dig4n6

This blog is dedicated to computer forensic research and topics that I come across that I feel are both beneficial to the forensic community and interesting/useful information to read. This is my own personal opinion and work and does not reflect any entity except for myself unless expressed otherwise.

THURSDAY, JULY 25, 2013

VDI-in-a-Box Analysis Results

Despite the fact that my capstone thesis was complete over three months ago, it's been a struggle to make this post. That being said, hopefully this blog post doesn't appear too much like a paper, but it was pretty hard to avoid doing. The full paper, as of right now, is not publically available, but hopefully will be some time in the near future. Please reach out with any questions relating to the research, the subject, my process, or anything.

Although it was previously highlighted in my prior blog posts, I feel that it is necessary to outline the importance of this research again with a little more detail.

Note: Clicking the pictures will enlarge them. I formatted most easy enough to read, but some need enlarging.

Why is this important to us?

> Technology is an ever-evolving creature. In the world of digital forensics, attempting to keep up to speed with the constant changes is an absolute must. Doing so will make not only for a better investigator, but a greater impact on the work that needs to be done. With the recent boom in the terms "cloud computing" and "virtualization," digital forensic examiners find themselves needing to immerse into a new era of the investigation age. According to the State of SMB IT Report, written by Spiceworks, the trends in the adoption of virtualization and cloud computing have been on a constant rise. Moving back to the first half of 2010, 44% of small to midsized businesses (SMB's) were using virtualized products. Progressing forward, it is estimated that nearly 79% of SMB's will be using virtualized platforms, (Sweeney).

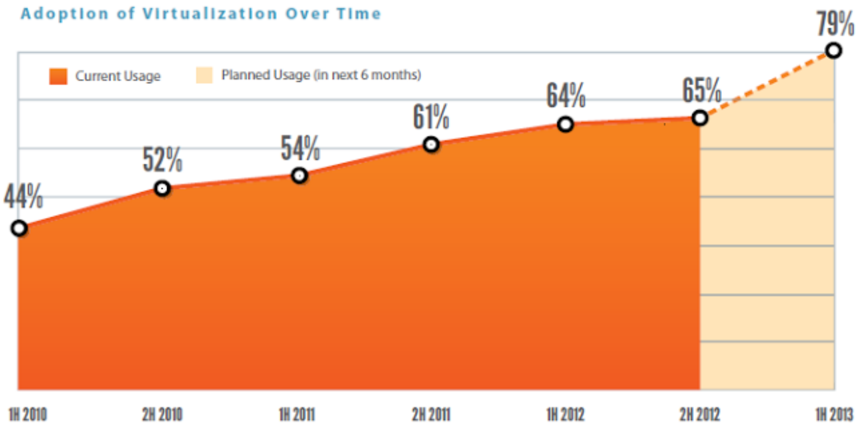
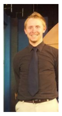


Figure 1: State of SMB IT Report, November 2012, Spiceworks (Source: Sweeney)

> With such a dramatic increase in the implementation of virtualized software, it is extremely pertinent that digital forensic investigators begin to understand the logic of the systems and what evidence can be found on them.
>
> Two of the most common companies that investigators will see in practice are VMware and its patented VMware Workstation, as well as Citrix and its XenDesktop and VDI-in-a-Box platforms. The low long-term cost of these products allow for small and large companies alike to implement and maintain these technologies. According to Phil Hochmuth of Forbes, "Providers of VDI technology say their systems can save between 30% and 50% of the current cost for IT administrators to manage, patch, upgrade and support employees' PCs in a client/server environment. By some estimates, this could cut the annual per-desktop support cost from around $530 to $376--a savings which can add up for the larger the organization," (Hochmuth). With an increased return on investment, companies that deploy VDI's will quickly advertise and transition partner companies to similar technologies.

ABOUT ME



Ethan Fleisher

2013 Champlain College graduate in Computer and Digital Forensics. Dedicated to learning about incident response and digital risk management and investigation.

View my complete profile

BLOG ARCHIVE

- ▼ 2013 (5)
  - ▼ July (1)
    - VDI-in-a-Box Analysis Results
  - ► March (1)
  - ► February (1)
  - ► January (2)
- ► 2012 (10)

BLOGS I FOLLOW

Windows Incident Response
New Stuff
2 hours ago

Forensics from the sausage factory
Mac OS X "Set date and time automatically"
3 weeks ago

A Fistful of Dongles
The State Of The Blog
4 weeks ago

Blogging Windows
Thoughts on Day 1 of Build 2014
4 weeks ago

JonRajewski.com
Have you seen IDrive in your computer forensic cases? This blog post discusses artifacts
1 month ago

The Digital Standard
2014 SANS DFIR Summit
1 month ago

Digital Forensics Stream
Office 2013: More MRUs
2 months ago

Random Thoughts of Forensics
Windows 8 Thesis DRAFT
10 months ago

Samsung Galaxy Camera Forensics
See ya later, Sammy Sung!
1 year ago

Unfortunately with all good comes some bad and implementation of cloud computing is no different. As virtualization becomes more prevalent in business practice, malicious code and malware will quickly take a turn towards attacking cloud computing. “Attackers will go where users go, so it should come as no surprise that mobile platforms and cloud services will be high-risk targets for attacks and breaches in 2013. The rapid rise in malware on Android in 2012 confirms this,” (Powledge). As attackers move towards cloud services and online platforms, it becomes more necessary to not only secure them better, but to be able to analyze and examine what happened after an attack and where vulnerabilities lie. According to Symantec, “the median cost of downtime for an SMB is $12,500 per day,” (Powledge). If a small sized business can lose this much money while being down for such a short period of time, imagine the ramifications if a large company like Amazon was hit for even two hours. It simply cannot be overstated enough; digital forensic examiners must be prepared for this to happen as it is inevitable.

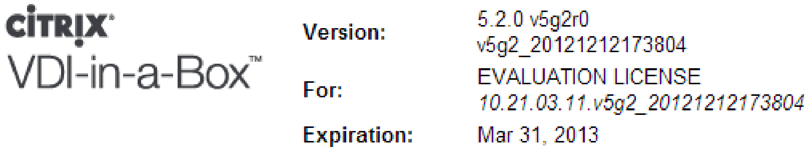
So, what are virtual desktop environments?

A Virtual Desktop Infrastructure is simply cloud computing. Virtualization changes the information technology work place. Desktops and workstations can be set up, configured, and dispersed in merely minutes instead of hours or days. Costs are reduced after initial investment while security and machine integrity are increased. The user experience becomes easier than before, allowing for employees to remotely connect and work from anywhere. Centralized storage provides administrators and incident responders with a plethora of information at their fingertips in the event of an emergency or breach.

An extremely popular company in the VDI business is Citrix. Through their products of XenDesktop, XenApp, and VDI-in-a-Box, Citrix has emerged as a forerunner, and major companies all over are to use their products. According to Eric Savitz of Forbes in his article entitled Citrix Shares Rally As Q4 Results Crush Street Estimates, “the enterprise software company posted revenue of $740 million, up 19% from a year ago, and ahead of the Street consensus at $705.7 million,” (Savitz). It’s rather clear by these numbers that the investment into cloud computing is booming and that all sizes of companies are transitioning. Citrix is among the top in VDI providers, and as such, is the focal point of this research.

Now we understand why this is important and what they are, so what am I doing?

VDI-in-a-Box is a unique toolset that provides a network administrator with all of the tools necessary to deploy a VDI to a business. Through the use of only a few physical machines, VDI-in-a-Box can be successfully setup and running in a very short time. Considering small to midsized businesses are the target audience for this product and that so many are making the transition already, VDI-in-a-Box version 5.2.0 is the software that is being analyzed.



CiTRiX VDI-in-a-Box™

Version: 5.2.0 v5g2r0
v5g2_20121212173804

For: EVALUATION LICENSE
10.21.03.11.v5g2_20121212173804

Expiration: Mar 31, 2013

Figure 2: Citrix VDI-in-a-Box Version 5.2

How did I go about doing this then?

Acquisition of a Citrix Virtual Desktop Infrastructure required a great deal of trial and error. Due to being unable to use some of the enterprise level tools because of licensing limitations, or the software not supporting remote imaging of a server, Windows Secure Copy (WinSCP) over port 22 was used to capture a live image.

The XenServer itself, being the physical hypervisor, was the primary target to acquire in hopes of finding all the virtual machines stored on it.

Android GPS forensics
Mock Locations
1 year ago

An Eye on Forensics
A Cold Day in E-Commerce - Guest Post
1 year ago

Computer Forensics for everyone
Using FTK Imager Lite Command Line
1 year ago

Snapchat Forensics
iPhone 4S Analysis with UFED Cellebrite and XRY
1 year ago

Trevin Mowery's Blog
Siri Forensics: Part 2
1 year ago

Girl, Unallocated
Be Very Quiet... I'm Tracking Emails Through Headers
1 year ago

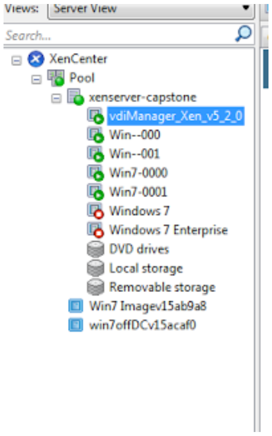
SecuriTree
HTCIA Conference Recap
1 year ago

Digital Forensics is a Science
Mobile Device Forensics - Course Update
1 year ago

Propeller Head Forensics
How cool is this?
1 year ago

LCDI Blog

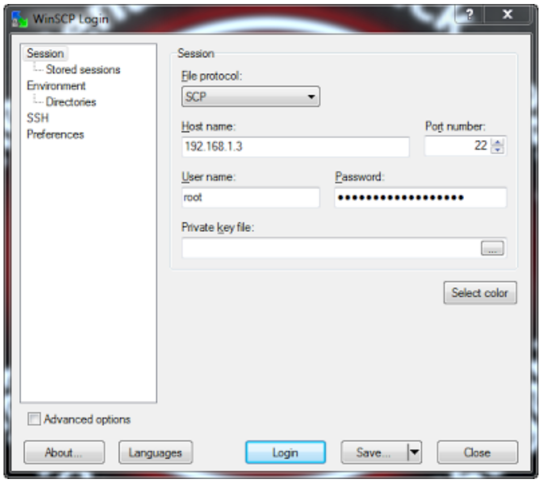
www.writeblocked.org



XenCenter
Pool
xenserver-capstone
vdiManager_Xen_v5_2_0
Win--000
Win--001
Win7-0000
Win7-0001
Windows 7
Windows 7 Enterprise
DVD drives
Local storage
Removable storage
Win7 Imagev15ab9a8
win7offDCv15acaf0

Figure 3: XenCenter VM Pool

WinSCP is a program that gives a user a graphical user interface to the secure copy protocol and will allow a choice of what information to copy. By entering a server address and administrative credentials, WinSCP will create a secure connection to a remote location allowing information to be viewed or duplicated.



File protocol: SCP

Host name: 192.168.1.3

Port number: 22

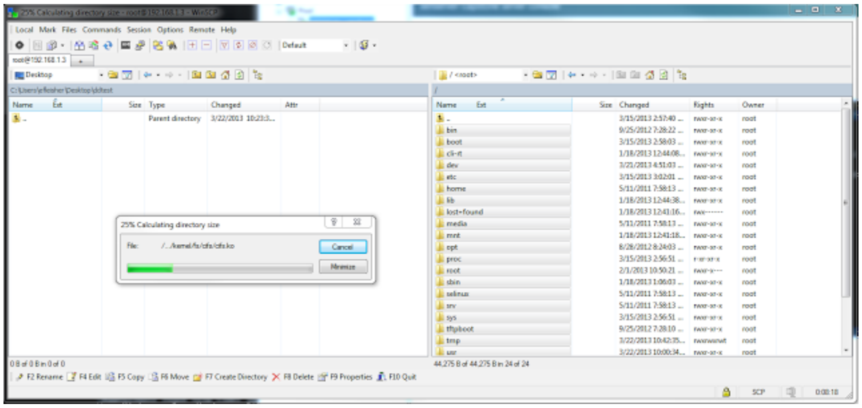
User name: root

Password: ••••••••••••••••••

Private key file:

Figure 4: WinSCP Login Prompt

Once logged into the server, WinSCP will provide the user with a side-by-side view of both the remote machine and the local machine. At this point, the entirety of the server folder structure was copied over from the server in an attempt to create the closest to a logical image as possible.



C:\Users\jefleisher\Desktop\ddtest

Name	Ext	Size	Type	Changed	Attr
..			Parent directory	3/22/2013 10:23:3...	

0 B of 0 B in 0 of 0

25% Calculating directory size

File: /.../kernel/fs/cifs/cifs.ko

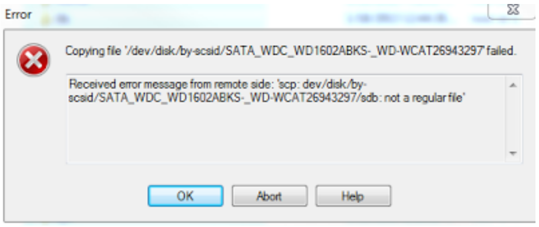
/

Name	Ext	Size	Changed	Rights	Owner
..			3/15/2013 2:57:40 ...	rwxr-xr-x	root
bin			9/25/2012 7:28:22 ...	rwxr-xr-x	root
boot			3/15/2013 2:58:03 ...	rwxr-xr-x	root
cli-rt			1/18/2013 12:44:08...	rwxr-xr-x	root
dev			3/21/2013 4:51:03 ...	rwxr-xr-x	root
etc			3/15/2013 3:02:01 ...	rwxr-xr-x	root
home			5/11/2011 7:58:13 ...	rwxr-xr-x	root
lib			1/18/2013 12:44:38...	rwxr-xr-x	root
lost+found			1/18/2013 12:41:16...	rwx------	root
media			5/11/2011 7:58:13 ...	rwxr-xr-x	root
mnt			1/18/2013 12:41:18...	rwxr-xr-x	root
opt			8/28/2012 8:24:03 ...	rwxr-xr-x	root
proc			3/15/2013 2:56:51 ...	r-xr-xr-x	root
root			2/1/2013 10:50:21 ...	rwxr-x---	root
sbin			1/18/2013 1:06:03 ...	rwxr-xr-x	root
selinux			5/11/2011 7:58:13 ...	rwxr-xr-x	root
srv			5/11/2011 7:58:13 ...	rwxr-xr-x	root
sys			3/15/2013 2:56:51 ...	rwxr-xr-x	root
tftpboot			9/25/2012 7:28:10 ...	rwxr-xr-x	root
tmp			3/22/2013 10:42:35...	rwxrwxrwt	root
usr			3/22/2013 10:00:34...	rwxr-xr-x	root

44,275 B of 44,275 B in 24 of 24

Figure 5: WinSCP File Transfer Session

It is important to note that multiple errors occurred while copying files and folders from the server to the examination machine. These errors would cause the file being copied to fail and not copy successfully. The errors would typically read either “Can’t create file…” or “…not a regular file.”

