APU Forensics Fieldkit



Getting Started: System Requirements



Windows 10 configuration tends to "drift" away from stability over time with continuous updates

- This can cause subtle problems for apps problems you may not notice until something won't start
- It may seem like a problem with the app, *but it is not* it is a problem with Windows!
- Fixing these problems requires a command line interface there is no other way to get this done



Fixing Windows

We have to run two apps from the Windows command line:

- a) dism checks Windoze Update to make sure everything is correct (so it needs a network connection)
- b) sfc uses the files maintained by dism to fix configuration issues in the running system

These both require Administrator Privileges



- Start Menu
- Windows System
- Command Prompt
- Right Click -> More
- Run as Administrator

Be Patient: these will take a few minutes, but let each command finish to 100%. There may be some pauses in progress, this is normal.

dism /Online /Cleanup-Image /RestoreHealth
 wait for dism to finish before running sfc

sfc /scannow

if sfc reports that it fixed errors, run it again (it can take up to 3 runs to make it happy)

when sfc reports no errors, shut down and restart

Run as Administrator



Administrator: Command Prompt	-	×
:\WINDOWS\system32>DISM.exe /Online /Cleanup-image /Restorehealth		
Deployment Image Servicing and Management tool Version: 10.0.19041.844		
Image Version: 10.0.19041.1052		
=======] The restore operation completed successfully The operation completed successfully.	•	
C:\WINDOWS\system32>sfc /scannow		
Beginning system scan. This process will take some time.		
Beginning verification phase of system scan. Verification 100% complete.		
Vindows Resource Protection found corrupt files and successfully repaired them. For online repairs, details are included in the CBS log file located at windir\Logs\CBS\CBS.log. For example C:\Windows\Logs\CBS\CBS.log. For offline repairs, details are included in the log file provided by the /OFFLOGFILE flag.		
:\WINDOWS\system32>sfc /scannow		
Beginning system scan. This process will take some time.		
Beginning verification phase of system scan. Verification 100% complete.		
Vindows Resource Protection did not find any integrity violations.		
C:\WINDOWS\system32>		







- The Basic Input Output System (BIOS) is code on a chip on the system motherboard.
- When the system is powered on the BIOS is the first software that runs. It identifies the hardware, configures it, tests it, and connects it to the operating system for further instruction.
 - This is called the boot process.

[Video] what is bios https://support.lenovo.com/videos/VID100790



- Entering the BIOS setup utility allows you to change the boot process order as well as a variety of CPU settings.
- Unified Extensible Firmware Interface (UEFI) is similar to BIOS, but has some advantages.
 - It can boot from USB disks, has a graphical user interface with network capability, and is backward and forward compatible.
- Over time, UEFI is expected to replace direct access to the BIOS.



- Hardware support for virtualization (Intel VT-x or AMD-v) is always required to run 64bit VMs, and any VM that uses more than one CPU core.
 - Virtualbox versions 5 and 6.0 (July 2020) can run 32-bit
 VMs with software virtualization on *almost* all hosts (no
 VT-x or AMD-V setting in the BIOS is required)
 - MyTyVM is one of the last 32-bit single-core VM Guest operating systems
- Start Menu Windows Admin Tools System Info
- at the bottom
 - Hyper-V Virtualization Enabled in Firmware: Yes
 Ready to go



Start Menu - Windows Admin Tools - System Info

• at the bottom

Hyper-V - Virtualization Enabled in Firmware: No

- You need to enable hardware support for virtualization in the host system BIOS.
- Note your exact system model, then check how to get into the BIOS settings at boot time.
- Once you get there you need to track down the setting, which is buried in a menu
 - There are examples at the end of this document







Getting Started: 3) Install Virtualbox

VirtualBox 6.1.20 (released 20 April 2021)

- VMM: Fixed guest OS hanging under certain circumstances when Hyper-V is present
- The current version is recommended for download
- Comes in two parts because of copyright
 - Platform Pack (main application) (Required)
 - Extension Pack (licensed) (Optional)

BE SURE to Right-Click and Run As Administrator when you install

Virtualbox works best from the default location – C:\Program Files (You can put the VMs anywhere)



Download the Base.iso from <u>http://my-tiny.net</u> and follow the pdf or the video

Virtualbox 6 has a slightly different icon layout than the version 5 interface in the videos, but it is not a problem.



