue Security Products and many other types of threats.
- Light on System Resources and won't slow down your computer like many other anti-spyware products. Won't conflict with your existing anti-spyware or anti-virus solution!

Title:	SuperAntiSpyware 4.35.1002
Filename:	SUPERAntiSpyware.exe
File size:	7.53MB (7,899,168 bytes)
Requirements:	Windows (All Versions)
Languages:	en-US, es-ES, pl-PL
License:	Freeware
Author:	SUPERAntiSpyware www.superantispyware.com

Real-Time Protection

- Real-Time Blocking of threats! Prevent potentially harmful software from installing or re-installing!
- First Chance Prevention examines over 50 critical points of your system each time your system starts up and shuts down to eliminate threats before they have a chance to infect and infiltrate your system.

- Schedule either Quick, Complete or Custom Scans Daily or Weekly to ensure your computer is free from harmful software.

Internet Explorer 9 Features

Author

Ms.F.Regina Mary
Lecturer, CS

Article Title

Micorsoft Internet Explorer 9 Features

Article Description

This article gives information about the features of Microsoft Internet Explorer 9.

Microsoft Internet Explorer 9 is the new virson of Internet Explorer 8 made by Microsoft Corporation. According to wikipedia the new virson of Internet explorer is currently in development which has complete or nearly complete support for all CSS 3 selectors, border-radius CSS 3 property, faster JavaScript, and hardware accelerated rendering using Direct2D and DirectWrite. Also Microsoft has displayed some dedication to passing the Acid3 test which may mean SVG support in Internet Explorer 9.

Internet Explorer 9 Features:

Internet Explorer has been designed to view a broad range of web pages and to provide certain features within the operating system, including Microsoft Update. During the heyday of the historic browser wars, Internet Explorer superseded Netscape only when it caught up technologically to support the progressive features of the time.

Standards support

Internet Explorer, using the Trident layout engine:

* fully supports HTML 4.01, CSS Level 1, XML 1.0 and DOM Level

1, with minor implementation gaps.

* fully supports XSLT 1.0 as well as an obsolete Microsoft dialect of XSLT often referred to as WD-xsl, which was loosely based on the December 1998 W3C Working Draft of XSL. Support for XSLT 2.0 lies in the future: semi-official Microsoft bloggers have indicated that development is underway, but no dates have been announced.

* partially supports CSS Level 2 and DOM Level 2, with major implementation gaps and conformance issues. Almost full conformance to CSS 2.1 has been added in the Internet Explorer 8 release.

* does not support XHTML, though it can render XHTML documents authored with HTML compatibility principles and served with a text/html MIME-type.

* does not support SVG, in any version.

Internet Explorer uses DOCTYPE sniffing to choose between “quirks mode” (renders similarly to older versions of MSIE) and standards mode (renders closer to W3C’s specifications[citation needed]) for HTML and CSS rendering on screen (Internet Explorer always uses standards mode for printing). It also provides its own dialect of ECMAScript called JScript.

Internet Explorer has been subjected to criticism over its limited support for open web standards.

Non-standard extensions

Internet Explorer has introduced an array of proprietary extensions to many of the standards, including HTML, CSS and the DOM. This has resulted in a number of web pages that appear broken in standards-compliant web browsers and has introduced the need for a “quirks mode” to allow for rendering improper elements meant for Internet Explorer in these other browsers.

Internet Explorer has introduced a number of extensions to JScript which have been adopted by other browsers. These include the innerHTML property, which returns the HTML string within an element; the XMLHttpRequest object, which allows the sending of HTTP request and receiving of HTTP response; and the designMode attribute of the contentDocument object, which enables rich text editing of HTML documents. Some of these functionalities were not possible until the introduction of the W3C DOM methods. Its Ruby character extension to HTML is also accepted as a module in W3C XHTML 1.1, though it is not found in all versions of W3C HTML.

Microsoft submitted several other features of IE for consideration by the W3C for standardization. These include the ‘behavior’ CSS property, which connects the HTML elements with JScript behaviors (known as HTML Components, HTC); HTML+TIME profile, which adds timing and media synchronization support to HTML documents (similar to the W3C XHTML+SMIL); and the VML vector graphics file format. However, all were rejected, at least in their original forms. VML was, however, subsequently combined with PGML (proposed by Adobe and Sun), resulting in the W3C-approved SVG format, currently one of the few vector image formats being used on the web, and which IE is now virtually unique in not supporting.