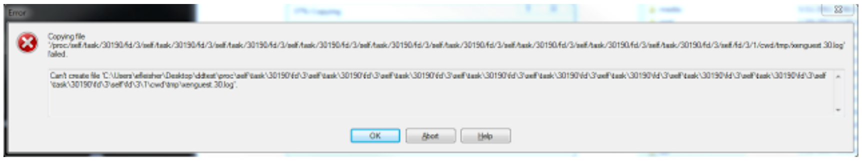


Error

Copying file '/dev/disk/by-scsid/SATA_WDC_WD1602ABKS-_WD-WCAT26943297' failed.

Received error message from remote side: 'scp: dev/disk/by-scsid/SATA_WDC_WD1602ABKS-_WD-WCAT26943297/sdb: not a regular file'

Figure 6: "Not a regular file" error message



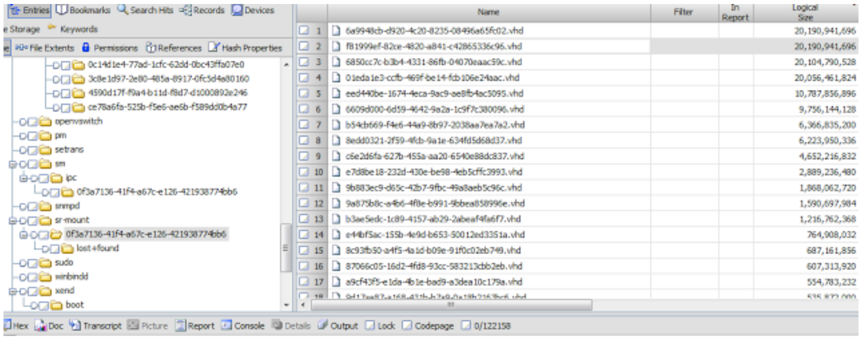
Error

Copying file '/proc/self/task/30190/fd/3/self/task/30190/fd/3/self/task/30190/fd/3/self/task/30190/fd/3/self/task/30190/fd/3/self/task/30190/fd/3/self/task/30190/fd/3/self/task/30190/fd/3/self/task/30190/fd/3/self/fd/3/1/cwd/tmp/xenguest.30.log' failed.

Can't create file 'C:\Users\afleisher\Desktop\ddtest\proc\self\task\30190\fd\3\self\task\30190\fd\3\self\task\30190\fd\3\self\task\30190\fd\3\self\task\30190\fd\3\self\task\30190\fd\3\self\task\30190\fd\3\self\task\30190\fd\3\self\task\30190\fd\3\self\fd\3\1\cwd\tmp\xenguest.30.log'.

Figure 7: "Can't create file" error message

Although there were errors on the transfer, it did complete successfully and allowed for examination of the drive. The most important item for review were the virtual hard disks (VHD's) that contained information relevant to the golden images as well as virtual machines that had been created.



```
    ├─ 0c14d1e4-77ad-1cfc-62dd-0bc43ffa07e0
    ├─ 3c8e1d97-2e80-485a-8917-0fc5d4a80160
    ├─ 4590d17f-f9a4-b11d-f8d7-d1000892e246
    └─ ce78a6fa-525b-f5e6-ae6b-f589dd0b4a77
├─ openvswitch
├─ pm
├─ setrans
├─ sm
│  ├─ ipc
│     └─ 0f3a7136-41f4-a67c-e126-421938774bb6
├─ snmpd
├─ sr-mount
│  ├─ 0f3a7136-41f4-a67c-e126-421938774bb6
│     └─ lost+found
├─ sudo
├─ winbindd
├─ xend
   └─ boot
```

	Name	Filter	In Report	Logical Size
1	6a9948cb-d920-4c20-8235-08496a65fc02.vhd			20,190,941,696
2	f81999ef-82ce-4820-a841-c42865336c96.vhd			20,190,941,696
3	6850cc7c-b3b4-4331-86fb-04070eaac59c.vhd			20,104,790,528
4	01eda1e3-ccfb-469f-be14-fcb106e24aac.vhd			20,056,461,824
5	eed440be-1674-4eca-9ac9-ae8fb4ac5095.vhd			10,787,856,896
6	6609d000-6d59-4642-9a2a-1c9f7c380096.vhd			9,756,144,128
7	b54cb669-f4e6-44a9-8b97-2038aa7ea7a2.vhd			6,366,835,200
8	8edd0321-2f59-4fcb-9a1e-634fd5d68d37.vhd			6,223,950,336
9	c6e2d6fa-627b-455a-aa20-6540e88dc837.vhd			4,652,216,832
10	e7d8be18-232d-430e-be98-4eb5cffc3993.vhd			2,889,236,480
11	9b883ec9-d65c-42b7-9fbc-49a8aeb5c96c.vhd			1,868,062,720
12	9a875b8c-a4b6-4f8e-b991-9bbea858996e.vhd			1,590,697,984
13	b3ae5edc-1c89-4157-ab29-2abeaf4fa6f7.vhd			1,216,762,368
14	e44bf5ac-155b-4e9d-b653-50012ed3351a.vhd			764,908,032
15	8c93fb50-a4f5-4a1d-b09e-91f0c02eb749.vhd			687,161,856
16	87066c05-16d2-4fd8-93cc-583213cbb2eb.vhd			607,313,920
17	a9cf43f5-e1da-4b1e-bad9-a3dea10c179a.vhd			554,783,232
18	9d17ae87-a168-431b-b7a9-0a18b2163bc6.vhd			535,872,000

Figure 8: Virtual Hard Disk Storage Location

These virtual hard disks are stored in a location determined during the initial setup, and in this project they were located at /var/run/sr-mount. Each VHD is listed by a universally unique identifier (UUID). These UUID's can be related back to specific machines in different ways. If access to the Citrix vdiManager is available, each virtual machines general properties will list its UUID. This will be extremely helpful when working with personal desktops as the VHD's will not be deleted, therefore finding the UUID through vdiManager would be a simple task. When working with pooled desktops, however, the VHD files are destroyed after the machine is shut down.

Pooled virtual hard disks being destroyed was an obstacle that was easily overcome by the use of snapshots, thus the virtual hard disks are now not destroyed. Much like VMware, Citrix allows for the use of snapshots.

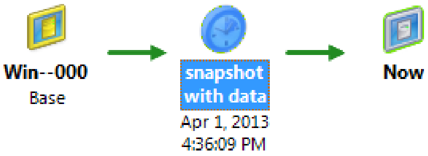
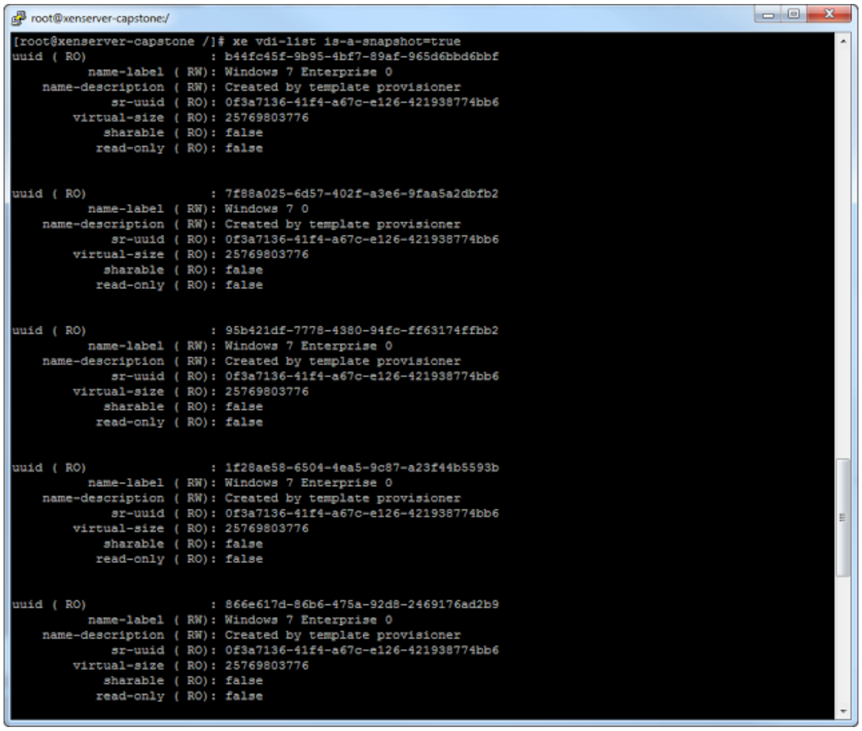


Figure 9: XenCenter Snapshot View

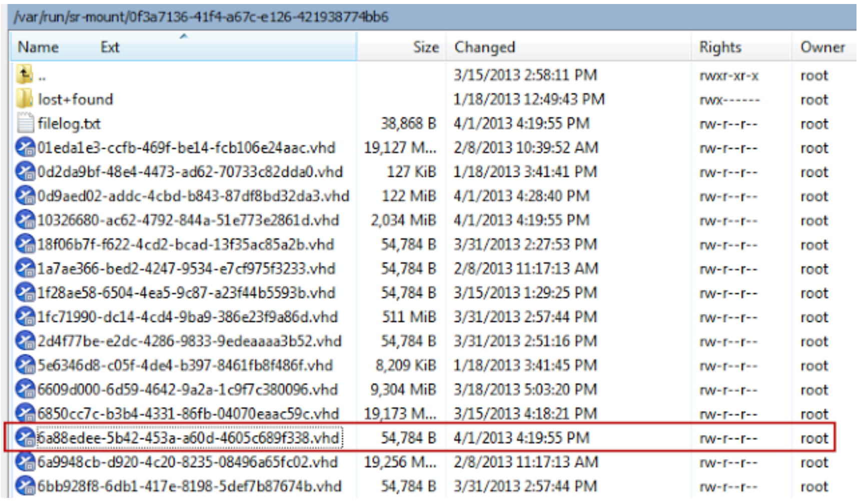
Each of these snapshots will create two VHDs. The user can determine which VHD's are snapshots by a command via the XenServer command line. From the root directory of the drive, the command xe vdi-list is-a-snapshot=true will prompt a list of all virtual hard disks that are snapshots.



```
[root@xenserver-capstone /]# xe vdi-list is-a-snapshot=true
uuid ( RO)                : b44fc45f-9b95-4bf7-89af-965d6bbd6bbf
          name-label ( RW): Windows 7 Enterprise 0
    name-description ( RW): Created by template provisioner
             sr-uuid ( RO): 0f3a7136-41f4-a67c-e126-421938774bb6
        virtual-size ( RO): 25769803776
            sharable ( RO): false
           read-only ( RO): false


uuid ( RO)                : 7f88a025-6d57-402f-a3e6-9faa5a2dbfb2
          name-label ( RW): Windows 7 0
    name-description ( RW): Created by template provisioner
             sr-uuid ( RO): 0f3a7136-41f4-a67c-e126-421938774bb6
        virtual-size ( RO): 25769803776
            sharable ( RO): false
           read-only ( RO): false


uuid ( RO)                : 95b421df-7778-4380-94fc-ff63174ffbb2
          name-label ( RW): Windows 7 Enterprise 0
    name-description ( RW): Created by template provisioner
             sr-uuid ( RO): 0f3a7136-41f4-a67c-e126-421938774bb6
        virtual-size ( RO): 25769803776
            sharable ( RO): false
           read-only ( RO): false


uuid ( RO)                : 1f28ae58-6504-4ea5-9c87-a23f44b5593b
          name-label ( RW): Windows 7 Enterprise 0
    name-description ( RW): Created by template provisioner
             sr-uuid ( RO): 0f3a7136-41f4-a67c-e126-421938774bb6
        virtual-size ( RO): 25769803776
            sharable ( RO): false
           read-only ( RO): false


uuid ( RO)                : 866e617d-86b6-475a-92d8-2469176ad2b9
          name-label ( RW): Windows 7 Enterprise 0
    name-description ( RW): Created by template provisioner
             sr-uuid ( RO): 0f3a7136-41f4-a67c-e126-421938774bb6
        virtual-size ( RO): 25769803776
            sharable ( RO): false
           read-only ( RO): false
```

Figure 10: XenServer Snapshot List by Command Line Instruction

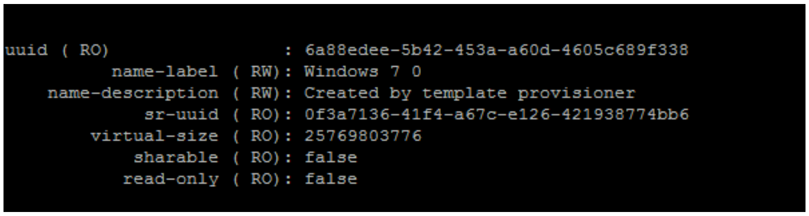
The list of snapshots that is returned will provide the UUID of each snapshot, a label of the golden image that it was generated from, the storage repository UUID that is holding the snapshot, and the virtual size of the snapshot. To verify that this command was accurately creating a list all snapshots, a new snapshot was taken and the command again was run again. This appended a new entry to the end of the list, and also created two new VHD's on the server.



