

# VMware server(ESXi) 수집 방법

---

*An, HwiHang*

*keyman.zero@gmail.com*





## 1. ESXi 는?

- 가상화 개념
- 사용 목적 및 기능
- VM을 구성하는 파일들

## 2. ESXi 데이터 수집

- 처음뵙겠습니다 ESXi
- Datastore browser로 저장 구조 확인
- SSH를 이용한 VM 확인 및 수집
- 가동중인 VM 확인 및 수집
- 그 외 수집 대상

## 3. VMDK 분석방법

# ESXi는?

- 가상화 개념
- 사용 목적 및 기능
- VM을 구성하는 파일들

## 가상화의 개념

### 가상화의 장점

- 하나의 물리적 시스템에서 여러 가상 머신 실행이 가능
- 각 가상머신은 단일 물리적 컴퓨터의 리소스를 공유
- 즉, 유휴 리소스를 최소화 할 수 있고, 다양한 OS를 동시에 구동하는 것이 가능
  - ✓ 그 외 관리 용이성 증대, 신속한 구축과 해체, 데이터센터의 규모 축소 등



### Traditional Architecture

- Single operating system
- Single application



### Virtual Architecture

- Virtualize many VMs using VMware Hypervisor

Using Hypervisor?

## 가상화의 개념

### ■ 하이퍼바이저(Hypervisor)

- A **hypervisor**, also known as a virtual machine monitor, is a process that **creates and runs virtual machines** (VMs). A hypervisor **allows one host computer** to support **multiple guest VMs by virtually sharing its resources**, like memory and processing. Generally, there are two types of hypervisors. **Type 1** hypervisors, called “bare metal,” run directly on the host’s hardware. **Type 2** hypervisors, called “hosted,” run as a software layer on an operating system, like other computer programs. (VMware - Hypervisor)



VMware  
Workstation



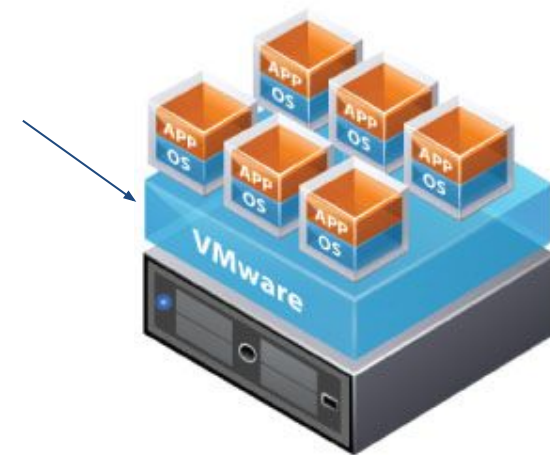
Oracle  
Virtualbox



Microsoft  
Hyper-V

Microsoft  
Hyper-V

OS & Application



Hypervisor type 2  
(VMware workstation)

## 가상화의 개념

### ■ ESXi는 하이퍼바이저 타입 1

- VM을 생성 및 실행, 관리 하기 위한 최소한의 구성(Host OS가 없음)
- 호스트 시스템에서 가상환경을 구축하기 위한 논리적 플랫폼
  - ✓ VM을 위한 저장 장치 관리
  - ✓ 다중 OS의 메모리 관리
  - ✓ 가상 네트워크 장치
  - ✓ 그 외 VM 유지보수를 위한 기능 구현



VMware  
ESXi

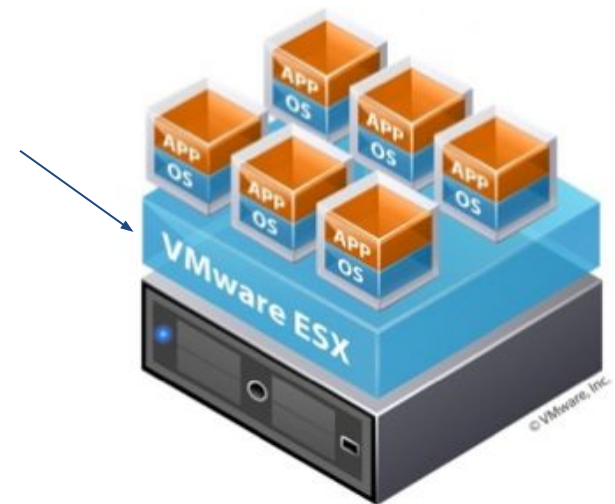


IBM  
PowerVM



Citrix  
XenServer

OS & Application을  
대체



Hypervisor type 1  
(VMware workstation)



## 사용 목적 및 기능

- 하나의 호스트로 여러 대의 **OS**를 운영하기 위함
- 새 **VM** 생성, 스냅샷, 가상 네트워크환경 등 기존의 **VMware workstation**의 기능 지원
- **VMware workstation**과 같으나 이를 설치하기 위한 별도의 **OS** 불필요
- 무엇보다도 무료로도 사용 가능!!!(성능의 제약)
  - 단일 물리 서버 활용(물리서버의 클러스터링 불가)
  - 물리 CPU 2코어 지원
  - 물리 메모리 12TB 지원
  - 최대 8개의 VM 지원
  - VM 네트워크 지원
  - vCenter를 이용한 관리 불가
  - VMware의 기술지원 불가



## VM을 구성하는 파일들

### ■ VM 구성 파일 종류 및 역할

확장자	파일 이름의 예	의미
.vmx	vmname.vmx (vmware.cfg on Linux)	VM의 기본 설정 정보
.log	vmname.log or vmware.log	메인 로그 파일
.nvram	vmname.nvram or nvram	BIOS 설정 정보
.vmdk	vmname.vmdk	현재 VM의 디스크
	vmname-s###.vmdk	사용시 증가, 용량 별 분할로 설정 시 VM의 디스크
	vmname-f###.vmdk	생성시 할당, 용량 별 분할로 설정 시 VM의 디스크
	vmname-disk-###.vmdk	스냅샷 분기시 생성되는 디스크
.vmem	uuid.vmem	VM의 paging 파일
	snapshot_name_number.vmem	스냅샷 별 메모리(구동중인 VM에 대해 스냅샷 생성 시 발생)
.vmsd	vmware.vmsd	스냅샷에 대한 정보 및 메타데이터
.vmsn	vmname.Snapshot.vmsn	스냅샷을 생성할 당시의 운영 상태 정보
	vmname.Snapshot###.vmsn	스냅샷의 상태 정보
.vmss	vmname.vmss	일시정지 된 VM의 상태



# ESXi 데이터 수집

- 처음 뵙겠습니다 ESXi
- Datastore browser로 저장 구조 확인
- SSH를 이용한 VM 확인 및 수집
- 가동중인 VM 확인 및 수집
- 그 외 수집 대상