Other non-standard behaviors include: support for vertical text, but in a syntax different from W3C CSS3 candidate recommendation; Support for a variety of image effects[40] and page transitions, which are not found in W3C CSS; Support for obfuscated script code, in particular JScript.Encode(). Support for embedding EOT fonts in web pages.

Favicon

The favicon (short for “favorites icon”) introduced by Internet Explorer is now also supported and extended in other browsers. It allows web pages to specify a 16-by-16 pixel image for use in bookmarks. In IE, support was provided only for the native Windows ICO format; in other browsers it has now been extended to other types of images such as PNG and GIF.

Usability and accessibility

Organizing Favorites in Internet Explorer 6 Internet Explorer makes use of the accessibility framework provided in Windows. Internet Explorer is also a user interface for FTP, with operations similar to that of Windows Explorer (although this feature requires a shell window to be opened in recent versions of the browser, rather than natively within the browser). Visual Basic for Applications (VBA) is not supported, but available via extension (iMacros). Recent versions feature pop-up blocking and tabbed browsing. Tabbed browsing can also be added to older versions by installing Microsoft’s MSN Search Toolbar or Yahoo’s Yahoo Toolbar.

WINDOWS 7 NEW FEATURES

Author

K.Dhanapal
I-BCA-C

Article Title

Windows 7 new features

Article Description

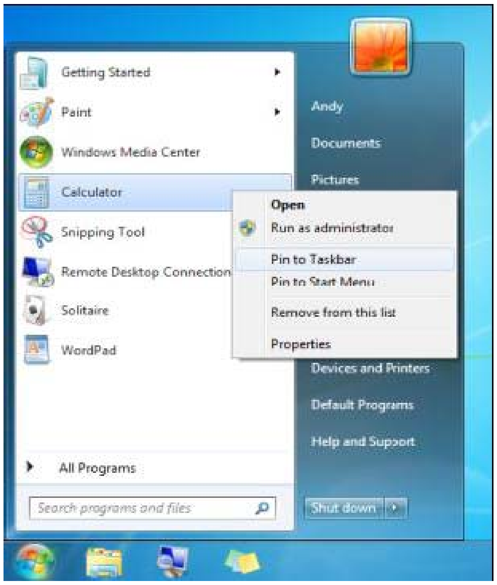
This article gives information about the new features of Windows 7.

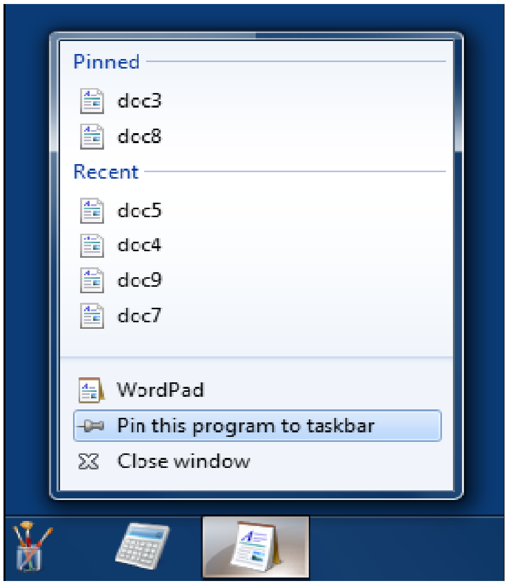
Pin a program to the taskbar

You can pin a program directly to the taskbar so that you can open it quickly and conveniently, rather than having to look for the program in the Start menu each time. Here's how:

□ If the program isn't running, click the **Start** button, click **All Programs**, find the program you want, right-click it, and then click **Pin to Taskbar**.