Where to put the VMs



File > Preferences

General	General	
Input	Default Machine Folder: D:\VMnovtx]	
🗃 Update	VRDP Authentication Library: VBoxAuth	8
Janguage		
Display		
Network		
Extensions		
Extensions Proxy		

- You can store your VMs anywhere by setting the Default Machine Folder
- But Remember: Windoze may change drive letters for removable drives

Exit Virtualbox after [OK] to be certain the setting is properly saved

TinyNet: linux 2.6/3x/4x/ (32-bit)



- When creating a VM, make sure you choose the proper version of the guest OS template
- Choosing the correct template allows virtualbox to select the correct settings for other processor features - it's not just about 64bit capability any more.

Name	and operation	ng system		
Please d type of o be used	noose a descriptiv operating system throughout Virtuz	ve name for the new virt you intend to install on i alBox to identify this mad	ual machine and t. The name you hine.	d select the u choose v
Name:	ToClone			
Type:	Linux			•
Version:	Linux 2.6 / 3.x /	/ 4.x (32-bit)		•

If the VM freezes, Disable Hyper-V



File Machine Help	
Tools	New Settings Discard Show
ToClone	🔯 ToClone [Running] - Oracle VM VirtualBox — 🗆 X 📃 Preview
2.6 🗘 Running	File Machine View Input Devices Help
There are certain combinations of Win10 versions and processors (especially Intel CPUs) where Hyper-V and Win10 "features" that depend on it	Loading /boot/umlinuz Loading /boot/initrd.img ready. early console in extract_kernel input_len: 0x004bf875 output: 0x01000000 output: 0x01000000 output: 0x00c47dd0 kernel_total_size: 0x00d2e000 Physical KASLR using RDTSC Decompressing Linux Parsing ELF Performing relocations done. Booting the kernel.
must be disabled	🖸 💿 📜 🗗 🖉 💭 🛄 💾 💟 🏈 🖬 Right Ctrl 🚊
before quest	USB Controller: OHCI Device Filters: 0 (0 active)
	Shared folders
systems can run.	None
	None





- Start menu
- Windows Sytem
- Control Panel
- Programs and Features
- Turn Features on or off

ALL Hyper-V settings OFF





Running VMs on a laptop:

Check your power settings – close lid, low battery, etc. Never Hibernate, only Sleep

("Hibernate" suspends too many host processes, and your VM will get corrupted – "Sleep" works well enough)

(or ... just make sure you ALWAYS poweroff the VM)

Logging in









Keep pressing the key 2 times per second until the BIOS Menu is displayed



System & Network Administration

BIOS Setup Utility	Startup Interrupt Menu
HEWLETT-PACKARD COMPUTER SETUP File Storage Security ower Advanced Setup Password Power-On Password Powe	Press one of the following keys to continue ESC to resume normal startup F1 to enter the BIOS Setup Utility F10 to diagnose hardware F11 to recover your system F12 to choose a temporary startup device Press ENTER to pause ThinkPad T480s (2017,2018) Main Config Date/Time Security Startup Restart
HEMLETT-PACKARD COMPUTER SETUP File Storage Security Power Advanced Setup Password Power-On Password Pas System Security Dev Dev Dev Virtualization Technology (VTx) Disabled Intei(R) VT-U Disabled System Security F10=Accept, ESC=Cancel	UEFI BIOS VersionN22ET33WUEFI BIOS Date (Year-Month-Day)2018-02-28Embedded Controller VersionN22ET33WME Firmware VersionX.X.XMachine Type Model20L7System-unit serial numberPF123System board serial numberWitKS6123Asset TagNo Asset InformationCPU TypeIntel(R) Core(TM) ix-xx00U CPUCPU Speed2.x00GHzInstalled memoryXxxX MBUUDe23b804c-36a8-11b2-a85c-1MAC Address (Internal LAN)54 XX 75 XX 31 XXUEFI Secure BootOnOA2Yes
Master Boot Record Security	Menus and keys are different for every make and model
Name and location of Virtualization Settings is different for every make and model	F1 Help 11 Select item 1/4 Change Values F9 Setup Defaults Esc Exit 1/4 Select Menu Enter Select > Sub-Menu F10 Save and Exit Contributed by Zongquan, VK.0, 2018/03/29 Select > Sub-Menu F10 Save and Exit