## 처음 뵙겠습니다 ESXi

- 콘솔로 확인한 인터페이스
- Web UI 접속을 위해 할당된 IP주소를 확인

```
VMware ESXi 6.7.0 (VMKernel Release Build 8169922)
VMware, Inc. VMware Virtual Platform
2 x Intel(R) Core(TM) i7-6500U CPU @ 2.50GHz
4 GiB Memory

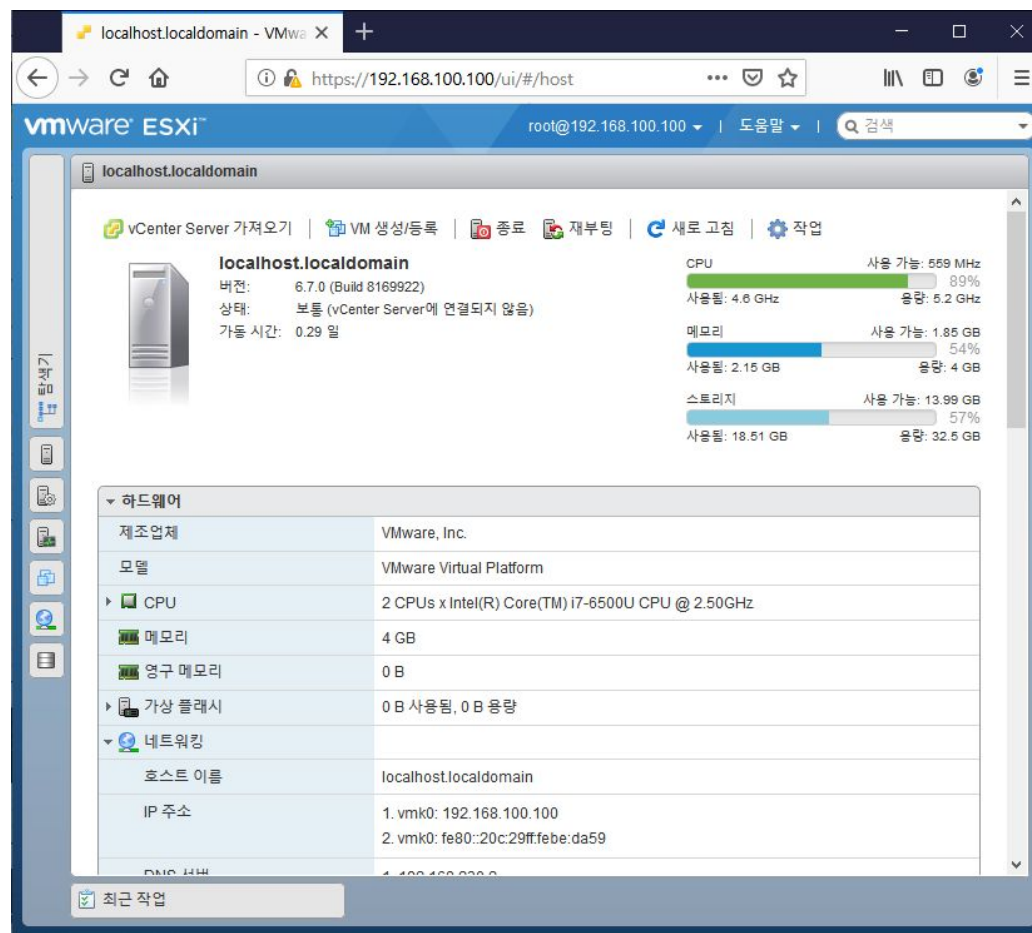
To manage this host go to:
http://192.168.100.100/ (STATIC)
http://[fe80::20c:29ff:febe:da59]/ (STATIC)

<F2> Customize System/View Logs
<F12> Shut Down/Restart
```



## 처음 뵙겠습니다 ESXi

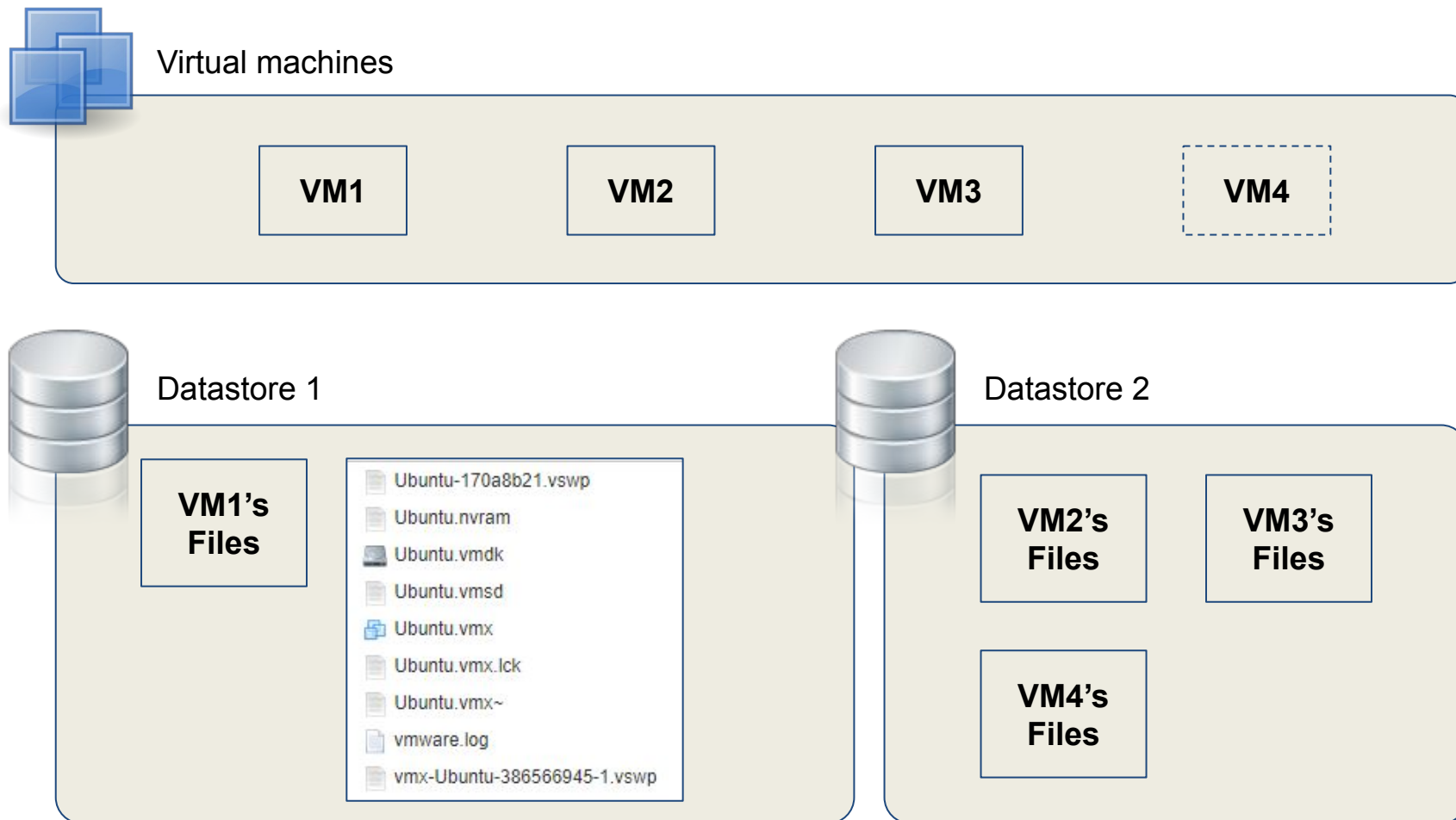
- 콘솔에서 확인한 IP로 접속
- 관리자 계정 필요
- 호스트 시스템
  - 하드웨어 사양
  - 호스트 시스템 모니터링
- VM
  - 등록(Register) VM 목록
  - 각 VM의 사양 및 설정
  - 하드웨어 연결 정보
- Datastore
  - 구성 리스트 및 가용/사용 용량
  - 저장된 파일 목록
  - 버전
- 네트워크
  - 가상 네트워크 구성 정보