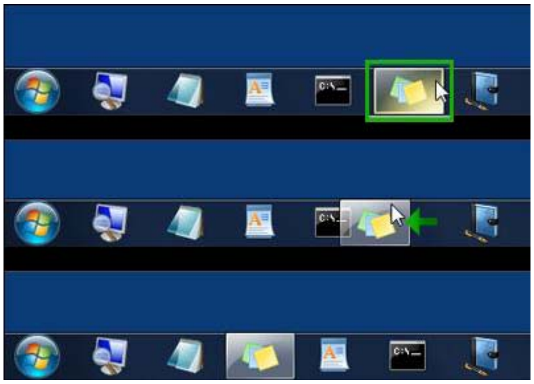
□ If the program is already running, right-click the program button on the taskbar, and then click **Pin this program to taskbar**.





Rearrange buttons on the taskbar

You can rearrange and organize program buttons on the taskbar so they appear in the order you prefer. To rearrange the order of program buttons on the taskbar, just drag a button from its current position to a different position on the taskbar.



Using Jump Lists

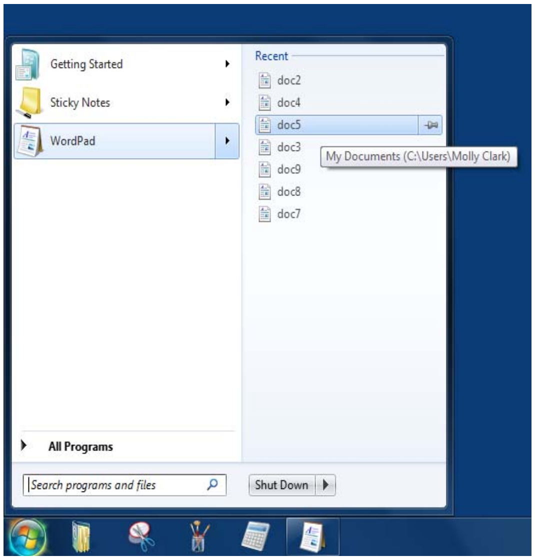
Jump Lists are lists of recent items, such as files, folders, or websites, organized by the program that you use to open them.

You can open programs, recent items, and favorite items using Jump Lists so that you can quickly get to the items you use every day. Here are some ways to use Jump Lists:

To open an item from a Jump List

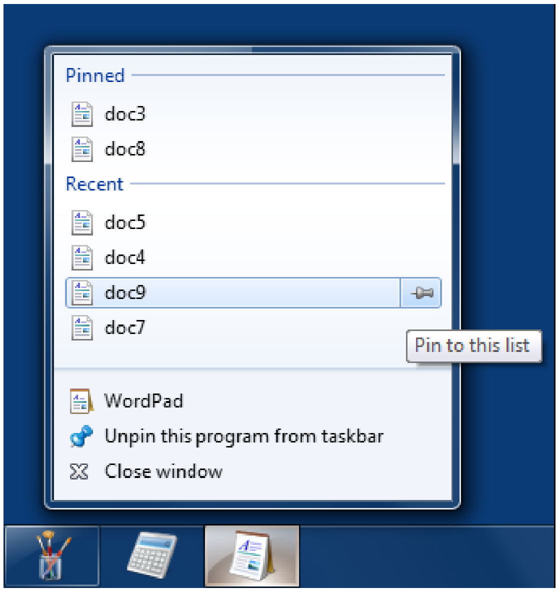
You can view the Jump List and then open items both from the taskbar and the Start menu. Here's how:

□ Right-click the program's icon on the taskbar, and then click the item.



- or -

□ Click the **Start** button, point to a pinned program or recently used program, point to or click the arrow next to the program, and then click the item.



To pin and unpin an item to a Jump List

You can pin a favorite item to a Jump List, so it will always appear at the top of the list. That way, you'll be able to get to the file quickly and easily. Here's how:

 To pin an item to a Jump List, open the program's Jump List, point to the item, click the pushpin icon, and then click **Pin to this list**.

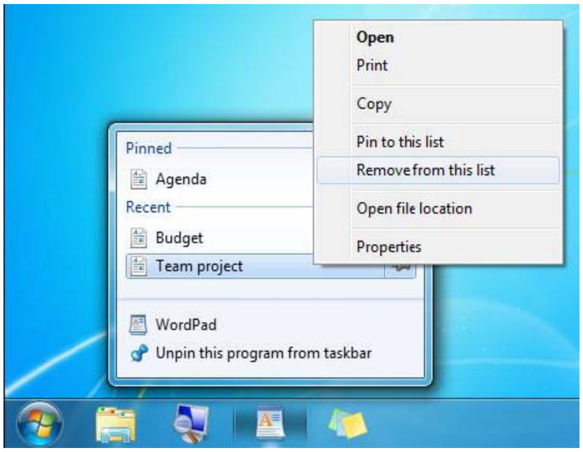
 To remove an item from a Jump List, open the program's Jump List, point to the item, click the pushpin icon, and then click **Unpin from this list**.