/var/run/sr-mount/0f3a7136-41f4-a67c-e126-421938774bb6

Name Ext	Size	Changed	Rights	Owner
..		3/15/2013 2:58:11 PM	rwxr-xr-x	root
lost+found		1/18/2013 12:49:43 PM	rwx------	root
filelog.txt	38,868 B	4/1/2013 4:19:55 PM	rw-r--r--	root
01eda1e3-ccfb-469f-be14-fcb106e24aac.vhd	19,127 M...	2/8/2013 10:39:52 AM	rw-r--r--	root
0d2da9bf-48e4-4473-ad62-70733c82dda0.vhd	127 KiB	1/18/2013 3:41:41 PM	rw-r--r--	root
0d9aed02-addc-4cbd-b843-87df8bd32da3.vhd	122 MiB	4/1/2013 4:28:40 PM	rw-r--r--	root
10326680-ac62-4792-844a-51e773e2861d.vhd	2,034 MiB	4/1/2013 4:19:55 PM	rw-r--r--	root
18f06b7f-f622-4cd2-bcad-13f35ac85a2b.vhd	54,784 B	3/31/2013 2:27:53 PM	rw-r--r--	root
1a7ae366-bed2-4247-9534-e7cf975f3233.vhd	54,784 B	2/8/2013 11:17:13 AM	rw-r--r--	root
1f28ae58-6504-4ea5-9c87-a23f44b5593b.vhd	54,784 B	3/15/2013 1:29:25 PM	rw-r--r--	root
1fc71990-dc14-4cd4-9ba9-386e23f9a86d.vhd	511 MiB	3/31/2013 2:57:44 PM	rw-r--r--	root
2d4f77be-e2dc-4286-9833-9edeaaaa3b52.vhd	54,784 B	3/31/2013 2:51:16 PM	rw-r--r--	root
5e6346d8-c05f-4de4-b397-8461fb8f486f.vhd	8,209 KiB	1/18/2013 3:41:45 PM	rw-r--r--	root
6609d000-6d59-4642-9a2a-1c9f7c380096.vhd	9,304 MiB	3/18/2013 5:03:20 PM	rw-r--r--	root
6850cc7c-b3b4-4331-86fb-04070eaac59c.vhd	19,173 M...	3/15/2013 4:18:21 PM	rw-r--r--	root
6a88edee-5b42-453a-a60d-4605c689f338.vhd	54,784 B	4/1/2013 4:19:55 PM	rw-r--r--	root
6a9948cb-d920-4c20-8235-08496a65fc02.vhd	19,256 M...	2/8/2013 11:17:13 AM	rw-r--r--	root
6bb928f8-6db1-417e-8198-5def7b87674b.vhd	54,784 B	3/31/2013 2:57:44 PM	rw-r--r--	root

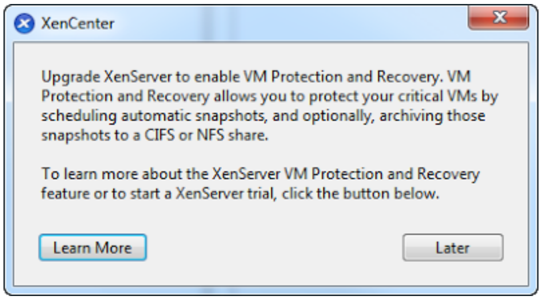
Figure 11: New Virtual Hard Disk Creation



```
uuid ( RO)                : 6a88edee-5b42-453a-a60d-4605c689f338
          name-label ( RW): Windows 7 0
    name-description ( RW): Created by template provisioner
             sr-uuid ( RO): 0f3a7136-41f4-a67c-e126-421938774bb6
        virtual-size ( RO): 25769803776
            sharable ( RO): false
           read-only ( RO): false
```

Figure 12: New Snapshot Verification

When using Citrix VM Protection and Recovery, two types of snapshots can be taken with three different scheduling options. Disk-only snapshots can be taken that will "store the VM's disks (storage) and metadata. They are crash-consistent and can be performed on all VM types, including Linux VMs," (Citrix EDocs). Disk and memory snapshots are also available which will "save the VM's disks (storage), metadata, and its current memory state (RAM)," (Citrix EDocs). Once the decision is made to either perform disk-only or disk and memory snapshots, the administrator must choose whether to do hourly, daily, or weekly snapshots. In any event, the snapshot retention policy is limited to a maximum of 10 scheduled snapshots or until archived, automatically deleting the oldest one when this number is exceeded.



Upgrade XenServer to enable VM Protection and Recovery. VM Protection and Recovery allows you to protect your critical VMs by scheduling automatic snapshots, and optionally, archiving those snapshots to a CIFS or NFS share.

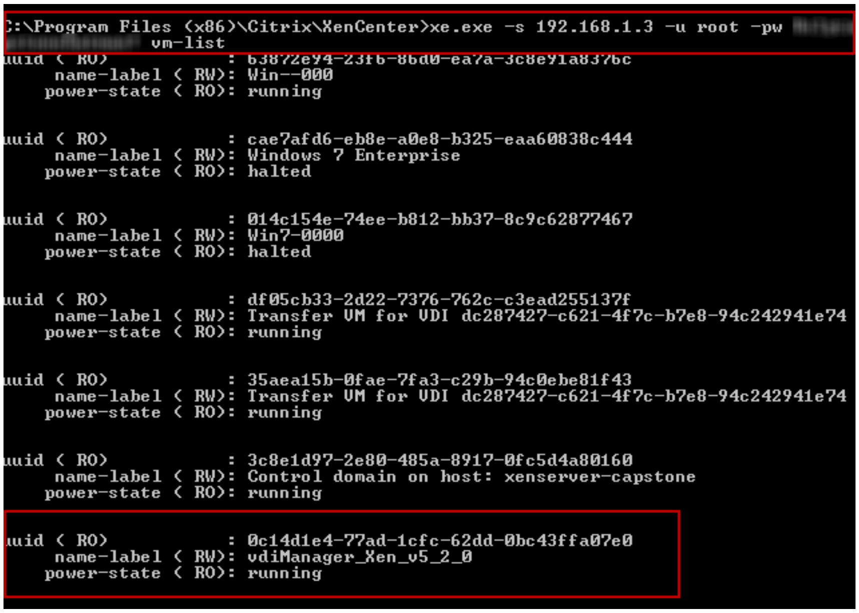
To learn more about the XenServer VM Protection and Recovery feature or to start a XenServer trial, click the button below.

Figure 13: Citrix VM Protection and Recovery

A daily or weekly archive schedule can then be configured, independent from the scheduled snapshots, which will archive all scheduled snapshots to a remote location for storage. Alternatively, all snapshots can be automatically archived if the administrator wishes. When examining the archived virtual hard disks, each archive folder is given a specific name. This naming convention will always be the VM name followed by the first sixteen characters of the UUID. For example, if the VM name is Win7 and the UUID is 6a88edee-5b42-453a-a60d-4605c689f338, the archive folder will be Win7_6a88edee-5b42-45. “This folder contains archived VM files, in the YYYYMMDD-HHMM.xva form,” (Citrix RSS).

Depending on how this is done, the investigator will need to link a user to a specific snapshot to alleviate the need to sift through what could be hundreds of snapshots. One method would be to examine each virtual hard disk file individually. Although this will take quite some time, it will still provide accurate results. One benefit to this method is that no information will be overlooked in the event that the suspect was using another user account or username.

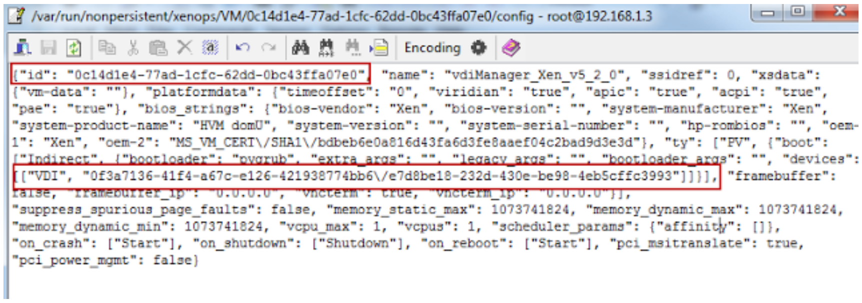
On the domain controller with XenCenter installed, running the command “xe vm-list –s <server> -u <user> -pw <password>” provides a list of all virtual machines currently being run. The virtual machine vdiManager_Xen is the interface that the administrator interacts with to initially configure the server, the machine that keeps activity logs, and the web portal that users must access in order to spawn a virtual desktop.



```
:\Program Files (x86)\Citrix\XenCenter>xe.exe -s 192.168.1.3 -u root -pw [redacted]
 vm-list
uuid ( RO)           : 63872e94-23f6-86d0-ea7a-3c8e91a8376c
     name-label ( RW): Win--000
    power-state ( RO): running


uuid ( RO)           : cae7afd6-eb8e-a0e8-b325-eaa60838c444
     name-label ( RW): Windows 7 Enterprise
    power-state ( RO): halted


uuid ( RO)           : 014c154e-74ee-b812-bb37-8c9c62877467
     name-label ( RW): Win7-0000
    power-state ( RO): halted


uuid ( RO)           : df05cb33-2d22-7376-762c-c3ead255137f
     name-label ( RW): Transfer VM for VDI dc287427-c621-4f7c-b7e8-94c242941e74
    power-state ( RO): running


uuid ( RO)           : 35aea15b-0fae-7fa3-c29b-94c0ebe81f43
     name-label ( RW): Transfer VM for VDI dc287427-c621-4f7c-b7e8-94c242941e74
    power-state ( RO): running


uuid ( RO)           : 3c8e1d97-2e80-485a-8917-0fc5d4a80160
     name-label ( RW): Control domain on host: xenserver-capstone
    power-state ( RO): running


uuid ( RO)           : 0c14d1e4-77ad-1cfc-62dd-0bc43ffa07e0
     name-label ( RW): vdiManager_Xen_v5_2_0
    power-state ( RO): running
```

Figure 14: XenCenter Command Line VM List

Still being SSH connected into the XenServer, under the directory /var/run/nonpersistent/xenops/VM, the investigator can locate and view the configuration files for the vdiManager. This will point to the virtual hard disk that retains these records.

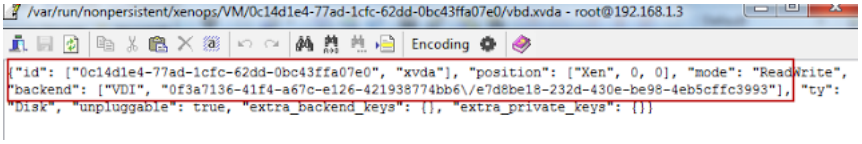


/var/run/nonpersistent/xenops/VM/0c14d1e4-77ad-1cfc-62dd-0bc43ffa07e0/config - root@192.168.1.3

```
{"id": "0c14d1e4-77ad-1cfc-62dd-0bc43ffa07e0", "name": "vdiManager_Xen_v5_2_0", "ssidref": 0, "xsdata":
{"vm-data": ""}, "platformdata": {"timeoffset": "0", "viridian": "true", "apic": "true", "acpi": "true",
"pae": "true"}, "bios_strings": {"bios-vendor": "Xen", "bios-version": "", "system-manufacturer": "Xen",
"system-product-name": "HVM domU", "system-version": "", "system-serial-number": "", "hp-rombios": "", "oem-
1": "Xen", "oem-2": "MS_VM_CERT\/SHA1\/bdbeb6e0a816d43fa6d3fe8aaef04c2bad9d3e3d"}, "ty": ["PV", {"boot":
["Indirect", {"bootloader": "pygrub", "extra_args": "", "legacy_args": "", "bootloader_args": "", "devices":
[["VDI", "0f3a7136-41f4-a67c-e126-421938774bb6\/e7d8be18-232d-430e-be98-4eb5cffc3993"]]}], "framebuffer":
false, "framebuffer_ip": "0.0.0.0", "vncterm": true, "vncterm_ip": "0.0.0.0"}],
"suppress_spurious_page_faults": false, "memory_static_max": 1073741824, "memory_dynamic_max": 1073741824,
"memory_dynamic_min": 1073741824, "vcpu_max": 1, "vcpus": 1, "scheduler_params": {"affinity": []},
"on_crash": ["Start"], "on_shutdown": ["Shutdown"], "on_reboot": ["Start"], "pci_msitranslate": true,
"pci_power_mgmt": false}
```

Figure 15: vdiManager Configuration File

This configuration file will first list the same UUID found when the XenCenter command was used. In the middle of the log is the VDI UUID, with the storage repository UUID being listed, followed by \/, and then the vdiManager's UUID. Within the /var/run/nonpersistent/xenops/VM directory are two files, vdb.xvda and vdb.xvdb. The first of these (.xvda) will correspond this information again, linking the two UUID's.



/var/run/nonpersistent/xenops/VM/0c14d1e4-77ad-1cfc-62dd-0bc43ffa07e0/vbd.xvda - root@192.168.1.3

```
{"id": ["0c14d1e4-77ad-1cfc-62dd-0bc43ffa07e0", "xvda"], "position": ["Xen", 0, 0], "mode": "ReadWrite",
"backend": ["VDI", "0f3a7136-41f4-a67c-e126-421938774bb6\/e7d8be18-232d-430e-be98-4eb5cffc3993"], "ty":
"Disk", "unpluggable": true, "extra_backend_keys": {}, "extra_private_keys": {}}
```

Figure 16: vdiManager Virtual Hard Disk Verification

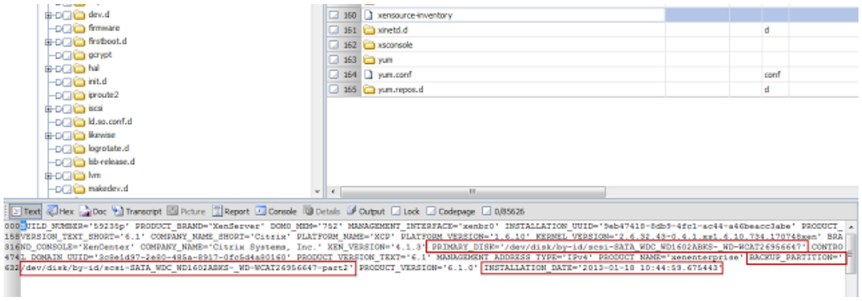
Once this is achieved, examination of the virtual hard disks can begin. The investigator should now be able to extract and examine the vdiManager machine as well as all of the snapshots that were taken. Unfortunately, when examining a VHD in EnCase, it is not recognized as a normal operating drive and therefore does not have any form of folder structure. Rather, it is all listed as unallocated and must be manually parsed.