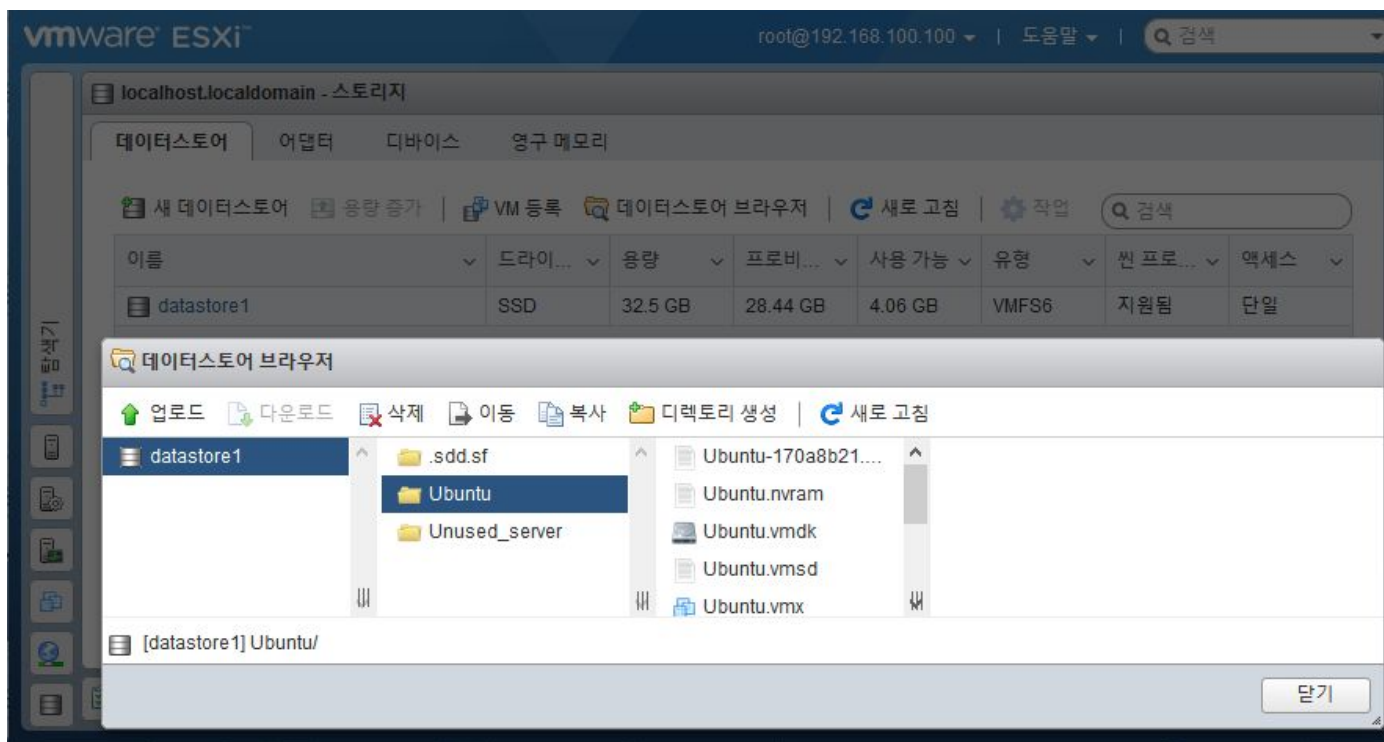
## 처음 뵙겠습니다 **ESXi**

- **ESXi의 데이터 공간 VM 구성(예시)**



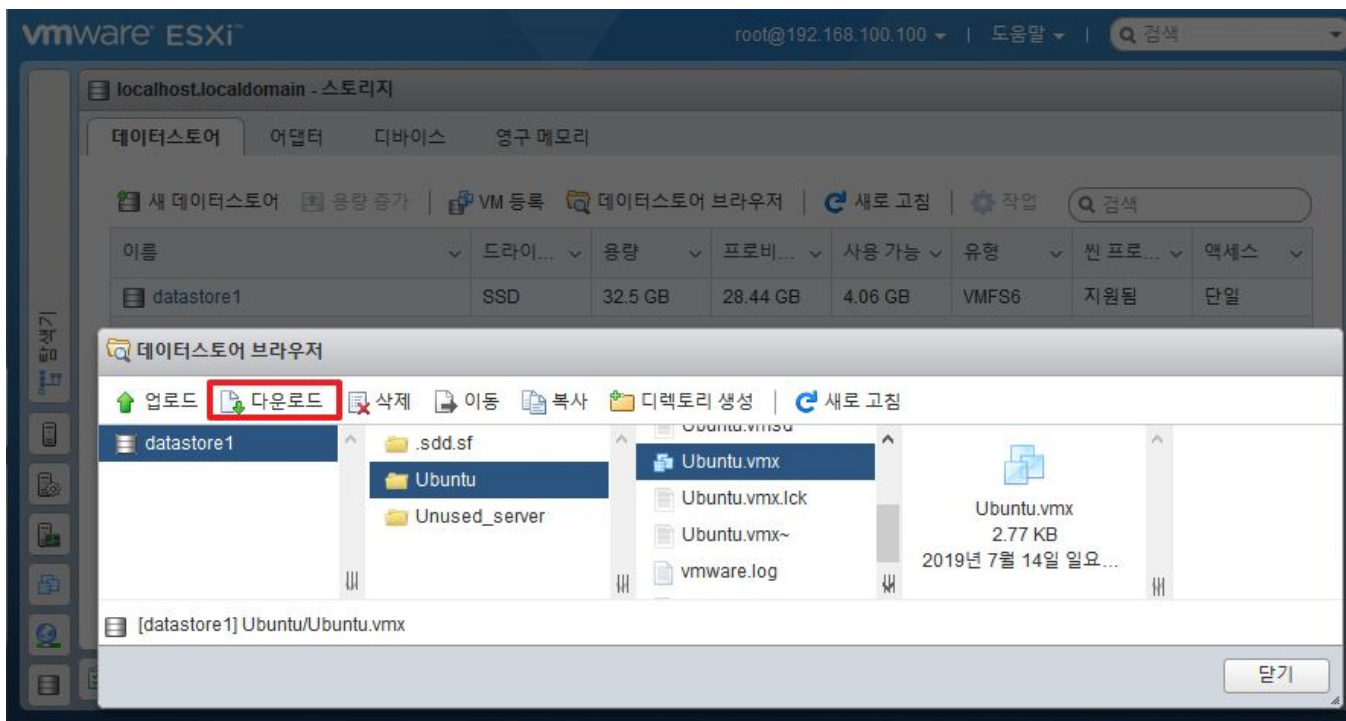
## Datastore browser로 저장 구조 확인

- UI 기능인 Datastore browser로 구성파일 저장 구조를 확인
  - VM의 구성 파일은 VM당 한 경로에 저장됨
  - 등록되지 않은 VM도 확인할 수 있으므로 VM 목록과 대조 필수
    - ✓ 등록된 VM 상태 : 운영중 or 일시정지 or 정지
    - ✓ 등록되지 않은 VM 상태 : 정지



## Datastore browser로 저장 구조 확인

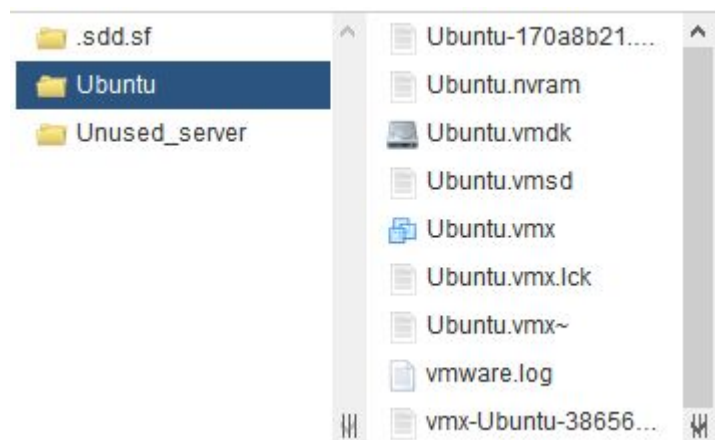
- 다운로드 기능으로 수집하면?
  - 손쉽다. 직관적이다. 만사 OK?
  - 무결성 확인이 어렵다.
  - 진행중인 VM 파일의 수집은?
  - 결정적인 문제는 보이지 않는 파일





## Datastore browser로 저장 구조 확인

- 다운로드 기능으로 수집하면?
  - <VMDK name>-flat.vmdk 파일은 Datastore에서 확인 불가
  - <VMDK name>.vmdk파일은 약 500 Byte일 뿐. 실제 데이터는 <VMDK name>-flat.vmdk 파일에 저장
  - 정상적인 수집을 위해선 SSH를 활용



```
[root@localhost:~] cd /vmfs/volumes/datastore1/Ubuntu
[root@localhost:/vmfs/volumes/5d2ae9aa-198ff681-d181-000c29beda59/Ubuntu] ls -lh
total 17939520
-rw----- 1 root root 1.0G Jul 14 10:44 Ubuntu-170a8b21.vswp
-rw----- 1 root root 16.0G Jul 15 13:26 Ubuntu-flat.vmdk
-rw----- 1 root root 8.5K Jul 15 08:46 Ubuntu.nvram
-rw----- 1 root root 500 Jul 14 10:46 Ubuntu.vmdk
-rw-r--r-- 1 root root 0 Jul 14 10:44 Ubuntu.vmsd
-rwxr-xr-x 1 root root 2.8K Jul 14 10:52 Ubuntu.vmx
-rw-r--r-- 1 root root 0 Jul 14 10:44 Ubuntu.vmx.lck
-rwxr-xr-x 1 root root 2.8K Jul 14 10:52 Ubuntu.vmx~
-rw-r--r-- 1 root root 278.6K Jul 14 15:30 vmware.log