To change the order of items in a Jump List

To change the order of either pinned items or recent items, open the Jump List, and then drag the item to a different position.

To remove a recent item from a Jump List

To remove a recent item entirely from a Jump List, open the Jump List, right-click the item, and then click **Remove from this list**. Don't worry, you won't delete the file, you're just removing it from the Jump List. The next time you open that item, it might reappear in the Jump List again.

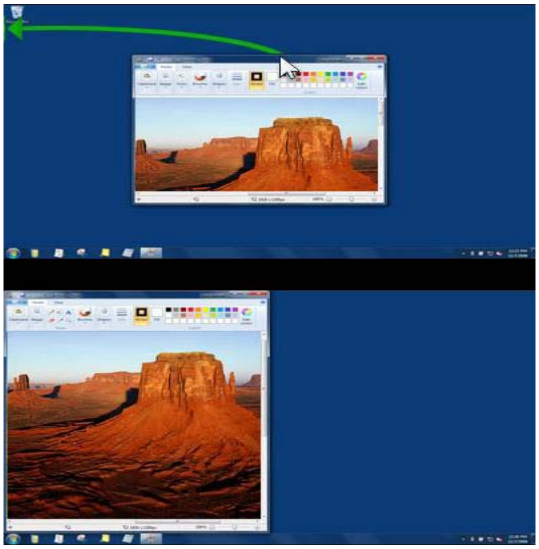


Snap a window to the side

You can use Snap to arrange windows side by side, which can be especially helpful when comparing two documents or when dragging files from one place to another. Here' how:

1. Drag the title bar of a window to the left or right side of the screen until an outline of the expanded window appears.
2. Release the title bar to expand the window.

3. Repeat steps 1 and 2 with another window to arrange the windows side by side.



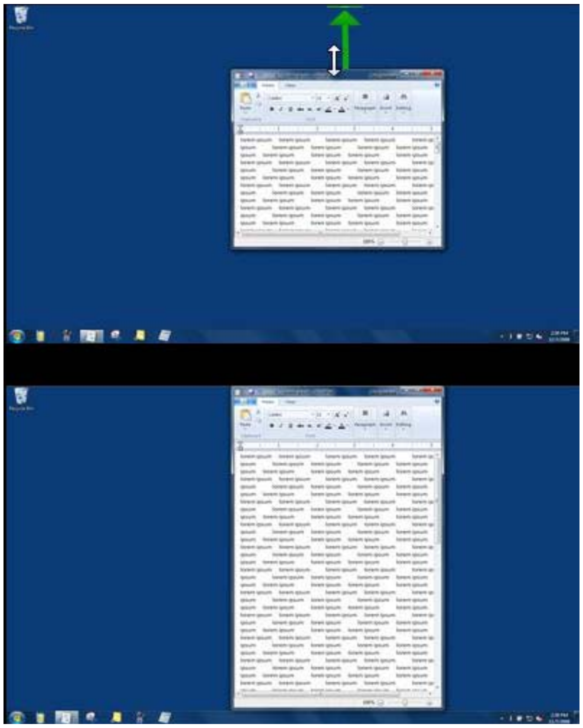
To return the window to its original size, drag the title bar away from the top of the desktop, and then release.

Snap a window vertically

You can use Snap to expand windows vertically, which can be especially helpful for reading longer documents. Here's how:

1. Point to the top or bottom edge of an open window until the pointer changes into a double-headed arrow.

2. Drag the edge of the window to the top or bottom of the screen to expand the window to the entire height of the desktop. The width of the window doesn't change.