What can I find from this?

There is a great deal of information that is recoverable from the XenServer. Some of these files are relevant to the server itself and will depict information about the XenServer, while others reflect the vdiManager. A plethora of virtual machine information is also recoverable **as long as a snapshot is present**.

XenServer Files

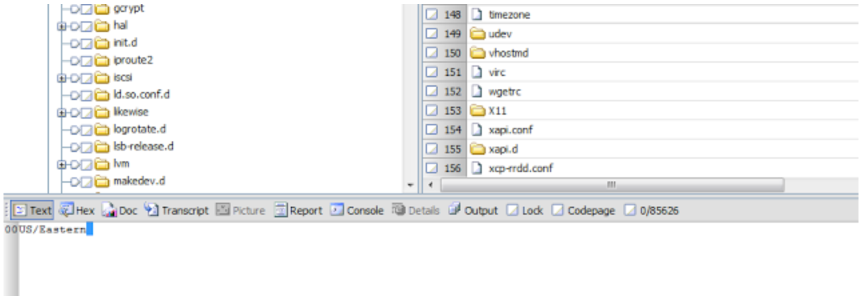
The first file of interest from the XenServer is xensource-inventory, located in /etc. This file contains information related to the actual server itself and would be useful in an investigation. The installation date of the server is recoverable, but more importantly, the primary disk and backup partition locations are located within this file as well.



```
000BUILD_NUMBER='59235p' PRODUCT_BRAND='XenServer' DOM0_MEM='752' MANAGEMENT_INTERFACE='xenbr0' INSTALLATION_UUID='5eb47418-8db5-4fc1-ac44-a46beacc3abe' PRODUCT_
158VERSION_TEXT_SHORT='6.1' COMPANY_NAME_SHORT='Citrix' PLATFORM_NAME='XCP' PLATFORM_VERSION='1.6.10' KERNEL_VERSION='2.6.32.43-0.4.1.xs1.6.10.734.170748xen' BRA
316ND_CONSOLE='XenCenter' COMPANY_NAME='Citrix Systems, Inc.' XEN_VERSION='4.1.3' PRIMARY_DISK='/dev/disk/by-id/scsi-SATA_WDC_WD1602ABKS-_WD-WCAT26956647' CONTRO
474L_DOMAIN_UUID='3c8e1d97-2e80-485a-8917-0fc5d4a80160' PRODUCT_VERSION_TEXT='6.1' MANAGEMENT_ADDRESS_TYPE='IPv4' PRODUCT_NAME='xenenterprise' BACKUP_PARTITION='
632/dev/disk/by-id/scsi-SATA_WDC_WD1602ABKS-_WD-WCAT26956647-part2' PRODUCT_VERSION='6.1.0' INSTALLATION_DATE='2013-01-18 10:44:59.675443'
```

Figure 17: XenServer Disk and Installation Details

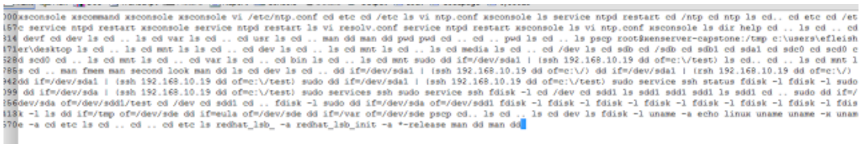
The next file of interest is located again in /etc and is the timezone file. Considering time zones are extremely important to any forensic investigation, examining this artifact will be very helpful as it lists in plaintext the time zone that the server is set for.



```
00US/Eastern
```

Figure 18: XenServer Timezone Details

The last file pertaining to information from the server is the bash history. Bash is a unix command-line interpreter, or shell, that will allow for a user to input commands and information into a system. It is comparable to the Windows command line. The bash history can be located at /root and is named .bash_history.

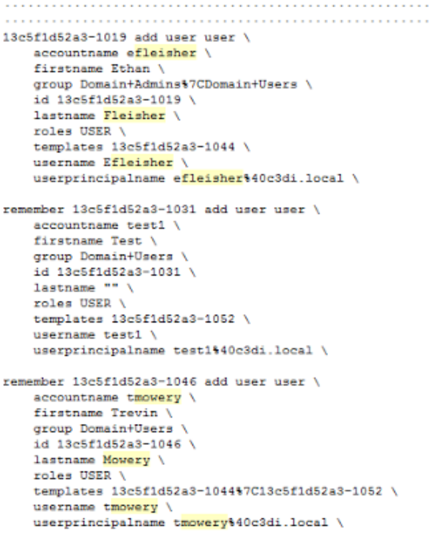


```
000xsconsole xscommand xsconsole xsconsole vi /etc/ntp.conf cd etc cd /etc ls vi ntp.conf xsconsole ls service ntpd restart cd /ntp cd ntp ls cd.. cd etc cd /et
157c service ntpd restart xsconsole service ntpd restart ls vi resolv.conf service ntpd restart xsconsole ls vi ntp.conf xsconsole ls dir help cd .. ls cd .. cd
314 devf cd dev ls cd .. ls cd var ls cd .. cd usr ls cd .. man dd man dd pwd pwd cd .. cd .. pwd ls cd .. ls pscp root@xenserver-capstone:/tmp c:\users\efleish
471er\desktop ls cd .. ls cd mnt ls ls cd .. cd dev ls cd .. ls cd mnt ls cd .. ls cd media ls cd .. cd /dev ls cd sdb cd /sdb cd sdb1 cd sda1 cd sdc0 cd scd0 c
628d scd0 cd .. ls cd mnt ls cd .. cd var ls cd .. cd bin ls cd .. ls cd mnt sudo dd if=/dev/sda1 | (ssh 192.168.10.19 dd of=c:\/test) ls cd.. cd .. ls cd mnt l
785s cd .. man fmem man second look man dd ls cd dev ls cd .. dd if=/dev/sda1 | (ssh 192.168.10.19 dd of=c:\/) dd if=/dev/sda1 | (rsh 192.168.10.19 dd of=c:\/)
942dd if=/dev/sda1 | (ssh 192.168.10.19 dd of=c:\/test) sudo dd if=/dev/sda1 | (ssh 192.168.10.19 dd of=c:\/test) sudo service ssh status fdisk -l fdisk -l sudo
099 dd if=/dev/sda | (ssh 192.168.10.19 dd of=c:\/test) sudo services ssh sudo service ssh fdisk -l cd /dev cd sdd1 ls sdd1 sdd1 sdd1 ls sdd1 cd .. sudo dd if=/
256dev/sda of=/dev/sdd1/test cd /dev cd sdd1 cd .. fdisk -l sudo dd if=/dev/sda of=/dev/sdd1 fdisk -l fdisk -l fdisk -l fdisk -l fdisk -l fdisk -l fdisk -l fdis
413k -l ls dd if=/tmp of=/dev/sde dd if=eula of=/dev/sde dd if=/var of=/dev/sde pscp cd.. ls cd .. ls cd dev ls fdisk -l uname -a echo linux uname uname -x unam
570e -a cd etc ls cd .. cd .. cd etc ls redhat_lsb_ -a redhat_lsb_init -a *-release man dd man dd
```

Figure 19: Bash History

vdiManager Files

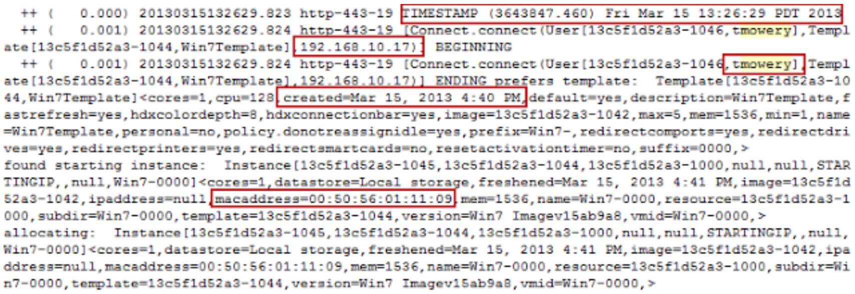
When examining the vdiManager virtual hard disk, the investigator is capable of pulling all users that were associated to the drive, what templates the user was assigned to, the groups the user was a part of, the user's ID in Citrix, and more.



```
13c5f1d52a3-1019 add user user \
    accountname efleisher \
    firstname Ethan \
    group Domain+Admins%7CDomain+Users \
    id 13c5f1d52a3-1019 \
    lastname Fleisher \
    roles USER \
    templates 13c5f1d52a3-1044 \
    username Efleisher \
    userprincipalname efleisher%40c3di.local \

remember 13c5f1d52a3-1031 add user user \
    accountname test1 \
    firstname Test \
    group Domain+Users \
    id 13c5f1d52a3-1031 \
    lastname "" \
    roles USER \
    templates 13c5f1d52a3-1052 \
    username test1 \
    userprincipalname test1%40c3di.local \

remember 13c5f1d52a3-1046 add user user \
    accountname tmowery \
    firstname Trevin \
    group Domain+Users \
    id 13c5f1d52a3-1046 \
    lastname Mowery \
    roles USER \
    templates 13c5f1d52a3-1044%7C13c5f1d52a3-1052 \
    username tmowery \
    userprincipalname tmowery%40c3di.local \
```

Figure 20: vdiManager User Entries

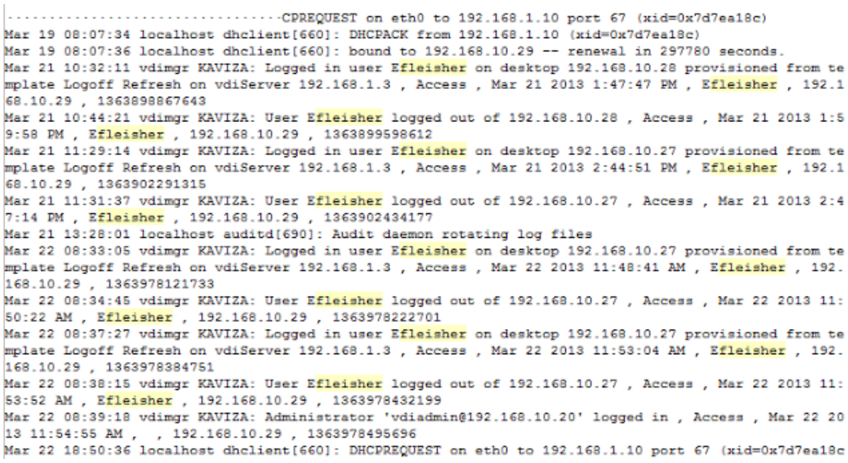
This VHD also contained logs in reference to the spawning of virtual machines, including the time and date that it was created. The log will list the user that connected, the machine IP address that the connection originated from, the template the user logged in with, and the MAC address that the created virtual machine was given.



```
  ++ (    0.000) 20130315132629.823 http-443-19 TIMESTAMP (3643847.460) Fri Mar 15 13:26:29 PDT 2013
  ++ (    0.001) 20130315132629.824 http-443-19 [Connect.connect(User[13c5f1d52a3-1046,tmowery],Templ
ate[13c5f1d52a3-1044,Win7Template],192.168.10.17)] BEGINNING
  ++ (    0.001) 20130315132629.824 http-443-19 [Connect.connect(User[13c5f1d52a3-1046,tmowery],Templ
ate[13c5f1d52a3-1044,Win7Template],192.168.10.17)] ENDING prefers template:  Template[13c5f1d52a3-10
44,Win7Template]<cores=1,cpu=128,created=Mar 15, 2013 4:40 PM,default=yes,description=Win7Template,f
astrefresh=yes,hdxcolordepth=8,hdxconnectionbar=yes,image=13c5f1d52a3-1042,max=5,mem=1536,min=1,name
=Win7Template,personal=no,policy.donotreassignidle=yes,prefix=Win7-,redirectcomports=yes,redirectdri
ves=yes,redirectprinters=yes,redirectsmartcards=no,resetactivationtimer=no,suffix=0000,>
found starting instance:  Instance[13c5f1d52a3-1045,13c5f1d52a3-1044,13c5f1d52a3-1000,null,null,STAR
TINGIP,,null,Win7-0000]<cores=1,datastore=Local storage,freshened=Mar 15, 2013 4:41 PM,image=13c5f1d
52a3-1042,ipaddress=null,macaddress=00:50:56:01:11:09,mem=1536,name=Win7-0000,resource=13c5f1d52a3-1
000,subdir=Win7-0000,template=13c5f1d52a3-1044,version=Win7 Imagev15ab9a8,vmid=Win7-0000,>
allocating:  Instance[13c5f1d52a3-1045,13c5f1d52a3-1044,13c5f1d52a3-1000,null,null,STARTINGIP,,null,
Win7-0000]<cores=1,datastore=Local storage,freshened=Mar 15, 2013 4:41 PM,image=13c5f1d52a3-1042,ipa
ddress=null,macaddress=00:50:56:01:11:09,mem=1536,name=Win7-0000,resource=13c5f1d52a3-1000,subdir=Wi
n7-0000,template=13c5f1d52a3-1044,version=Win7 Imagev15ab9a8,vmid=Win7-0000,>
```