-rw----- 1 root root 110.0M Jul 14 10:44 vmx-Ubuntu-386566945-1.vswp
[root@localhost:/vmfs/volumes/5d2ae9aa-198ff681-d181-000c29beda59/Ubuntu]
```



## SSH를 이용한 VM 확인 및 수집

- 수집 대상 파악
  - ESXi는 각 VM의 구성 파일을 을 경로로 구분하여 저장
    - ✓ /vmfs/volumes 하위에 저장
    - ✓ 모든 경로는 GUID이름으로 저장되어 있으며 부여한 Datastore 이름을 링크로 만들어 연결
  - find 명령어를 이용하여 VM 탐색
    - ✓ find /vmfs/volumes -name \*.vmx

```
[root@localhost:~] cd /vmfs/volumes
[root@localhost:/vmfs/volumes] ls -al
total 2052
drwxr-xr-x  1 root    root          512 Jul 15 08:32 .
drwxr-xr-x  1 root    root          512 Jul 14 08:38 ..
drwxr-xr-x  1 root    root           8 Jan  1 1970 5d2ae9a4-3e3ab941-d562-000c29beda59
drwxr-xr-t  1 root    root       73728 Jul 15 07:34 5d2ae9aa-198ff681-d181-000c29beda59
drwxr-xr-x  1 root    root           8 Jan  1 1970 5d2ae9ab-485a3b52-d15c-000c29beda59
lrwxr-xr-x  1 root    root           35 Jul 15 08:32 datastore1 -> 5d2ae9aa-198ff681-d181-000c29beda59
drwxr-xr-x  1 root    root           8 Jan  1 1970 ebd98f7a-8ea6590a-deae-fb0906b4df96
drwxr-xr-x  1 root    root           8 Jan  1 1970 f4c0e179-374761e6-2d36-e3a59f883ca0
[root@localhost:/vmfs/volumes] find . -name *.vmx
./5d2ae9aa-198ff681-d181-000c29beda59/Unused_server/Unused_server.vmx
./5d2ae9aa-198ff681-d181-000c29beda59/Ubuntu/Ubuntu.vmx
[root@localhost:/vmfs/volumes] █
```