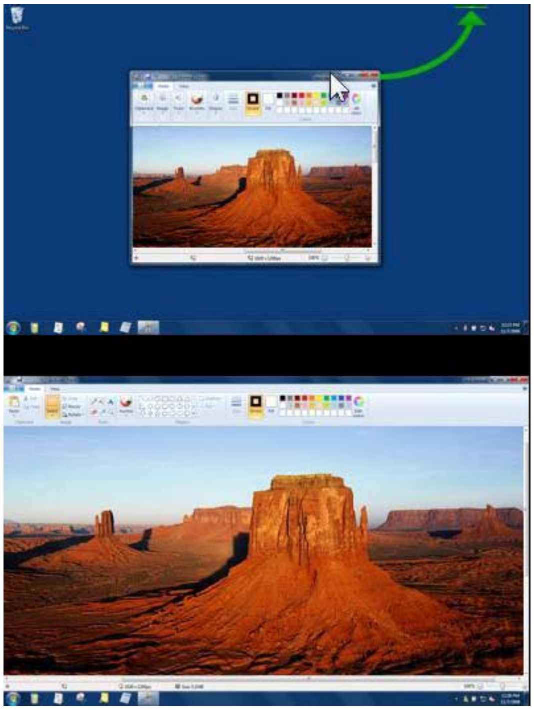
To return the window to its original size, drag the title bar away from the top of the desktop, or drag the bottom edge of the window away from the bottom of the desktop.

Snap a window to the top

You can use Snap to maximize a window, which makes it easier to focus solely on that window with less distraction from other open windows. Here’s how:

1. Drag the title bar of the window to the top of the screen until an outline of the expanded window appears.

2. Release the title bar to expand the window to fill the entire desktop.

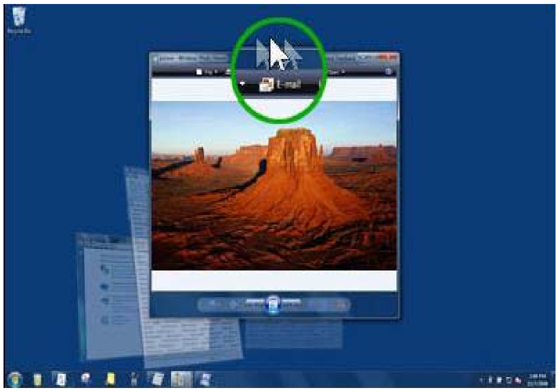


Minimize open windows using Aero Shake

You can use Aero Shake to quickly minimize every open window except the one you want. You can then restore all of your windows just as easily. Here’s how:

1. In the window you want to keep open, drag (or shake) the title bar back and forth quickly.

2. To restore the minimized windows, shake the open window again.



SKIPFISH

Author

AR.abdul jabbar sheriff,
II Bsc(cs) B

Article Title

Google’s Skipfish

Article Description

This article helps to know about the Gooogle’s Web Security Scanner called SKIPFISH.

Google has released an open-source web-security scanner called Skipfish that is designed to allow people to scan web applications for security holes.

The tool scans a web application for flaws including "tricky scenarios" such as blind SQL or XML injection, Google developer Michal Zalewski said in the Skipfish wiki.

Skipfish prepares a sitemap annotated with interactive crawl results, highlighting flaws, after a recursive crawl and dictionary-based probing of the target site. The tool can also generate a final report that can be used as a basis for a security assessment.

That there are already a number of both commercial and open-source scanning tools available, including Nikto and Nessus, and recommended that people use the tool that suits them. However, that Skipfish is high performance, with over 500 requests per second against internet targets, and over 2,000 requests per second on LANs, depending on the capabilities of the server being tested.

Skipfish is "not a silver bullet", saying the tool deliberately does not satisfy the majority of the requirements outlined in the Wasc Web Application Security Scanner Evaluation Criteria. In addition, Skipfish does not come with an extensive database of known vulnerabilities.

Opera & the Freedom of Choice
Go to Ubuntu 9.10 – real life experiences
Get lots of free content for Amazon Kindle

Google asked people to use the tool responsibly. "First and foremost, please do not be evil," said by Zalewski. "Use Skipfish only against services you own, or have a permission to test."

The tool, which is written in pure C, is provided under Apache Licence 2.0. The most recent version of Skipfish available is the 1.10 beta.