Figure 21: vdiManager User Connection

Further investigation of these logs provides more information on user interaction with virtual machines, specifying when a user logged both in and out of a desktop, what IP address it was given, what template it was provisioned from, and what vdiServer it accessed.



```
-----------------------------------CPREQUEST on eth0 to 192.168.1.10 port 67 (xid=0x7d7ea18c)
Mar 19 08:07:34 localhost dhclient[660]: DHCPACK from 192.168.1.10 (xid=0x7d7ea18c)
Mar 19 08:07:36 localhost dhclient[660]: bound to 192.168.10.29 -- renewal in 297780 seconds.
Mar 21 10:32:11 vdimgr KAVIZA: Logged in user Efleisher on desktop 192.168.10.28 provisioned from te
mplate Logoff Refresh on vdiServer 192.168.1.3 , Access , Mar 21 2013 1:47:47 PM , Efleisher , 192.1
68.10.29 , 1363898867643
Mar 21 10:44:21 vdimgr KAVIZA: User Efleisher logged out of 192.168.10.28 , Access , Mar 21 2013 1:5
9:58 PM , Efleisher , 192.168.10.29 , 1363899598612
Mar 21 11:29:14 vdimgr KAVIZA: Logged in user Efleisher on desktop 192.168.10.27 provisioned from te
mplate Logoff Refresh on vdiServer 192.168.1.3 , Access , Mar 21 2013 2:44:51 PM , Efleisher , 192.1
68.10.29 , 1363902291315
Mar 21 11:31:37 vdimgr KAVIZA: User Efleisher logged out of 192.168.10.27 , Access , Mar 21 2013 2:4
7:14 PM , Efleisher , 192.168.10.29 , 1363902434177
Mar 21 13:28:01 localhost auditd[690]: Audit daemon rotating log files
Mar 22 08:33:05 vdimgr KAVIZA: Logged in user Efleisher on desktop 192.168.10.27 provisioned from te
mplate Logoff Refresh on vdiServer 192.168.1.3 , Access , Mar 22 2013 11:48:41 AM , Efleisher , 192.
168.10.29 , 1363978121733
Mar 22 08:34:45 vdimgr KAVIZA: User Efleisher logged out of 192.168.10.27 , Access , Mar 22 2013 11:
50:22 AM , Efleisher , 192.168.10.29 , 1363978222701
Mar 22 08:37:27 vdimgr KAVIZA: Logged in user Efleisher on desktop 192.168.10.27 provisioned from te
mplate Logoff Refresh on vdiServer 192.168.1.3 , Access , Mar 22 2013 11:53:04 AM , Efleisher , 192.
168.10.29 , 1363978384751
Mar 22 08:38:15 vdimgr KAVIZA: User Efleisher logged out of 192.168.10.27 , Access , Mar 22 2013 11:
53:52 AM , Efleisher , 192.168.10.29 , 1363978432199
Mar 22 08:39:18 vdimgr KAVIZA: Administrator 'vdiadmin@192.168.10.20' logged in , Access , Mar 22 20
13 11:54:55 AM ,  , 192.168.10.29 , 1363978495696
Mar 22 18:50:36 localhost dhclient[660]: DHCPREQUEST on eth0 to 192.168.1.10 port 67 (xid=0x7d7ea18c
```

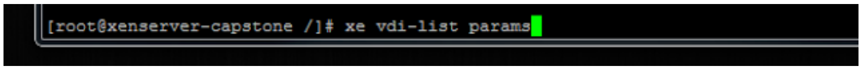
Figure 22: vdiManager Connection Log

This log file is also able to be obtained via the vdiManager web portal. Within the admin menu is a View Audit Log function that provides an excel spreadsheet containing user activity.

Virtual Machine Files

The virtual hard disk files are the focal point of investigation when attempting to uncover information from non-persistent machines. The non-persistent VHD's will be destroyed when the reset policy is set, either at logout or on a schedule. Due to this, snapshots of these hard disks are necessary to uncover potential evidence.

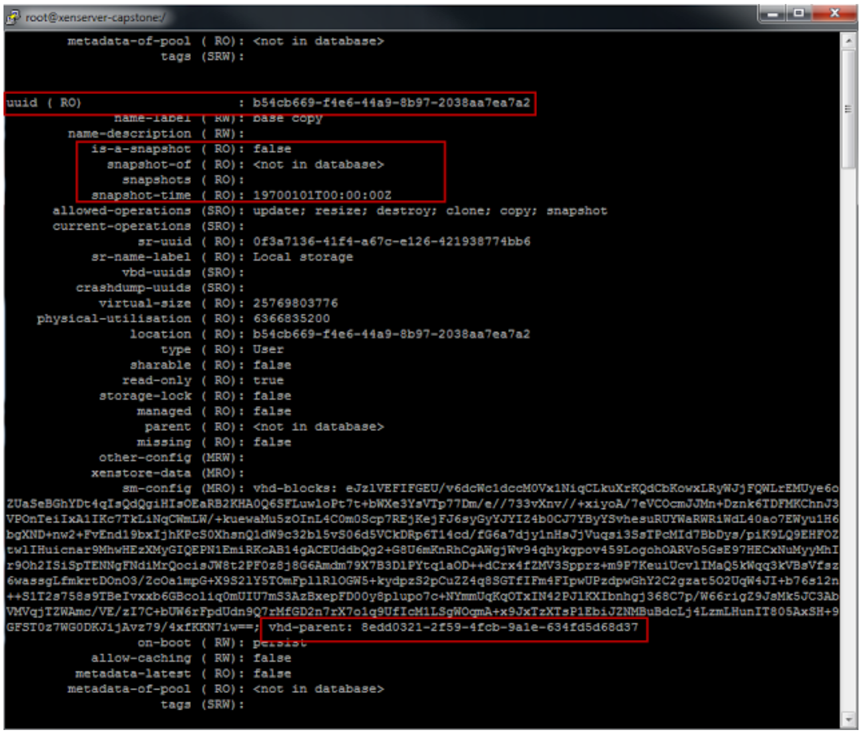
Each virtual hard disk contains a header that points to its parent drive. Although EnCase was listing these pointers at the beginning and making it relatively easy to navigate between, server-side verification of this was completed. Running the command xe vdi-list params will provide a list of metadata about each virtual hard disk.



```
[root@xenserver-capstone /]# xe vdi-list params
```

Figure 23: VDI-List Parameters Command

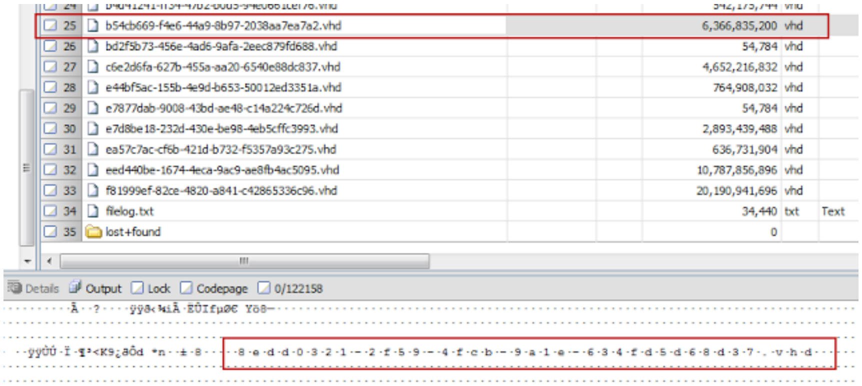
This command can populate a list that will tell the user the UUID of the virtual disk, whether it is a snapshot or not, the time of the snapshot if one was taken, the number of snapshots taken, and the virtual hard disks parent.



```
         metadata-of-pool ( RO): <not in database>
                     tags (SRW):


uuid ( RO)                    : b54cb669-f4e6-44a9-8b97-2038aa7ea7a2
               name-label ( RW): base copy
         name-description ( RW):
            is-a-snapshot ( RO): false
              snapshot-of ( RO): <not in database>
                snapshots ( RO):
            snapshot-time ( RO): 19700101T00:00:00Z
       allowed-operations (SRO): update; resize; destroy; clone; copy; snapshot
       current-operations (SRO):
                  sr-uuid ( RO): 0f3a7136-41f4-a67c-e126-421938774bb6
            sr-name-label ( RO): Local storage
                vbd-uuids (SRO):
          crashdump-uuids (SRO):
             virtual-size ( RO): 25769803776
     physical-utilisation ( RO): 6366835200
                 location ( RO): b54cb669-f4e6-44a9-8b97-2038aa7ea7a2
                     type ( RO): User
                 sharable ( RO): false
                read-only ( RO): true
             storage-lock ( RO): false
                  managed ( RO): false
                   parent ( RO): <not in database>
                  missing ( RO): false
             other-config (MRW):
           xenstore-data (MRO):
                sm-config (MRO): vhd-blocks: eJzlVEFIFGEU/v6dcWc1dccM0Vx1NiqCLkuXrKQdCbKowxLRyWJjFQWLrEMUye6o
ZUaSeBGhYDt4qIsQdQgiHIsOEaRB2KHA0Q6SFLuwloPt7t+bWXe3YsVTp77Dm/e//733vXnv//+xiyoA/7eVCOcmJJMn+Dznk6TDFMKChnJ3
VPOnTeiIxA1IKc7TkLiNqCWmLW/+kuewaMu5zOInL4C0m0Scp7REjKejFJ6syGyYJYIZ4b0CJ7YByYSvhesuRUYWaRWRiWdL40ao7EWyu1H6
bgXND+nw2+FvEnd19bxIjhKPcS0XhsnQ1dW9c32bl5vS06d5VCkDRp6T14cd/fG6a7djy1nHsJjVuqsi3SsTPcMId7BbDys/piK9LQ9EHFOZ
twlIHuicnar9MhwHEzXMyGIQEPN1EmiRKcAB14gACEUddbQg2+G8U6mKnRhCgAWgjWv94qhykgpov459LogohOARVo5GsE97HECxNuMyyMhI
r9Oh2ISiSpTENNgFNdiMrQocisJW8t2PF0z8j8G6Amdm79X7B3D1PYtq1aOD++dCrx4fZMV3Spprz+m9P7KeuiUcvlIMaQ5kWqq3kVBsVfsz
6wassgLfmkrtDOnO3/ZcOa1mpG+X9S2lY5TOmFpllR1OGW5+kydpzS2pCuZZ4q8SGTfIFm4FIpwUPzdpwGhY2C2gzat5O2UqW4JI+b76s12n
++S1T2s758s9TBeIvxxb6GBcoliq0mUIU7mS3AzBxepFD00y8plupo7c+NYmmUqKqOTxIN42PJ1KXIbnhgj368C7p/W66rigZ9JsMk5JC3Ab
VMVqjTZWAmc/VE/zI7C+bUW6rFpdUdn9Q7rMfGD2n7rX7o1q9UfIcM1LSgWOqmA+x9JxTzXTsP1EbiJZNMBuBdcLj4LzmLHunIT805AxSH+9
GFST0z7WG0DKJ1jAvz79/4xfKKN7iw==; vhd-parent: 8edd0321-2f59-4fcb-9a1e-634fd5d68d37
                  on-boot ( RW): persist
            allow-caching ( RW): false
          metadata-latest ( RO): false
         metadata-of-pool ( RO): <not in database>
                     tags (SRW):
```

Figure 24: Parent UUID Verification

By proving that the virtual disk with the UUID of b54cb669-f4e6-44a9-8b97-2038aa7ea7a2 has the parent with the UUID of 8edd0321-2f59-4fcb-9a1e-634fd5d68d37, the results being displayed by EnCase were verified and thus trustworthy.

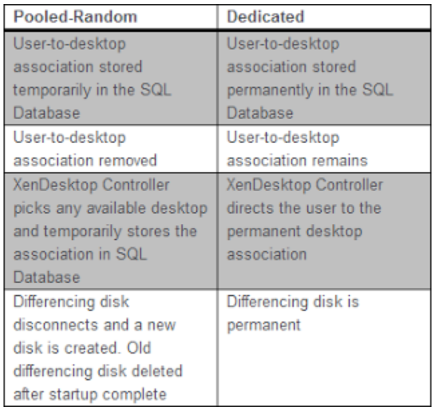


□	24	b4d41241-f134-4702-b0d5-94e0661ce176.vhd	342,173,744	vhd	
□	25	b54cb669-f4e6-44a9-8b97-2038aa7ea7a2.vhd	6,366,835,200	vhd	
□	26	bd2f5b73-456e-4ad6-9afa-2eec879fd688.vhd	54,784	vhd	
□	27	c6e2d6fa-627b-455a-aa20-6540e88dc837.vhd	4,652,216,832	vhd	
□	28	e44bf5ac-155b-4e9d-b653-50012ed3351a.vhd	764,908,032	vhd	
□	29	e7877dab-9008-43bd-ae48-c14a224c726d.vhd	54,784	vhd	
□	30	e7d8be18-232d-430e-be98-4eb5cffc3993.vhd	2,893,439,488	vhd	
□	31	ea57c7ac-cf6b-421d-b732-f5357a93c275.vhd	636,731,904	vhd	
□	32	eed440be-1674-4eca-9ac9-ae8fb4ac5095.vhd	10,787,856,896	vhd	
□	33	f81999ef-82ce-4820-a841-c42865336c96.vhd	20,190,941,696	vhd	
□	34	filelog.txt	34,440	txt	Text
□	35	lost+found	0		

```
·········Ã··?····ÿÿ8<¾iÃ·ÊÛIfµØ€ Yö8—·····························


··ÿÿÛÚ·Ï·¶³<K9¿ãÕd *n··±·8···8·e·d·d·0·3·2·1·–·2·f·5·9·–·4·f·c·b·–·9·a·1·e·–·6·3·4·f·d·5·d·6·8·d·3·7·.·v·h·d·····
```

Figure 25: EnCase Parent UUID Correlation to XenServer Verification

As previously mentioned, there are two virtual hard disk files associated with each snapshot. The first of these disks is the identity disk, which will typically range up to sixteen megabytes and simply provides each VM with a unique identity. The second disk, referred to as the difference disk, is "used to store any writes made to the VM. The disk is thin provisioned (if supported by the storage) and will increase to the maximum size of the base VM if required," (Feller).



Pooled-Random	Dedicated
User-to-desktop association stored temporarily in the SQL Database	User-to-desktop association stored permanently in the SQL Database
User-to-desktop association removed	User-to-desktop association remains
XenDesktop Controller picks any available desktop and temporarily stores the association in SQL Database	XenDesktop Controller directs the user to the permanent desktop association
Differencing disk disconnects and a new disk is created. Old differencing disk deleted after startup complete	Differencing disk is permanent

Figure 26: Disk Creation (Source: Feller)

Review of the identity disk yields just a pointer UUID to the difference disk associated with it. The difference disk contains content from the virtual machine as well as a pointer to the golden image it was created from. Although this is all shown as unallocated space and needs manual parsing, some very helpful artifacts remain and can be found.