## SSH를 이용한 VM 확인 및 수집

- 수집 전 해시 계산
  - md5sum을 이용하여 해시 확보

```
[root@localhost:/vmfs/volumes/5d2ae9aa-198ff681-d181-000c29beda59/Unused_server] md5sum *
a541cda674e635ffcb885ca746606c17  Unused_server-flat.vmdk
5fcd6e632c5b4587d4b74e2bd5f18951  Unused_server.nvram
4b0957adalf76633da4410d3a6ff7337  Unused_server.vmdk
d41d8cd98f00b204e9800998ecf8427e  Unused_server.vmsd
498d780f2b4dlb50399541643e76a462  Unused_server.vmx
[root@localhost:/vmfs/volumes/5d2ae9aa-198ff681-d181-000c29beda59/Unused_server] █
```



## SSH를 이용한 VM 확인 및 수집

### ▪ NFS 연결 및 전송

- esxcfg-nas를 이용하여 수집시스템의 NFS 공유 경로에 연결
- esxcfg-nas -a -o <Hostname or IPaddress> -s <Path of shared on Hostname> <Label>

### ▪ dd를 이용한 파일 복사

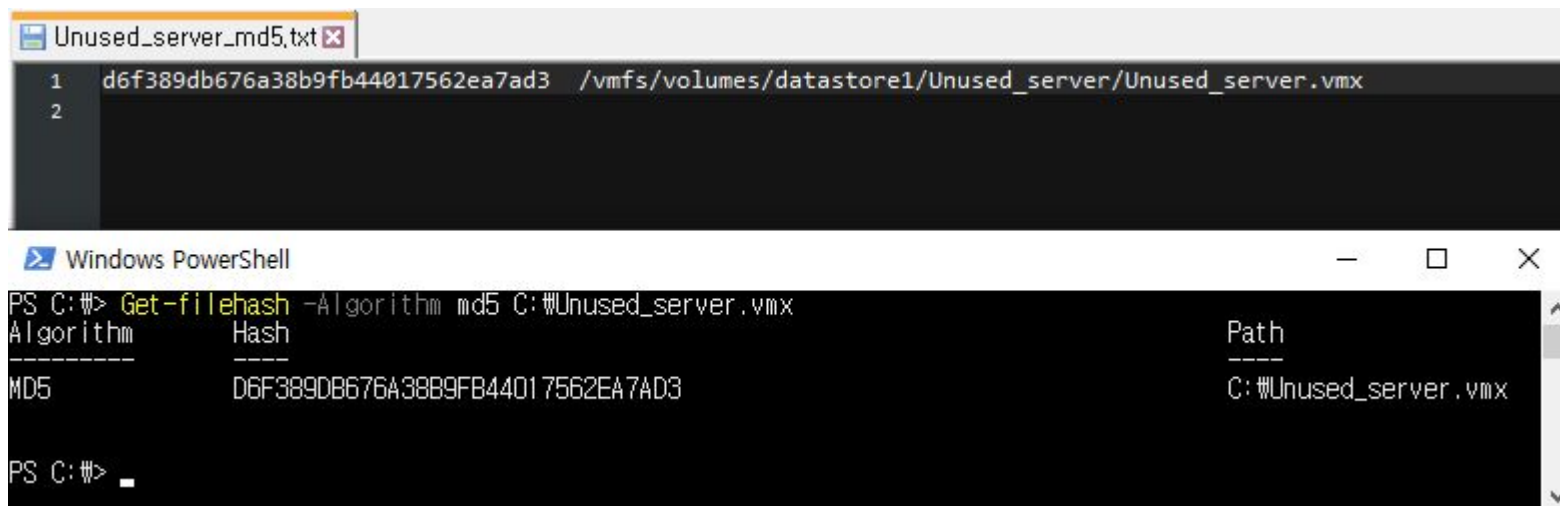
- dd if=<대상파일 경로> of=<esxcfg-nas를 통해 생성된 경로&파일이름>

```
[root@localhost:~] md5sum /vmfs/volumes/datastore1/Unused_server/Unused_server.vmx >> /vmfs/volumes/datastore1/Unused_server/Unused_server_md5.txt
[root@localhost:~] esxcfg-nas -a -o 192.168.100.200 -s /mnt/forensic forensic
Connecting to NAS volume: forensic
forensic created and connected.
[root@localhost:~] dd if=/vmfs/volumes/datastore1/Unused_server/Unused_server.vmx of=/vmfs/volumes/forensic/Unused_server.vmx bs=4096 conv=notrunc,noerror
0+1 records in
0+1 records out
[root@localhost:~] cp /vmfs/volumes/datastore1/Unused_server/Unused_server_md5.txt /vmfs/volumes/forensic/Unused_server_md5.txt
[root@localhost:~] █
```



## SSH를 이용한 VM 확인 및 수집

- 수집 결과 확인



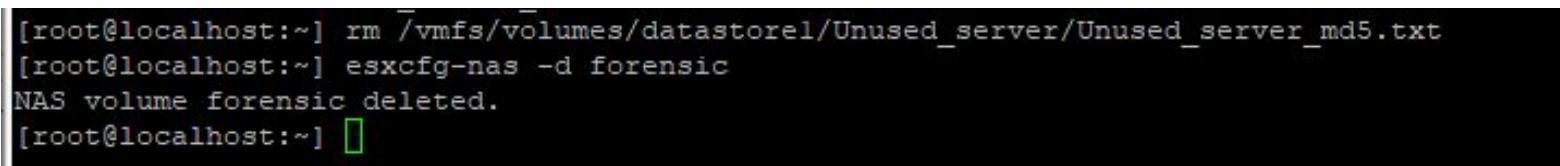
```
Unused_server_md5.txt
1 d6f389db676a38b9fb44017562ea7ad3 /vmfs/volumes/datastore1/Unused_server/Unused_server.vmx
2

Windows PowerShell
PS C:\> Get-filehash -Algorithm md5 C:\Unused_server.vmx
Algorithm      Hash
-----
MD5            D6F389DB676A38B9FB44017562EA7AD3
Path
C:\Unused_server.vmx

PS C:\> _
```

- NFS 설정 제거

- esxcfg-nas -d <Label>



```
[root@localhost:~] rm /vmfs/volumes/datastore1/Unused_server/Unused_server_md5.txt
[root@localhost:~] esxcfg-nas -d forensic
NAS volume forensic deleted.
[root@localhost:~]
```



