

SEARCH



2012 San Diego International Conference on Child and Family Maltreatment

Virtualization



What is SEARCH?

- Non-profit based in Sacramento, CA
- Funded to offer assistance to law enforcement throughout the country

The screenshot shows the SEARCH website homepage. At the top left is the SEARCH logo with the tagline "The online resource for justice and public safety decision makers". Navigation links include HOME, CAREERS, CONTACT US, ABOUT SEARCH, PRODUCTS & SERVICES, PROGRAMS, PUBLICATIONS, and CALENDAR. A search bar is located on the right. The main content area features a "Celebrating 40 Years of Leadership" banner (1969-2009) with the text "JUSTICE, PUBLIC SAFETY AND BEYOND". Below this is a yellow button for "Register Today! 2011 Winter Membership Meeting". A central image shows hands in handcuffs. To the right is a "In the Spotlight" section titled "SEARCH Offers High-Tech Crime Investigative Resources" with a "LEARN MORE" button. On the far right is a "Quick Links" sidebar with items like "CRIMINAL HISTORY RECORDS", "HIGH-TECH INVESTIGATIVE GUIDES", "IDENTITY THEFT", "ISP LIST", "JIEM® TOOL", "PODCASTS", "PUBLIC SAFETY ISSUE BRIEFS", "SEARCH INVESTIGATIVE TOOLBAR", "SEX OFFENDER REGISTRIES", and "SURVEYS". A video player interface is visible at the bottom of the spotlight section.



What is SEARCH?

www.search.org

- Low-cost (or free) law enforcement training around the U.S.
 - Introduction to Computer Crime
 - Cell Phone Data Recovery
 - Advanced Responders: Search and Seizure of Networks
 - Social Networking Website Investigations
 - Peer-to-Peer



What is SEARCH?

- Free technical assistance to federal, tribal, state and local LE
- Other resources
 - SEARCH ISP List
 - SEARCH Investigative Toolbar
 - Whitepapers
 - LE conference speakers



Who We Are

Chris Armstrong

High-Tech Crime Training Specialist

carmstrong@search.org



Who We Are

Timothy Lott

High-Tech Crime Training Specialist

tim@search.org



Virtualization

What is Virtualization

In layman's terms a computer operating system running within a computer operating system.

For Instance: Windows XP running within the Apple OS X operating system as a separate stand alone computer.





Virtualization

Why Virtualization

- **With Virtualization, one can run software written for one operating system on another operating system (for example, running Windows on a Mac) without having to reboot the computer.**
- **Since you can configure the hardware, you can even install an old operating systems such as DOS or OS/2 even if your real computer's hardware is no longer supported by that operating system.**
- **Testing and disaster recovery. Once installed, a virtual machine and its virtual hard disks can be considered a “container” that can be arbitrarily frozen, woken up, copied, backed up, and transported between hosts.**



Virtualization

Why Virtualization

- **With the use of another feature called “snapshots”, one can save a particular state of a virtual machine and revert back to that state, if necessary. In this way, one can freely experiment with a computing environment. If something goes wrong (e.g. after installing misbehaving software or infecting the guest with a virus), one can easily switch back to a previous snapshot and avoid the need of frequent backups and restorations.**
- **For the forensic investigator, it’s a way to test in a guest environment without effecting the host environment. It’s possible to test for virus software or malware without infecting your examination computer.**
- **For the detective, it’s a way to conduct UC investigations without infecting or damaging your investigative computer.**



Virtualization

Terminology

Virtual Machine – the virtual machine is the special environment that your virtual software creates for your guest operating system. In other words, you run your guest operating system “within” a virtual machine. Normally a virtual machine will be shown as a window on your desktop with a separate computer running within the window.

Hosting Operating System – the operating system of the physical computer on which VirtualBox was installed. There are versions of VirtualBox that will run on Windows, Mac OS X and Solaris.

Guest Operating System – the operating system running inside the virtual environment. Theoretically, VirtualBox can run any x86 operating system (DOS, Windows, OS/2, FreeBSD, OpenBSD).



Virtualization

Terminology

Guest Additions – shared folders, seamless windows, 3D virtualization. The VirtualBox Guest Additions are software packages which can be installed inside a supported guest operating system to improve their performance and to provide additional integration and communication with the host system. After installation, the Guest Additions will support automatic adjustments of video resolutions, seamless windows, accelerated 3D graphics and more.



Virtualization

Questions