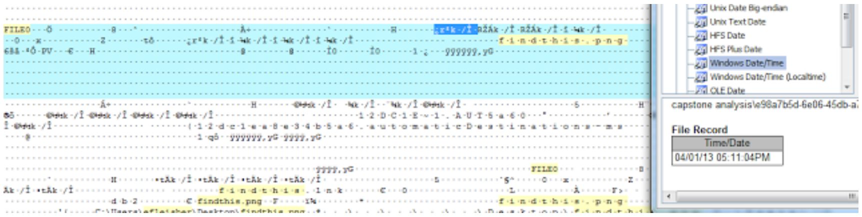
A virtual machine was created that had limited activity on it but with enough different items to look for. The following table depicts the activity on the machine.

Time	Activity
5:09pm	Visited Msn.com using Internet Explorer (IE)
5:09pm	Visited Amazon.com using IE
5:10pm	Visited Google.com using IE
5:10pm	Ran MSPaint.exe
5:11pm	Saved a paint file – "findthis.png" to the desktop
5:12pm	Visited www.champlain.edu
6:10pm	Google search for "april fools jokes"
6:11pm	Visited dig4n6.blogspot.com
6:11pm	Saved file from website – xzibit_meme.png
6:11pm	Changed the file type of xzibit_meme.png to xzibit_meme.bmp
6:13pm	Created a file named Deleted Item and deleted it, removed it from the recycling bin
6:18pm	Changed file type of xzibit_meme.bmp to xzibit_meme.jpeg

Due to the disk being all unallocated space, the quickest way to determine if any information was still recoverable on the drive was by doing simple keyword searches. Keyword searches were executed for the following phrases:

"msn.com", "amazon.com", "google.com", "paint", "paint.exe", "findthis.png", "findthis", "efleisher", "www.champlain.edu", "april fools jokes", "dig4n6.blogspot.com", "deleted item", "xzibit_meme".

One of the most intriguing and important artifacts that was recovered were multiple entries from the Master file table (MFT). These MFT entries contain accurate time stamps and accurate information in regards to the files that were created on the virtual machine.



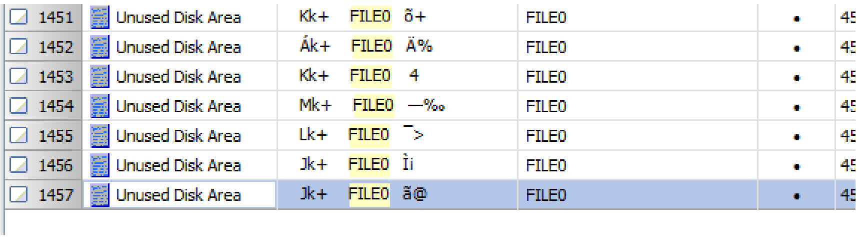
capstone analysis\e98a7b5d-6e06-45db-a

File Record

Time/Date
04/01/13 05:11:04PM

Figure 27: MFT Entry for "findthis.png" with accurate creation date

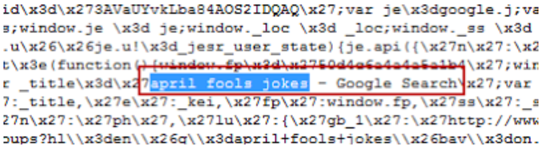
A search was done for the phrase "FILE0" as this is a typical indicator of a MFT record. There were a total of 1457 hits in response to this keyword. This is at least indicative of 1457 MFT entries being present on this virtual disk. There were MFT entries present for each file and folder that was created on the machine which will at least provide information about some pertinent items on the machine.



☐	1451	Unused Disk Area	Kk+ FILE0 õ+	FILE0	•	45
☐	1452	Unused Disk Area	Ák+ FILE0 Ä%	FILE0	•	45
☐	1453	Unused Disk Area	Kk+ FILE0 4	FILE0	•	45
☐	1454	Unused Disk Area	Mk+ FILE0 —‰	FILE0	•	45
☐	1455	Unused Disk Area	Lk+ FILE0 ¯>	FILE0	•	45
☐	1456	Unused Disk Area	Jk+ FILE0 Ìi	FILE0	•	45
☐	1457	Unused Disk Area	Jk+ FILE0 ã@	FILE0	•	45

Figure 28: Keyword results for MFT Entry Header "FILE0"

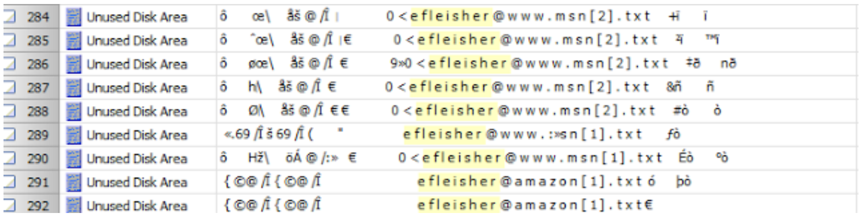
The keyword search for the phrase "april fools jokes" successfully pulled the Google search in plaintext from the unallocated space as well.



```
id\x3d\x273AVaUYvkLba84AOS2IDQAQ\x27;var je\x3dgoogle.j;va
s;window.je \x3d je;window._loc \x3d _loc;window._ss \x3d
.u\x26\x26je.u!\x3d_jesr_user_state){je.api({\x27n\x27:\x2
t\x3e(function(){window.fp\x3d\x2750d4e6a4a4a5a1b4\x27;wir
r _title\x3d\x27april fools jokes - Google Search\x27;var
7:_title,\x27e\x27:_kei,\x27fp\x27:window.fp,\x27ss\x27:_s
27n\x27:\x27ph\x27,\x27lu\x27:{\x27gb_1\x27:\x27http://www
oups?hl\\x3den\\x26q\\x3dapril+fools+jokes\\x26bav\\x3don.
```

Figure 29: Retrieved Google Search

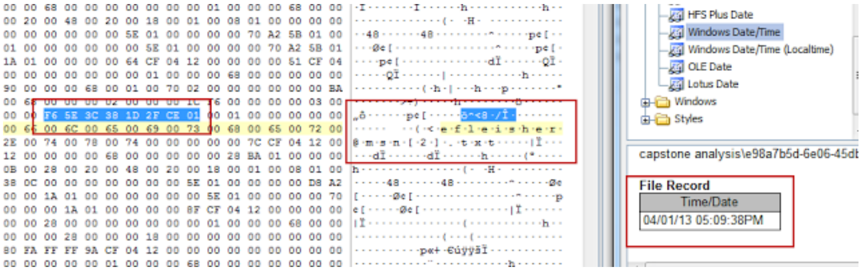
A keyword search was done with a username of "efleisher" to search for any data that may be relevant to what the user was doing on the computer. Nearly two thousand hits responded containing information primarily relating to browsing history. The data was in a plaintext readable format, with results being displayed in similar format to "efleisher@amazon.com".



284	Unused Disk Area	ô œ\ åš @ /Î 0 < e f l e i s h e r @ w w w . m s n [2] . t x t ᵻ ï
285	Unused Disk Area	ô ˆœ\ åš @ /Î |€ 0 < e f l e i s h e r @ w w w . m s n [2] . t x t ¬ ™ï
286	Unused Disk Area	ô øœ\ åš @ /Î € 9»0 < e f l e i s h e r @ w w w . m s n [2] . t x t ‡ð nð
287	Unused Disk Area	ô h\ åš @ /Î € 0 < e f l e i s h e r @ w w w . m s n [2] . t x t &ñ ñ
288	Unused Disk Area	ô Ø\ åš @ /Î €€ 0 < e f l e i s h e r @ w w w . m s n [2] . t x t ‡ò ò
289	Unused Disk Area	«.69 /Î š 69 /Î (" e f l e i s h e r @ w w w . :»s n [1] . t x t ƒò
290	Unused Disk Area	ô Hž\ öÁ @ /:» € 0 < e f l e i s h e r @ w w w . m s n [1] . t x t Éò °ò
291	Unused Disk Area	{ ©@ /Î { ©@ /Î e f l e i s h e r @ a m a z o n [1] . t x t ó þò
292	Unused Disk Area	{ ©@ /Î { ©@ /Î e f l e i s h e r @ a m a z o n [1] . t x t €

Figure 30: User Activity via Username Search

This data provides the investigator with insight into the users browsing history. By manually parsing these entries, the investigator is able to ascertain when the username was accessing certain websites. These time stamps can be found prior to the website address. It will be stored in little endian hex format and will be eight bytes long.



```
00 00 68 00 00 00 00 00 00 00 01 00 00 00 68 00 00
00 20 00 48 00 20 00 18 00 01 00 08 01 00 00 00 00
00 00 00 00 00 00 5E 01 00 00 00 00 70 A2 5B 01 00
01 00 00 00 00 00 00 5E 01 00 00 00 00 70 A2 5B 01
1A 01 00 00 00 00 64 CF 04 12 00 00 00 00 51 CF 04
00 00 00 00 00 00 00 01 00 00 00 68 00 00 00 00 00
90 00 00 00 68 00 01 00 70 02 00 00 00 00 00 00 BA
00 68 00 00 00 02 00 00 00 1C 76 00 00 00 00 03 00
00 00 F6 5E 3C 38 1D 2F CE 01 00 01 00 00 00 00 00
00 66 00 6C 00 65 00 69 00 73 00 68 00 65 00 72 00
2E 00 74 00 78 00 74 00 00 00 00 00 7C CF 04 12 00
12 00 00 00 00 68 00 00 00 00 00 28 BA 01 00 00 00
0B 00 28 00 20 00 48 00 20 00 18 00 01 00 08 01 00
38 0C 00 00 00 00 00 00 00 5E 01 00 00 00 00 D8 A2
00 00 1A 01 00 00 00 00 00 00 5E 01 00 00 00 00 70
00 00 00 1A 01 00 00 00 00 8F CF 04 12 00 00 00 00
00 00 28 00 00 00 00 00 00 00 01 00 00 00 68 00 00
00 00 00 28 00 00 00 18 00 00 00 00 00 00 00 00 00
80 FA FF FF 9A CF 04 12 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 00 00 00 68 00 00 00 00 00 00 00
```

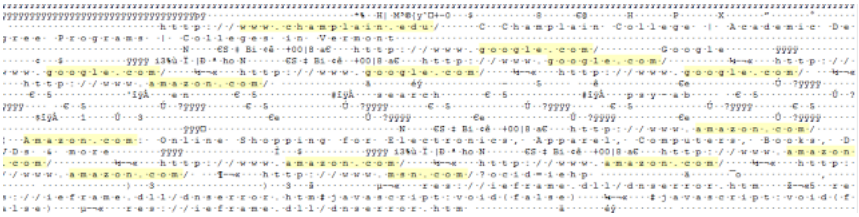
capstone analysis\e98a7b5d-6e06-45d

File Record

Time/Date
04/01/13 05:09:38PM

Figure 31: Internet History Timestamp Verification

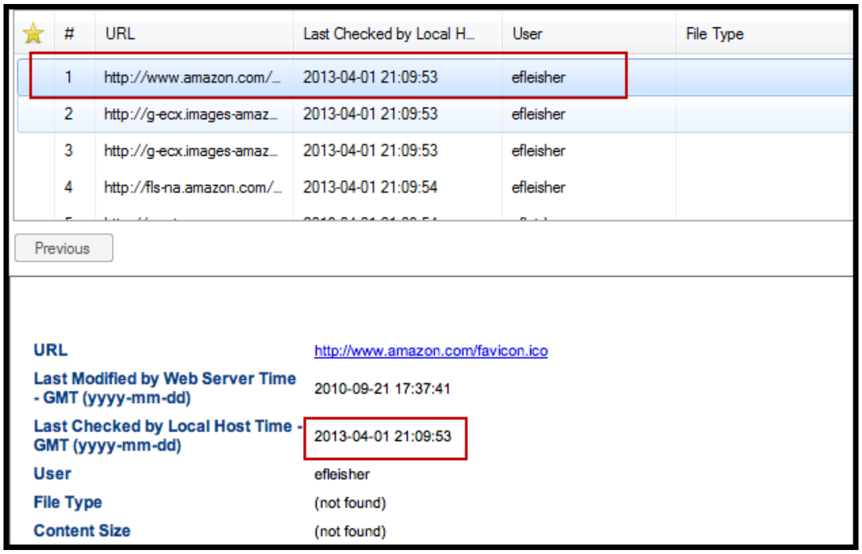
Through keyword searches of websites that were visited, an entry was found that revealed each website that was browsed to. The order that these websites were presented was in the reverse order that they were visited, with the last website browsed to being the first website listed in the entry. It is potentially indicative of a file that contained all web browsing history, similar to an index.dat file. Unlike most internet history entries, however, there were no records of potential timestamp information.



```
http://www.champlain.edu/ C Champlain College | Academic De
gree Programs | Colleges in Vermont
N €S‡ Bi cê +00|8 a€ http://www.google.com/ Google ÿÿÿÿ
c $ ÿÿÿÿ 13¾ù Ì |Ð* ho N €S‡ Bi cê +00|8 a€ http://www.google.com/ ¼¬« http://
www.google.com/ ¼¬« http://www.google.com/ ¼¬« http://www.google.com/ ¼¬«
http://www.amazon.com/ â éý 5 ê €e Ù ?ÿÿÿÿ
€ 5 'iÿÅ en € 5 #iÿÅ search € 5 #iÿÅ pay-ab € 5 Ù ?
ÿÿÿÿ € 5 Ù ?ÿÿÿÿ € 5 Ù ?ÿÿÿÿ € 5 Ù ?ÿÿÿÿ € 5
$iÿÅ 1 Ù 3 €e Ù ?ÿÿÿÿ €e Ù ?ÿÿÿÿ €e Ù ?ÿÿÿÿ
ÿÿÿ□ N €S‡ Bi cê +00|8 a€ http://www.amazon.com/
: Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, D
VDs & more ÿÿÿÿ Ì $ ÿÿÿÿ 13¾ù Ì |Ð* ho N €S‡ Bi cê +00|8 a€ http://www.amazon
.com/ ¼¬« http://www.amazon.com/ ¼¬« http://www.amazon.com/ ¼¬« http:
//www.amazon.com/ Ì¬« http://www.msn.com/?ocid=iehp ã ¯o ,
) 3 ) 3 ã µ¬« res://ieframe.dll/dnserror.htm ž¬«5 re
s://ieframe.dll/dnserror.htm‡javascript:void(false) ¼¬« ‡javascript:void(f
alse) µ¬« res://ieframe.dll/dnserror.htm ã éý
```

Figure 32: Complete Browsing History

With the previous findings presenting a plethora of internet history information, the next step was to try an automated tool. Internet history tools will attempt to perform an automated acquisition of the internet history on a hard disk and present the findings to an investigator in an easy to read format. Internet Evidence Finder v5 was able to successfully parse and extract internet history, including cookies, with accurate time stamps and user correlation.