## SSH를 이용한 VM 확인 및 수집

### ■ SFTP를 이용한 전송

- SFTP를 이용하면 NFS Server 없이 사용 가능.
- 단, md5sum 등의 기능은 사용 할 수 없으므로 SSH 콘솔을 별도로 연결하여 동작하여야 함

```
C:\>mkdir forensic
C:\>cd forensic
C:\forensic>sftp root@192.168.100.100
Password:
Connected to root@192.168.100.100.
sftp> ls /vmfs/volumes/datastore1/Unused_server/Unused_server.vmx
/vmfs/volumes/datastore1/Unused_server/Unused_server.vmx
sftp> get /vmfs/volumes/datastore1/Unused_server/Unused_server.vmx
Fetching /vmfs/volumes/datastore1/Unused_server/Unused_server.vmx to Unused_server.vmx
/vmfs/volumes/datastore1/Unused_server/Unused_server.vmx 100% 3100 609.2KB/s 00:00
sftp> exit
C:\forensic>dir
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: A2F2-B3DD

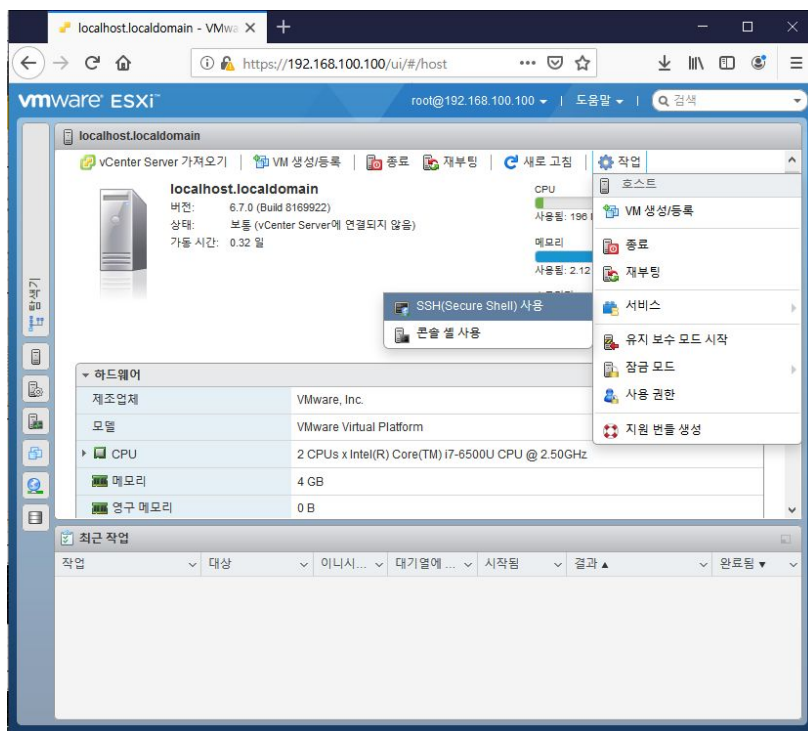
C:\forensic 디렉터리

2019-07-16 오전 01:26 <DIR> .
2019-07-16 오전 01:26 <DIR> ..
2019-07-16 오전 01:26 3,100 Unused_server.vmx
                1개 파일      3,100 바이트
                2개 디렉터리 86,854,656,000 바이트 남음

C:\forensic>
```

## 가동중인 VM 확인 및 수집

- SSH 기능 활성화 후 esxcli를 이용하여 조작
  - esxcli는 ESXi 서버를 관리하기 위한 명령어 Set
  - SSH 접속 후 CLI로 사용
  - Syntax : esxcli [dispatcher options] <namespace> [<namespace> ...] <cmd> [cmd options]



```
[root@localhost:~] esxcli
Usage: esxcli [options] {namespace}+ {cmd} [cmd options]

Options:
--formatter=FORMATTER
    Override the formatter to use for a given command.
    Available formatter: keyvalue, xml, csv
--debug
    Enable debug or internal use options
--version
    Display version information for the script
-?, --help
    Display usage information for the script

Available Namespaces:
device      Device manager commands
esxcli      Commands that operate on the esxcli system itself
            allowing users to get additional information.
fcoe        VMware FCOE commands.
graphics    VMware graphics commands.
hardware    VMKernel hardware properties and commands for configuring
            hardware.
iscsi       VMware iSCSI commands.
network     Operations that pertain to the maintenance of networking
            on an ESX host. This includes a wide variety of commands
            to manipulate virtual networking components (vswitch,
            portgroup, etc) as well as local host IP, DNS and general
            host networking settings.
nvme        VMware NVMe driver esxcli extensions
rdma        Operations that pertain to remote direct memory access
            (RDMA) protocol stack on an ESX host.
sched       VMKernel system properties and commands for configuring
            scheduling related functionality.
software    Manage the ESXi software image and packages
storage     VMware storage commands.
system      VMKernel system properties and commands for configuring
            properties of the kernel core system and related system
            services.
vm          A small number of operations that allow a user to Control
            Virtual Machine operations.
vsan        VMware vSAN commands

[root@localhost:~] █
```



## 가동중인 VM 확인 및 수집

### ■ 운영중인 VM 확인

#### • esxcli vm process list

<input type="checkbox"/>	가상 시스템 ▲	상태 ▾	사용된 공간 ▾	게스트 운영 체제 ▾	호스트 이름 ▾	호스트 ... ▾	호스트 ... ▾
<input type="checkbox"/>	Ubuntu	✓...	17.11 GB	Ubuntu Linux(64...	localhost.locald...	96 MHz	1.03 GB
<input type="checkbox"/>	Unused_server	✓...	8 GB	Ubuntu Linux(64...	알 수 없음	0 MHz	0 MB

빠른 필터... ▾ 2 항목

```
[root@localhost:~] esxcli vm process list
Ubuntu
World ID: 2100220
Process ID: 0
VMX Cartel ID: 2100219
UUID: 56 4d 05 d4 9f f1 11 e8-e5 7d 22 6e 6f 05 38 e6
Display Name: Ubuntu
Config File: /vmfs/volumes/5d2ae9aa-198ff681-d181-000c29beda59/Ubuntu/Ubuntu.vmx
[root@localhost:~]
```

#### • vim-cmd vmsvc/getallvms

```
[root@localhost:~] vim-cmd vmsvc/getallvms
Vmid      Name                File                                Guest OS      Version  Annotation
1         Ubuntu              [datastore1] Ubuntu/Ubuntu.vmx      ubuntu64Guest vmx-14
2         Unused_server        [datastore1] Unused_server/Unused_server.vmx  ubuntu64Guest vmx-14
[root@localhost:~]
```





## 가동중인 VM 확인 및 수집

### ■ 스냅샷 생성 및 확인

- 스냅샷 생성 : `vim-cmd vmsvc/snapshot.create <Vmid> <Label>`

```
[root@localhost:~] vim-cmd vmsvc/getallvms
```

Vmid	Name	File	Guest OS	Version	Annotation
1	Ubuntu	[datastore1] Ubuntu/Ubuntu.vmx	ubuntu64Guest	vmx-14	
2	Unused_server	[datastore1] Unused_server/Unused_server.vmx	ubuntu64Guest	vmx-14	

```
[root@localhost:~] vim-cmd vmsvc/snapshot.create 1 snapshot_for_collection
```

Create Snapshot:

```
[root@localhost:~]
```

- 생성된 스냅샷 확인 : `vim-cmd vmsvc/snapshot.get <Vmid>`

```
[root@localhost:~] vim-cmd vmsvc/snapshot.get 1
```