Penryn processors

Author

S.Sundarraj,
III BCA ‘C’

Article Title

Penryn Processors

Article Description

This article gives information about Intel’s Penryn processors.

Intel has officially launched its next-generation processors based on the 45-nanometer manufacturing process.

Codename Penryn, it consists of a family of chips for desktops, notebooks and servers, based on Intel's Core Microarchitecture, and is available in dual-core or quad-core configurations.

Adesh Gupta, regional platform architecture manager for the server platform group at Intel Asia-Pacific, told ZDNet Asia in a phone interview today that 15 server processors--including 12 quad-core chips and three dual-core chips--as well as one high-end PC processor have been launched. The mainstream versions of Penryn will be available in the first quarter of 2008.

The 12 new quad-core chips boast clock speeds ranging between 2GHz and 3.20GHz, with front-side bus speeds up to 1,600MHz, and cache sizes of 12MB. The three new dual-core chips feature clock speeds of up to 3.40GHz, and front-side bus frequency of up to 1,600MHz, and cache sizes of 6MB, according to Intel.

Intel first revealed details of Penryn a year ago, and showed off the 45-nanometer chips in January this year.

Essentially a shrink of its Core 2 Duo chips, Penryn is built with a 45-nanometer manufacturing process, which lets chipmakers cut out more processors from a piece of silicon wafer, while improving energy efficiency. In addition, the transistors within the Penryn chips are using Intel's Hafnium-based high-k metal gate (Hi-k) formula for the first time, according to the company.

Comparing Penryn to its predecessor, Gupta noted that the die size of the chip has been "significantly reduced" by approximately 25 percent to 30 percent. The die size has shrunk from 143 square millimeters to 107 square millimeters.

While the die size of the processor has been reduced, the number of transistors within the processor has increased by about 30 percent. "It has gone up from 582 million transistors on a 65-nanometer die to 820 million transistors for a quad-core [processor] on a 45-nanometer die."

The cache size of the processor has also increased by about 50 percent, "from 8MB of level 2 cache to 12MB of level 2 cache", the 45-nanometer chips have given the front-side bus frequency a boost. Speeds have gone up from 1333MHz to 1600MHz.

"So overall, the smaller dies which are highly energy efficient deliver up to 61 percent improvement in performance for high-performance computing (HPC) applications".

Penryn will come with new features, such as the SSE4 instructions--the fourth generation of Streaming SIMD (single instruction, multiple data) Extensions, which are "47 new instructions that speed up workloads including video encoding for high-definition and photo manipulation, as well as key HPC and enterprise applications".

SIMD lets a chip take the same action with more than one data element, instead of requiring an instruction to be paired with each element--an approach that economizes many operations dealing with graphics, video and audio.

It look forward into the future, the 45-nanometer [processor] will give us the ability to enter into segments of markets like mobile Internet devices, consumer electronics or even low-cost computers, which really require processors which are highly integrated, dissipate significantly less amount of heat, but deliver exceptional performance,".

"For Intel, the 45-nanometer [processor] is like a magic for us...giving us the ability to significantly leap forward, in terms of innovation, new opportunities, new segments [and] new markets,".

In the second half of 2008, Penryn will undergo a microarchitecture transition--codename Nehalem, which will "unlock the potential" of the 45-nanometer chip.

Microsoft is ready with the final versions of its Visual Studio 2010 developer tools software and Silverlight 4, as well as version 4 of the .Net Framework.

Microsoft's Updated Version

Author

V.Kavitha
Lecturer, CS

Article Title

Micorsoft's Updated Version

Article Description

This article gives information about Microsoft's Updated Version.

The company is announcing the launch of the three products on Monday at a Visual Studio developer conference in Las Vegas. Visual Studio 2010 and the updated .Net Framework are now broadly available, Microsoft said, while Silverlight 4 will be made available for download later this week.

"The functionality of Visual Studio 2010, .Net Framework 4, and Silverlight 4 creates a powerful and unique combination, opening up new opportunities for developers to build applications that take advantage of new and existing devices, as well as emerging platforms like cloud services."

The new version of Visual Studio includes a TiVo-like function for tracking how a program behaves, a feature now called IntelliTrace. Visual Studio 2010 also includes support for Windows 7 and Windows Azure, as well as tools for building on top of Microsoft's Sharepoint product.