System & Network Administration

The option *should be called something like*

- Virtualization
- Intel VT-x
- \circ AMD V
- Secure Virtual Mode
- SVM Mode

The option is usually in

- Security
- Configuration
- \circ Advanced



Advanced	enovo BTOS Setu
CPU Setup	
EIST Support Intel(R) Hyper-Threading Technology	[Enabled] [Enabled]
Core Multi-Processing	[Enabled]
UT-d	[Enabled]
TxT	[Disabled]
C1E Support	[Enabled]
C State Support	[C1C3C6C7C8]
Turbo Mode	[Enabled]

Info. Action Configuration	Secur i ty	Boot Exit		
System Time		[11:14:37]		
/stem Date		[03/04/2020]		
Wireless LAN		[Enabled]		
Intel Virtual Technology		[Enabled]		
BIOS Back Flash		[Disabled]		
Hotkey Mode		[Enabled]		
Always On USB		[Enabled]		
Workload Hint	[Intelligent [Disabled]			
		Security		
	U	irtualization		

Enabled

AMD U(TH) Technology

Odunned Processor Cartingentin	Ténus Prov	wifis Hala	Advanced		AMD	Processor
CPU Mismatch Detection: [F Core Multi-Processing: [F Processor Power Management: [F	Enabled] When enable Enabled] (Virtual Ma Disabled] Monitor) c	led, a UMM Module Achine AGESA U	figuration Version: 13.58 ersion: 3.5.3.1		Enab Secu Mode	le/Disabl re Virtua (SVM)
tel(R) Virtualization Technology [] cecute Disable Bit: Ijacent Cache Line Prefetch: [] irdware Prefetch: [] irect Cache Access [] et Max Ext CPUID = 3 []	Enabled] the additi Enabled] the additi Enabled] capabilitie by Vanderpp Disabled] Technology Disabled] If this op changed, a sequence w Disabled] applied on boot. boot.	ional hardware ies provided pool J. ption is a Power Off-On will be n the next GART Er Microco	Ilon(tm) II X4 640 Proces m: C3 1: 512KB 2: 2048KB 3: N/A : 3000MHz, NB C1 uency : 1000MHz Change Freq. : Yes tatch Level : 0x10000 Fror Reporting de Updation	Options isabled habled DAF Disabled] (Enabled]	↔ †1 +- F1	Select S Select I Change O General
Info 14 Select Item -/+ Char c Exit + Select Menu Enter Sele	nge Values - F9 Setu ect ⊨ Sub-Menu - F10 Save	tup Defaults Cool'n'	Virtual Nachine Node Quiet	[Enabled]	F10 ESC	Save and Exit
Setup Confirm	nation		CM02 Setup Utilitu	Commight (C)	004 2	000
Save configuration chang	res and exit now?		cmus setup utility	Advanced BIOS Fe	ature:	909 Awar s
HEWLETT-PAU Cunity Power Advanced Setup Password Sower-On Password Oevice JSB Se Slot S Networ System Intel TXT(LT) Supp	tem Security evention chnology (VTx) D	TUP TUP TUP X Su X On In Vi AM Vi AM Vi AM Vi AM Vi Se Th Pa Inabled Isabled Vi Aw Ba	ternal Graphics Mode A Frame Buffer Size rround View board VGA output con it Display First rtualization D K8 Cool&Quiet cont rd Disk Boot Priorit rst Boot Device cond Boot Device ird Boot Device ssword Check D S.M.A.R.T. Capabil ay Mode ckup BIOS Image to H	[Disabled] 128MB Disabled mect D-SUB/DVI [PEG] [Enabled] rol [Auto] y [Press Enter] [Hard Disk] [USB-HDD] [CDROM] [Setup] lity [Enabled] [Disabled] HDD [Enabled]		Me Ha Vi Te im Sy Vi So Vi a l on si
Master System Security	— F10=Accept, ESC	C=Cance1 "Vir is	tual Directed I/0 s a different thir	O" (Intel VT- <mark>d</mark> / ng, the default	/AM[is C	D- <mark>V</mark> i) 9K

S I O

System & Network Administration





BIOS Settings

- A full restart from power off is best after saving BIOS changes
- just rebooting or resuming may not do the job.





Access the BIOS from Windows