Get Snapshot:

```
|--ROOT
--Snapshot Name      : snapshot_for_collection
--Snapshot Id        : 1
--Snapshot Description :
--Snapshot Created On : 7/15/2019 16:47:9
--Snapshot State     : powered off
[root@localhost:~]
```



## 가동중인 VM 확인 및 수집

- 사용중인 VM은 스냅샷 기능을 이용하여 수집
- vim-cmd를 이용하여 스냅샷 생성 및 제거
- 생성된 스냅샷은 앞의 “SSH를 이용한 수집” 으로 수집
- 스냅샷으로 생성된 VM수집

확장자	파일 이름의 예	의미
.vmx	vmname.vmx(vmware.cfg on Linux)	VM의 기본 설정 정보
.log	vmname.log or vmware.log	메인 로그 파일
.nvram	vmname.nvram or nvram	BIOS 설정 정보
.vmdk	vmname-f###.vmdk	생성시 할당, 용량 별 분할로 설정 시 VM의 디스크
	vmname-disk-###.vmdk	스냅샷 분기시 생성되는 디스크
.vmem	uuid.vmem	VM의 paging 파일
	snapshot_name_number.vmem	스냅샷 별 메모리(구동중인 VM에 대해 스냅샷 생성 시 발생)
.vmsd	vmware.vmsd	스냅샷에 대한 정보 및 메타데이터
.vmsn	vmname.Snapshot.vmsn	스냅샷을 생성할 당시의 운영 상태 정보
	vmname.Snapshot###.vmsn	스냅샷의 상태 정보





## 가동중인 VM 확인 및 수집

- 수집이 완료된 스냅샷 제거

- `vim-cmd vmsvc/snapshot.remove <Vmid> <Snapshot Id>`

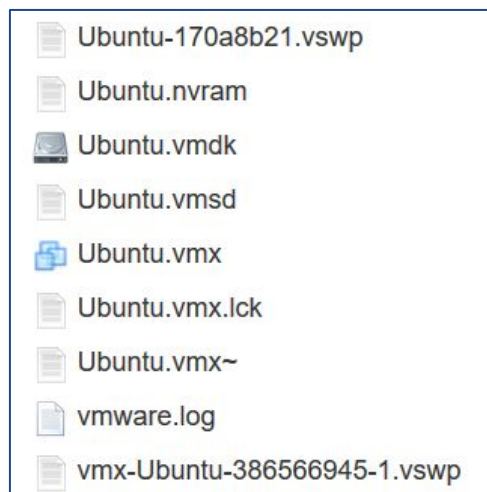
```
[root@localhost:~] vim-cmd vmsvc/snapshot.create 1 snapshot_for_collection
Create Snapshot:
[root@localhost:~] vim-cmd vmsvc/snapshot.get 1
Get Snapshot:
|-ROOT
--Snapshot Name      : snapshot_for_collection
--Snapshot Id       : 2
--Snapshot Description :
--Snapshot Created On  : 7/16/2019 2:36:15
--Snapshot State      : powered off
[root@localhost:~] vim-cmd vmsvc/snapshot.remove 1 2
Remove Snapshot:
[root@localhost:~]
```



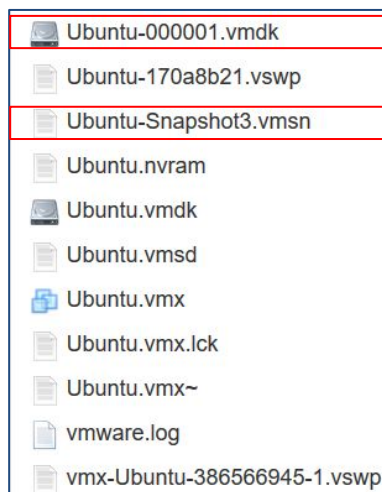
## 가동중인 VM 확인 및 수집

### ■ 스냅샷 생성 및 삭제에 따른 파일 변화

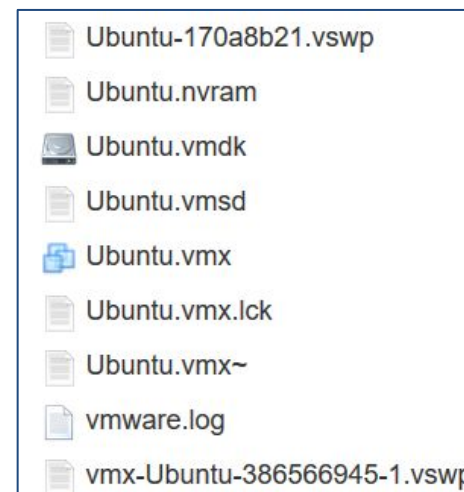
- <vmname>-#####.vmdk : 스냅샷 생성 후 변경상태 저장
- <vmname>-Snapshot#.vmsn : 스냅샷의 상태 정보
  - ✓ 반드시 <vmname>-Snapshot#.vmdk의 숫자와 일치 하는 것은 아님
  - ✓ 수집 시점 이전 정보를 획득하기 위해 수집을 위해 생성한 스냅샷 정보를 제외한 모든 파일을 수집



스냅샷 생성 전



스냅샷 생성 후



스냅샷 삭제 후



## 그 외 수집 대상

### ▪ RDM Storage

- 물리적인 저장장치(디스크)를 Datastore로 사용하지 않고 VM에 바로 연결되도록 매핑
- RDM의 결과로 VMDK파일이 생성되지만 실제 데이터는 디스크에 저장
- .VMDK의 “Extent description”에서 VMFSRDM 옵션을 확인

```
# Disk DescriptorFile
version=1
encoding="UTF-8"
CID=fffffffe
parentCID=fffffffe
isNativeSnapshot="no"
createType="vmfsPassthroughRawDeviceMap"
```

```
# Extent description
RW 7814037168 VMFSRDM "localrdm1-rdmp.vmdk"
```

```
# Extent description
RW 268435456 VMFS "mgmt_0-flat.vmdk"
```

```
# The Disk Data Base
#DDB
```

```
ddb.adapterType = "lsilogic"
ddb.geometry.cylinders = "486401"
ddb.geometry.heads = "255"
ddb.geometry.sectors = "63"
ddb.longContentID = "e104cd9dbb723eed933de7efffffffffe"
ddb.uuid = "60 00 C2 93 48 6a 50 1d-30 98 60 54 22 bf 95 91"
ddb.virtualHWVersion = "13"
```



## 그 외 수집 대상

### ▪ RDM Storage

- vmkfstools -q 명령어를 이용하여 매핑된 원본 디스크를 확인 후 dd 명령어를 이용하여 수집

RDM 생성 및  
생성 결과 확인

```
[root@esxi:~] ls /vmfs/devices/disks/t10.ATA_____ST4000DM0002D1F2168_____
Z307KQ0Z
/vmfs/devices/disks/t10.ATA_____ST4000DM0002D1F2168_____Z30
7KQ0Z
[root@esxi:~] vmkfstools -z /vmfs/devices/disks/t10.ATA_____ST4000DM0002D1F2168_____
Z307KQ0Z /vmfs/volumes/ds1/RDM/localrdm1.vmdk
```