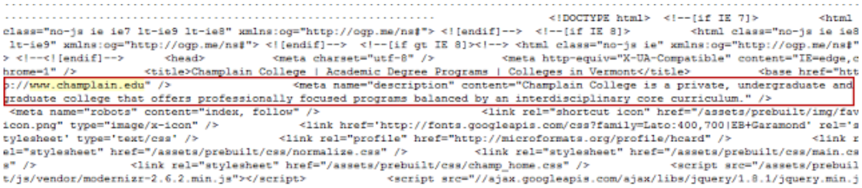


★	#	URL	Last Checked by Local H...	User	File Type
	1	http://www.amazon.com/...	2013-04-01 21:09:53	efleisher	
	2	http://g-ecx.images-amaz...	2013-04-01 21:09:53	efleisher	
	3	http://g-ecx.images-amaz...	2013-04-01 21:09:53	efleisher	
	4	http://fls-na.amazon.com/...	2013-04-01 21:09:54	efleisher	

URL	http://www.amazon.com/favicon.ico
Last Modified by Web Server Time - GMT (yyyy-mm-dd)	2010-09-21 17:37:41
Last Checked by Local Host Time - GMT (yyyy-mm-dd)	2013-04-01 21:09:53
User	efleisher
File Type	(not found)
Content Size	(not found)

Figure 33: Successful Internet Evidence Finder Parsing of VHD

Further research into web browsing artifacts provided HTML code for specific websites that were visited. This code provides a plaintext view of some of the information that was on the webpage when it was visited by the user.

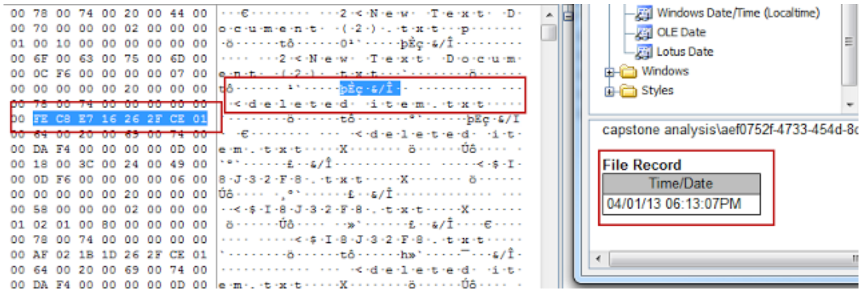


```
<!DOCTYPE html>  <!--[if IE 7]>          <html
class="no-js ie ie7 lt-ie9 lt-ie8" xmlns:og="http://ogp.me/ns#"> <![endif]-->  <!--[if IE 8]>         <html class="no-js ie ie8
 lt-ie9" xmlns:og="http://ogp.me/ns#"> <![endif]-->  <!--[if gt IE 8]><!--> <html class="no-js ie" xmlns:og="http://ogp.me/ns#"
> <!--<![endif]-->       <head>         <meta charset="utf-8" />          <meta http-equiv="X-UA-Compatible" content="IE=edge,c
hrome=1" />        <title>Champlain College | Academic Degree Programs | Colleges in Vermont</title>          <base href="htt
p://www.champlain.edu" />              <meta name="description" content="Champlain College is a private, undergraduate and
graduate college that offers professionally focused programs balanced by an interdisciplinary core curriculum." />
 <meta name="robots" content="index, follow" />                   <link rel="shortcut icon" href="/assets/prebuilt/img/fav
icon.png" type="image/x-icon" />           <link href='http://fonts.googleapis.com/css?family=Lato:400,700|EB+Garamond' rel='s
tylesheet' type='text/css' />          <link rel="profile" href="http://microformats.org/profile/hcard" />          <link r
el="stylesheet" href="/assets/prebuilt/css/normalize.css" />          <link rel="stylesheet" href="/assets/prebuilt/css/main.cs
s" />            <link rel="stylesheet" href="/assets/prebuilt/css/champ_home.css" />           <script src="/assets/prebuil
t/js/vendor/modernizr-2.6.2.min.js"></script>          <script src="//ajax.googleapis.com/ajax/libs/jquery/1.8.1/jquery.min.j
```

Figure 34: Plaintext HTML Code of Webpage

An important and common artifact that is looked at in a forensic investigation is deleted items. A deleted item can mean many things to an investigator, such as an attempt to hide information, an attempt at removing evidence, or perhaps merely an attempt at removing clutter. Both data recovery and forensic investigations frequently deal with deleted items, thus making the ability to recover them a desirable skill.

During this research, a text file was created named deleted item. This item was created on April 1st, 2013 at 6:13:07pm and immediately deleted afterwards at 6:13:20pm. The keyword search for this particular artifact provided multiple hits, including accurate timestamps for the file creation time.



```
00 78 00 74 00 20 00 44 00   ···€·········  ···2·<·N·e·w· ·T·e·x·t· ·D·
00 70 00 00 00 02 00 00 00   o·c·u·m·e·n·t· ·(·2·)·.·t·x·t···p·······
01 00 10 00 00 00 00 00 00   ·ö·······tô······0¹`·····þÈç·&/Î·········
00 6F 00 63 00 75 00 6D 00   ····  ···2·<·N·e·w· ·T·e·x·t· ·D·o·c·u·m·
00 0C F6 00 00 00 00 07 00   e·n·t· ·(·2·)·.·t·x·t···`·········ö······
00 00 00 00 00 20 00 00 00   tô······ ¹`·····þÈç·&/Î·  ··········  ···
00 78 00 74 00 00 00 00 00   ·<·d·e·l·e·t·e·d· ·i·t·e·m·.·t·x·t·····
00 FE C8 E7 16 26 2F CE 01   ·········ö······tô·········°`·······þÈç·&/Î
00 64 00 20 00 69 00 74 00   ·€·········  ···<·d·e·l·e·t·e·d· ·i·t·
00 DA F4 00 00 00 00 0D 00   e·m·.·t·x·t·····X·········ö······Úô·····
00 18 00 3C 00 24 00 49 00   `°`·······£··&/Î···················<·$·I·
00 0D F6 00 00 00 00 06 00   8·J·3·2·F·8·.·t·x·t·····X·········ö······
00 00 00 00 00 20 00 00 00   Úô····  ·,°`·······£··&/Î·················
00 58 00 00 00 02 00 00 00   ··<·$·I·8·J·3·2·F·8·.·t·x·t·····X·······
01 02 01 00 80 00 00 00 00   ö·······Úô····  ··»`·······£··&/Î····€····
00 78 00 74 00 00 00 00 00   ····  ······<·$·I·8·J·3·2·F·8·.·t·x·t·····
00 AF 02 1B 1D 26 2F CE 01   `·········ö·······tô·······h»`·····¯···&/Î·
00 64 00 20 00 69 00 74 00   ·············  ···<·d·e·l·e·t·e·d· ·i·t·
00 DA F4 00 00 00 00 0D 00   e·m·.·t·x·t·····X·········ö······Úô·····
```

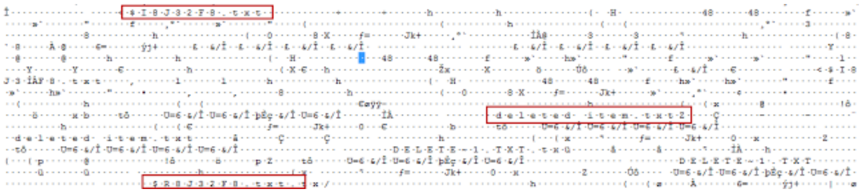
capstone analysis\aef0752f-4733-454d-8c

File Record

Time/Date
04/01/13 06:13:07PM

Figure 35: Accurate Timestamp of Deleted Item Creation Time

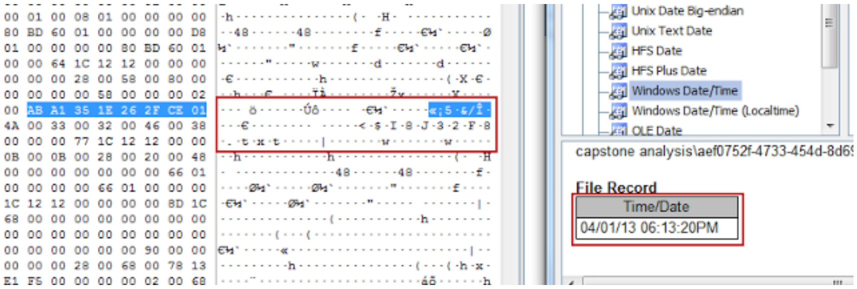
When a file is deleted on a Windows machine, it creates two files in the recycling bin that are associated with it. These files are known as “$I” and “$R” files. The $I file will contain the original name and path of the file, along with its deletion date. The $R file will retain the actual data of the file. When examining the evidence near the location to the original file, the investigator will find references to $I and $R files associated with the deleted item.



```
·$·I·8·J·3·2·F·8·.·t·x·t·
·d·e·l·e·t·e·d· ·i·t·e·m·.·t·x·t·2·
·d·e·l·e·t·e·d· ·i·t·e·m·.·t·x·t·
·D·E·L·E·T·E·~·1·.·T·X·T·
·$·R·8·J·3·2·F·8·.·t·x·t·
```

Figure 36: Discovery of Deleted Item as well as $I and $R files

In order to recover the deletion time of the file, it is necessary to obtain the creation time of the $I and $R files. This timestamp can be recovered by moving twenty bytes prior to the $ symbol and then obtaining the previous eight bytes prior to that. If done correctly, these eight bytes can be decoded in little-endian format to produce the created time of both $I and $R files, therefore the deletion time of the original file.



```
00 01 00 08 01 00 00 00 00
80 BD 60 01 00 00 00 00 D8
01 00 00 00 00 80 BD 60 01
00 00 64 1C 12 12 00 00 00
00 00 00 28 00 58 00 80 00
00 00 00 00 58 00 00 00 02
00 AB A1 35 1E 26 2F CE 01
4A 00 33 00 32 00 46 00 38
00 00 00 77 1C 12 12 00 00
0B 00 0B 00 28 00 20 00 48
00 00 00 00 00 00 00 66 01
00 00 00 00 66 01 00 00 00
1C 12 12 00 00 00 00 8D 1C
68 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 90 00 00
00 00 00 28 00 68 00 78 13
E1 F5 00 00 00 00 02 00 68
```

capstone analysis\aef0752f-4733-454d-8d6

File Record

Time/Date
04/01/13 06:13:20PM

Figure 37: Accurate Timestamp of Deleted Item Deletion Time

Perhaps the most interesting piece of evidence left behind on the virtual hard disk was the resemblance to a timeline of system activity. An entry within the virtual hard disk depicted a chain of events that occurred on the hard drive, including website visits, usernames, applications opening, files being created, and a list of some of the values that would have been updated on a system during the activity that occurred.

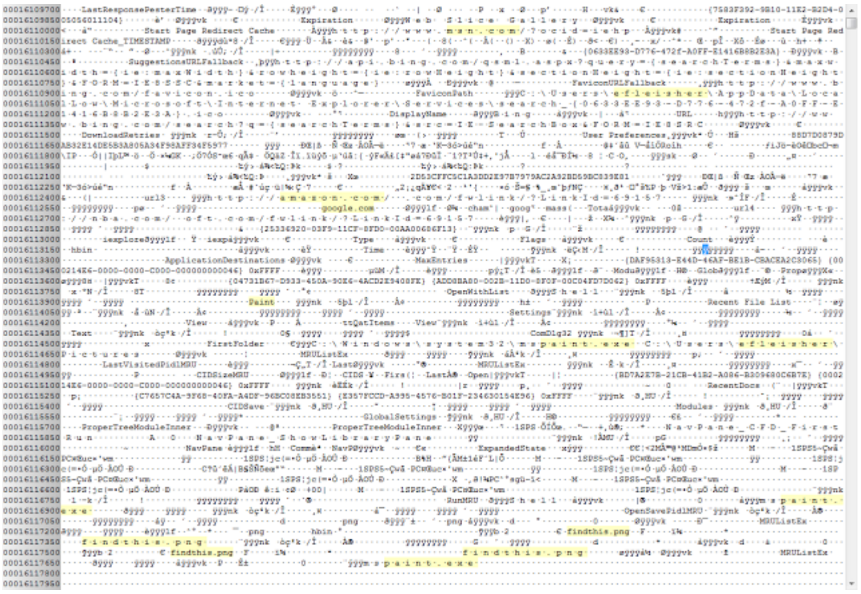


Figure 38: Entry reflecting Timeline of Events

What would you recommend my company to do?

Analysis of a Citrix Virtual Desktop Environment requires a fair amount of setup behind the scenes in order for it to be accomplished successfully. Without the presence of snapshots, an investigator would be hard pressed in finding any information that occurred on a pooled virtual machine. Although network monitoring tools could be put in place that would monitor everything that occurs, these options are often very costly and can still miss important artifacts. For a SMB or large business that is implementing a VDI, it would be recommended that snapshots be scheduled of at least the hard disk. Depending on storage available, if both disk and memory snapshots are capable, more information would be recoverable. This type of snapshot would require high quantities of storage.

Through implementation of snapshots and with appropriate administrative access, an investigator is able to manually parse through virtual hard disk files that the Citrix VDI-in-a-Box maintains. User information such as web history, created files and folders, opened programs, Google searches, passwords, deleted items, and master file table entries are all recoverable. This information may not be everything that is needed to crack the case, but it is surely a huge stepping stone into uncovering more information and perhaps even the “smoking gun.”

When looking at the vdiManager virtual hard disk, the investigator is able to obtain information about when a user is logging into a virtual desktop. Using this and information from the domain controller, further research needs to be done to be able to successfully link a specific user to a given UUID. Doing this will allow for the investigator to not need to sift through hundreds of hard drives for information, and instead have immediate access to which snapshots are linked to which users. Doing so will provide for a streamlined investigative process in both acquisition and analysis. Although this is just the tip of the iceberg, there is without a doubt much more information that can be uncovered. While access to these servers and machines are no longer available, I hope to someday expand this research, or at least see another professional take what has already been done and expand upon it to allow for even more thorough analysis of Citrix VDI's in the future.