Microsoft had originally planned to release Visual Studio 2010 on March 22, but delayed the launch by a few weeks to resolve some performance issues.

As for the Silverlight update, it adds improved out-of-the-browser capabilities, among other enhancements. Despite some glitches--and a notable falling-out with Major League Baseball, Microsoft's Flash rival has been on a bit of a roll, including its use by NBC for the Vancouver Olympics as well as Microsoft's decision to make it one of the main ways to write applications for Windows Phone 7.

Mailing List

To whom we send

- The Vice-Chancellor, Periyar University ,Salem-11
- The Registrar, Periyar University ,Salem
- The Controller of Examination, Periyar University ,Salem-11
- The HOD, Department of Computer Science, Periyar University,Salem-11
- The HOD, Government Arts College for Women, Salem-8
- The HOD, Government Arts College for Women , Krishnagiri
- The HOD, Government Arts & Science College (W), Burgur, Kirshnagiri
- The HOD, J.K.K Nataraja College of Arts & Science
- The HOD, M.G.R College of Arts & Science
- The HOD, Sengunthar Arts & Science College
- The HOD, Muthayammal College of Arts & Science
- The HOD, PEE GEE College of Arts &, Science
- The HOD, Harur Muthu Arts & Science College for Women
- The HOD, Vivekanandha College of Arts & Sciences (W)
- The HOD, Mahendra Arts & Science college
- The HOD, Selvam Arts & Science college
- The HOD, St.Joseph's College of Arts & Science for (W)
- The HOD, Vysya College of Arts &, Science
- The HOD, NKR Government Arts College for Women

- **The HOD, Arignar Anna Government Arts College**
- **The HOD, Salem Sowdeswari College**
- **The HOD, P.G.P College of Arts & Science**
- **The HOD, Attur Arts & Science College**
- **The HOD, SSM College of Arts & Science**
- **The HOD, Government Arts College Salem**
- **The HOD, Government Arts College Men**
- **The HOD, Government Arts College, Dharmapuri**
- **The HOD, Gobi Arts and Science College (Autonomous)**
- **The HOD, Sri Kandhan College of Arts & Science**
- **The HOD, Sri Ganesh College of Arts & Science**
- **The HOD, Jairam Arts & Science College**
- **The HOD, Sri Balamurugan College of Arts & Science**
- **The HOD, PSG College of Arts and Science**
- **The Secretary, PSG College of Arts and Science**
- **The HOD, Kongunadu Arts and Science College(Autonomous)**
- **The HOD, Vivekanandha College for Women**
- **The HOD, Sri Vidhya Mandir Arts & Science College**
- **The HOD, *St.*John's College *Palayamkottai* - 627 007**
- **Mr. S.T.Rajan, St. Joseph's College, Trichy**

Overview of 3G/IMT-2000 standards

ITU IMT-2000	common name(s)		bandwidth of data	pre-4G	duplex	channel	description	geographical areas
TDMA Single-Carrier (IMT-SC)	EDGE (UWT-136)		EDGE Evolution	*none*		TDMA	evolutionary upgrade to GSM/GPRS	worldwide, except Japan and South Korea
CDMA Multi-Carrier (IMT-MC)	CDMA2000		EV-DO	UMB	FDD	CDMA	evolutionary upgrade to cdmaOne (IS-95)	Americas, Asia, some others
CDMA Direct Spread (IMT-DS)	UMTS	W-CDMA	HSPA	LTE			family of revolutionary standards.	worldwide
CDMA TDD (IMT-TC)		TD-CDMA						Europe
		TD-SCDMA						China
FDMA/TDMA (IMT-FT)	DECT		*none*		TDD	FDMA/TDMA	short-range; standard for cordless phones	Europe, USA
IP-OFDMA			WiMAX (IEEE 802.16)			OFDMA		worldwide

We welcome your valuable comments, suggestions & articles to
Ishare, Department of Computer Science & Applications (UG)
K.S.R College of Arts and Science, Tiruchengode-637215
Phone: 04288 -274741(4), Mail : ksrcas.ishare@gmail.com

Finally the CPU becomes inside the keyboard