수집 대상  
디스크 식별

```
[root@esxi:~] ls /vmfs/volumes/ds1/RDM
localrdm1-rdmp.vmdk localrdm1.vmdk
[root@esxi:~]
[root@esxi:~] vmkfstools -q /vmfs/volumes/ds1/RDM/localrdm1.vmdk
Disk /vmfs/volumes/ds1/RDM/localrdm1.vmdk is a Passthrough Raw Device Mapping
Maps to: vml.0100000000202020202020202020202020205a3330374b51305a535434303030
[root@esxi:~] ls -l /vmfs/devices/disks | grep vml.0100000000202020202020202020202020205a3
330374b51305a535434303030
lrwxrwxrwx 1 root root 73 Jul 16 16:26 vml.0100000000202020202020202020202020205a3330374b51305a535434303030 -> t10.ATA_____ST4000DM0002D1F2168_____
Z307KQ0Z
```

NFS & DD로  
수집

```
[root@esxi:~] esxcfg-nas -a -o 192.168.0.251 -s /mnt/forensic forensic
Connecting to NAS volume: forensic
forensic created and connected.
[root@esxi:~] dd if=/vmfs/devices/disks/t10.ATA_____ST4000DM0002D1F2168_____
Z307KQ0Z of=/vmfs/volumes/forensic/localrdm1.dd bs=4096 conv=notrunc,no
error
```



## 그 외 수집 대상

### ▪ USB 스토리지

- 호스트 서버에 물리적으로 연결된 USB 장치
- VMFS가 아닌 일반적인 파일시스템
- 명령어 “lsusb”를 이용하여 연결된 USB 장치 확인 후 저장장치를 식별하여 추가 수집

```
[root@esxi:~] lsusb
Bus 004 Device 002: ID 152d:0567 JMicron Technology Corp. / JMicron USA Technology Corp.
Bus 006 Device 001: ID 0e0f:8002 VMware, Inc.
Bus 005 Device 001: ID 0e0f:8001 VMware, Inc.
Bus 004 Device 001: ID 0e0f:8002 VMware, Inc.
Bus 003 Device 001: ID 0e0f:8001 VMware, Inc.
Bus 002 Device 001: ID 0e0f:8002 VMware, Inc.
Bus 001 Device 001: ID 0e0f:8001 VMware, Inc.
[root@esxi:~]
```

# VMDK 분석 방법



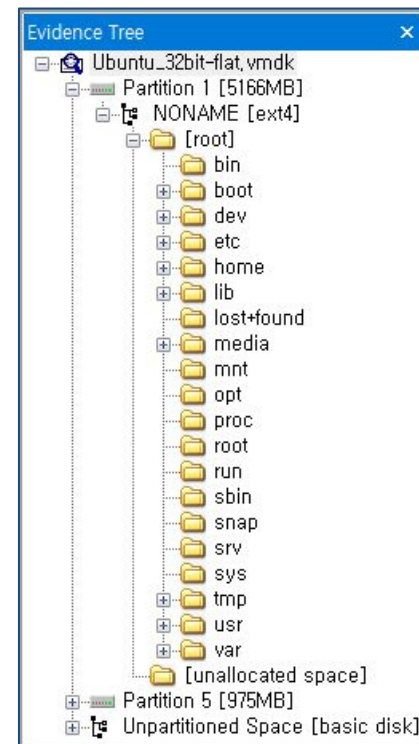
## VMDK 분석

### ■ 용량이 확정된 VMDK

- RAW 이미지와 동일
- 일반적인 이미지 처리 도구 활용

Location	[Ubuntu_32bit] Ubuntu_32bit/	Browse...
Disk Provisioning	<input type="radio"/> Thin provisioned <input checked="" type="radio"/> Thick provisioned, lazily zeroed <input type="radio"/> Thick provisioned, eagerly zeroed	
Shares	Normal	1000
Limit - IOPs	Unlimited	
Controller location	SCSI controller 0	SCSI (0:1)
Disk mode	Dependent	
Sharing	None	

Disk sharing is only possible with eagerly zeroed, thick provisioned disks.





## VMDK 변환

### ■ 사용량에 따라 용량이 증가하는 VMDK

- 가상디스크의 사용량에 따라 VMDK 파일의 용량 증가
- Qemu를 이용하여 일반 RAW포맷으로 변경 후 분석
- `qemu-img.exe convert -f vmdk -O raw <vmdk_path> <output raw_path>`

```
Windows PowerShell
PS C:\Users\keyma\Downloads\qemu-img-win-x64-2.3.0> .\qemu-img.exe convert -f vmdk -O
raw .\VM_Storage_0x01_Init.vmdk .\VM_Storage_0x01_Init.raw
PS C:\Users\keyma\Downloads\qemu-img-win-x64-2.3.0> ls VM_Storage_0x01_Init*

디렉터리: C:\Users\keyma\Downloads\qemu-img-win-x64-2.3.0

Mode                LastWriteTime         Length Name
----                -
-a-----         2019-01-21 오후 9:22    10737418240 VM_Storage_0x01_Init.raw
-a-----         2019-01-01 오후 8:02         14811136 VM_Storage_0x01_Init.vmdk

PS C:\Users\keyma\Downloads\qemu-img-win-x64-2.3.0>
```

qemu-img.exe 를 이용한 VMDK to RAW 변환  
vmdk(14.1 MB) -> raw(10.0 GB)





- **VMware Hands-on Labs - HOL - 1810-01-SDC\_KO**
  - [http://docs.hol.vmware.com/HOL-2017/Localization/manuals/hol-1810-01-sdc\\_ko\\_html\\_en/](http://docs.hol.vmware.com/HOL-2017/Localization/manuals/hol-1810-01-sdc_ko_html_en/)
- **How To - Digital Forensic Imaging In VMware ESXi**
  - <https://digital-forensics.sans.org/blog/2010/10/04/digital-forensic-imaging-vmware-esxi>
- **Virtual Machine Files**
  - <https://pubs.vmware.com/workstation-9/index.jsp?topic=%2Fcom.vmware.ws.using.doc%2FGUID-A968EF50-BA25-450A-9D1F-F8A9DEE640E7.html>
- **Create snapshots via commandline in ESXi 5.5**
  - <https://www.bytebang.at/Blog/Create+snapshots+via+commandline+in+ESXi+5.5>
- **vSphere CLI Online Documentation**
  - <https://code.vmware.com/docs/1499/vsphere-cli>
- **Converting between image formats**
  - <https://docs.openstack.org/image-guide/convert-images.html>