References

"Citrix XenServer ® 5.6 Feature Pack 1 Administrator's Guide." Citrix RSS. Citrix, 24 Mar. 2011. Web.

“Create the First Windows Image." Citrix EDocs. Citrix, 12 Feb. 2013. Web.

"Create a VM Protection Policy." Citrix EDocs. Citrix, 26 Nov. 2012. Web.

Feller, Daniel. "Machine Creation Services Primer – Part 1." Citrix Blogs. Citrix, 28 June 2011. Web.

Hochmuth, Phil. "The Benefits Of Virtual Desktops." Forbes. Forbes Magazine, 12 Jan. 2010. Web.

"Internet Evidence Finder." Magnet Forensics. N.p., n.d. Web.

"Master Boot Record." Master Boot Record. Microsoft TechNet, n.d. Web.

"NTFS Master File Table (MFT)." NTFS Master File Table (MFT). N.p., n.d. Web

Powledge, Tom. "Top 7 SMB Information Protection Predictions for 2013." Endpoint, Cloud, Mobile & Virtual Security Solutions. Symantec, 4 Dec. 2012. Web.

Savitz, Eric. "Citrix Shares Rally As Q4 Results Crush Street Estimates." Forbes. Forbes Magazine, 30 Jan. 2013. Web.

Sweeney, Brandon. "State of SMB IT Report – Equip Yourself with These Stats to Help Make Vital IT Decisions." VMware SMB Blog. VMware, 20 Feb. 2013. Web.

Posted by Ethan Fleisher at 12:59 PM 4 comments:

FRIDAY, MARCH 22, 2013

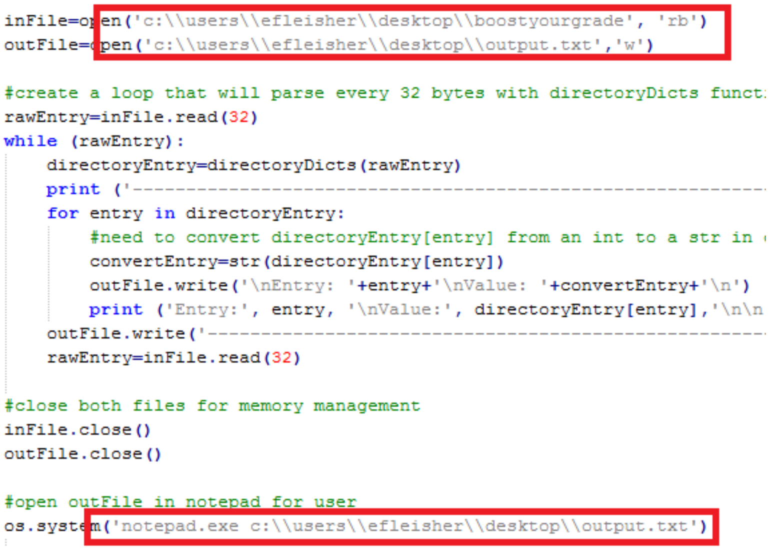
Script for FAT Root Directory Parsing

So I recently finished a class at Champlain College entitled Scripting for Digital Forensics. This class was quite simply bootcamp for learning Python. We started with basic operators and moved quickly through the eight weeks to eventually being able to write scripts that would be useful for the forensic workplace.

I decided to write my script on parsing a FAT root directory. At the time of choosing what to do, I was enrolled in another class focusing on file system forensics and we were doing in depth analysis of the FAT file system. Quickly turned into a no brainer as to what would be a useful and fun script for me to write.

A quick how-to for using the script:

With a FAT file system, navigate to the root directory using WinHex or a similar hex editing tool. Copy the entirety of the root directory and place it into a new file. Do a quick edit of the script and change the following sections:



```
inFile=open('c:\\users\\efleisher\\desktop\\boostyourgrade', 'rb')
outFile=open('c:\\users\\efleisher\\desktop\\output.txt','w')

#create a loop that will parse every 32 bytes with directoryDicts funct
rawEntry=inFile.read(32)
while (rawEntry):
    directoryEntry=directoryDicts(rawEntry)
    print ('-----------------------------------------------------------------
    for entry in directoryEntry:
        #need to convert directoryEntry[entry] from an int to a str in
        convertEntry=str(directoryEntry[entry])
        outFile.write('\nEntry: '+entry+'\nValue: '+convertEntry+'\n')
        print ('Entry:', entry, '\nValue:', directoryEntry[entry],'\n\n
    outFile.write('------------------------------------------------------------
    rawEntry=inFile.read(32)

#close both files for memory management
inFile.close()
outFile.close()

#open outFile in notepad for user
os.system('notepad.exe c:\\users\\efleisher\\desktop\\output.txt')
```

These sections just need to be changed to reflect the path of the root directory file that was created, and then the output path that the user desires. The third path that needs changed will allow for the script to open the file in notepad automatically.

All that being said, here is the script!

https://www.dropbox.com/s/qu93cx5ep4zt6mv/rootdirParse.py

Posted by Ethan Fleisher at 10:31 AM No comments:

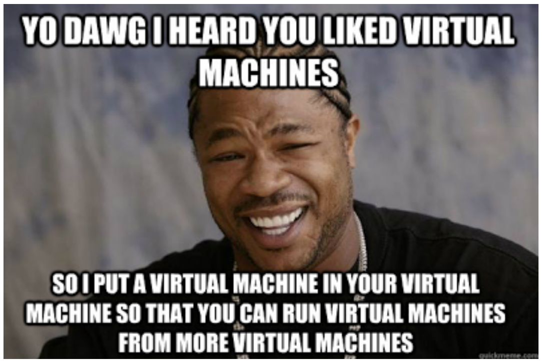
g+1 Recommend this on Google

THURSDAY, FEBRUARY 7, 2013

Creating a Citrix VDI for Digital Forensic Analysis

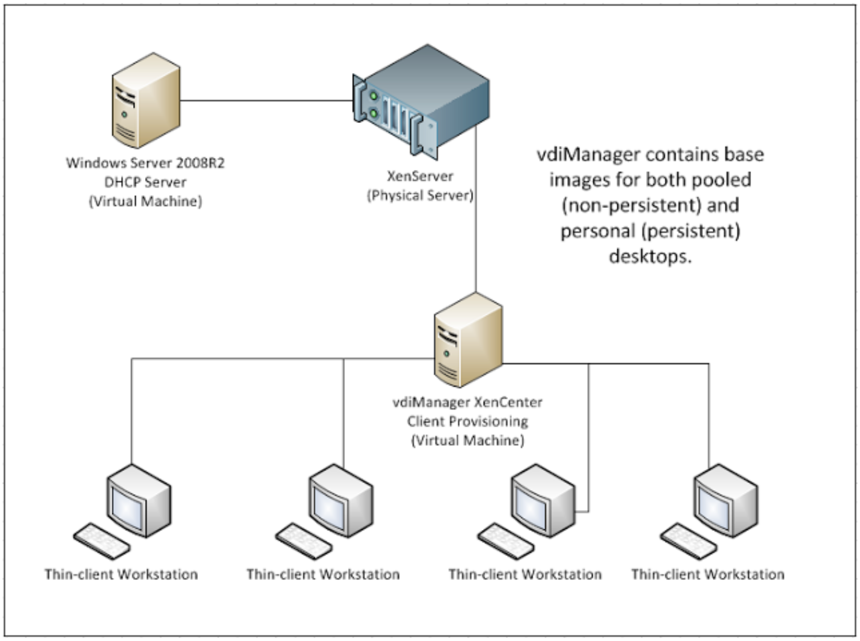
If the past few weeks have taught me anything so far, it would be that the process of creating a Citrix environment is rather difficult. What seemed like it would be rather cut and dry installing and setting up a few basic parameters has easily turned into what may be the hardest part of the project.

My initial issue was attempting to find a location that I could actually set a miniature virtual environment up in. My first thoughts were almost to the level of Inception – a virtual machine hypervisor hosting a virtual machine domain controller delegating IP's to multiple virtual machines that are each being hosted by…surprise!, a virtual machine (Citrix's vdiManager). For any of you that follow meme's, I'm pretty sure Xzibit would have something to say about my attempt here (if you don't get the reference, see here). Needless to say, it was an idea I dropped pretty quickly and went on to finding some hardware that I could use instead.

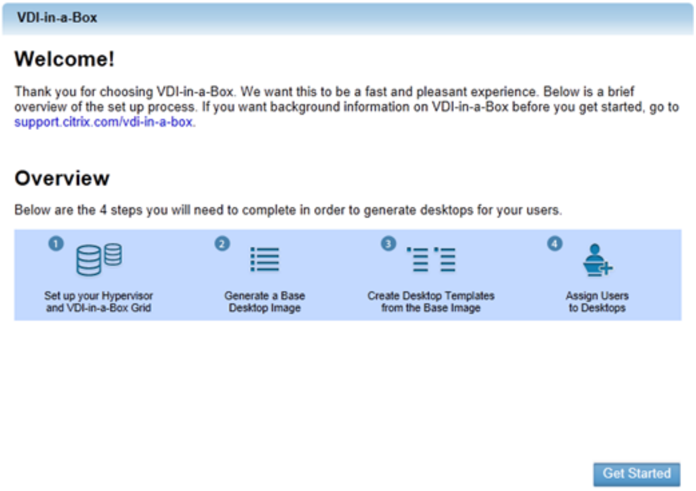

YO DAWG I HEARD YOU LIKED VIRTUAL MACHINES
SO I PUT A VIRTUAL MACHINE IN YOUR VIRTUAL MACHINE SO THAT YOU CAN RUN VIRTUAL MACHINES FROM MORE VIRTUAL MACHINES
quickmeme.com

Fortunately, the Senator Patrick Leahy Center for Digital Investigation (LCDI) has multiple servers, and one of them wasn't currently in use. This gave me the server that I needed for my hypervisor, and from here I was able to start moving forward. The first go around with real hardware involved setting up an ESXi 5 hypervisor on the Dell Server that would be used to host a virtual machine of XenServer. After doing some quick setup with this, which was rather painless, I ran into a few roadblocks. Attempting to create a Windows virtual machine using XenServer hosted on top of ESXi 5 prompted multiple errors and wouldn't allow for appropriate virtualization to ensue. Turns out I managed to overlook the fact that XenServer is a hypervisor and not similar to Windows Server that would rest on top of a hypervisor.

It tends to work out more often than not that the third time is the charm, and so far my third attempt is looking that way. This go around, I installed XenServer as the hypervisor on the server and then hosted vdiManager to it. I am using Citrix's VDI-in-a-Box (ViaB) to quickly set up a small environment that doesn't require multiple protocols and variables to be put into place that their other programs, such as Virtual Desktop, would.



There have definitely been a few stopping points that have been frustrating, but it's more little things on the internal network that I needed to tweak. For example, it was necessary to create a new domain controller due to limitations and restrictions set in place on the current domain controller. After I recognized a few of the simple networking problems, moving forward started to become easier and easier.


VDI-in-a-Box

Welcome!

Thank you for choosing VDI-in-a-Box. We want this to be a fast and pleasant experience. Below is a brief overview of the set up process. If you want background information on VDI-in-a-Box before you get started, go to support.citrix.com/vdi-in-a-box.

Overview

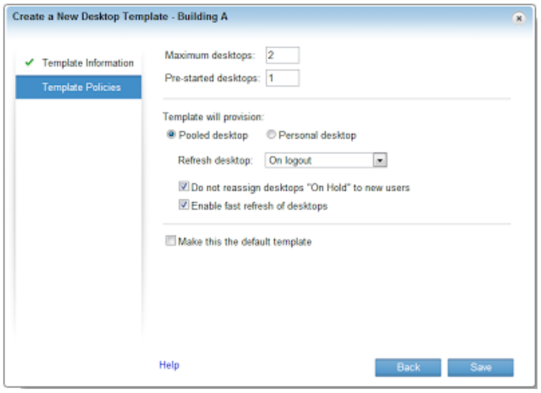
Below are the 4 steps you will need to complete in order to generate desktops for your users.

1 Set up your Hypervisor and VDI-in-a-Box Grid
2 Generate a Base Desktop Image
3 Create Desktop Templates from the Base Image
4 Assign Users to Desktops
Get Started

Setup Overview for VDI-in-a-Box

The next frustrating stop with my process came very quickly, though, and again I started face-palming every few minutes wondering why I couldn't get it working. In order to host a VM to vdiManager to create a base image, RDP needs to be configured as does File and Printer sharing. Although this is one of the most basic things to do on a computer, my virtual machine just wouldn’t have it. Yet again though, some quick network troubleshooting and I noticed that the DNS was incorrect, changed it, and the settings were up and running. Finally, at long last, the conversion to upload the image was beginning.

Stepping back from the setup process of the environment, it is important to take a look at the semantics of this project and the blogs that I will be writing. My initial blog post stated that I would be looking at the difference between persistent and non-persistent VDI’s. Though this is still the case and nothing has changed, ViaB uses different terminology to describe these two states of an image. A persistent image is known as a “personal desktop”, and a non-persistent image is referenced as a “pooled desktop.” Please take note that, although I will try to keep my own wording consistent, there may be images and references throughout to pooled versus personal desktops.



Create a New Desktop Template - Building A

Maximum desktops: 2
Pre-started desktops: 1

Template will provision:
● Pooled desktop ○ Personal desktop
Refresh desktop: On logout
☑ Do not reassign desktops "On Hold" to new users
☑ Enable fast refresh of desktops

□ Make this the default template

Template setup for Pooled vs Personal (Non-persistent vs Persistent)

Check back in the near future for more updates on the progress of this project. The environment should be finished setting up soon, and not too long after the real fun should start!

Please feel free to leave any comments and/or suggestions for me!

Posted by Ethan Fleisher at 6:58 AM 3 comments:

g+1 Recommend this on Google

Home Older Posts

Subscribe to: Posts (Atom)

Picture Window template. Powered by Blogger.