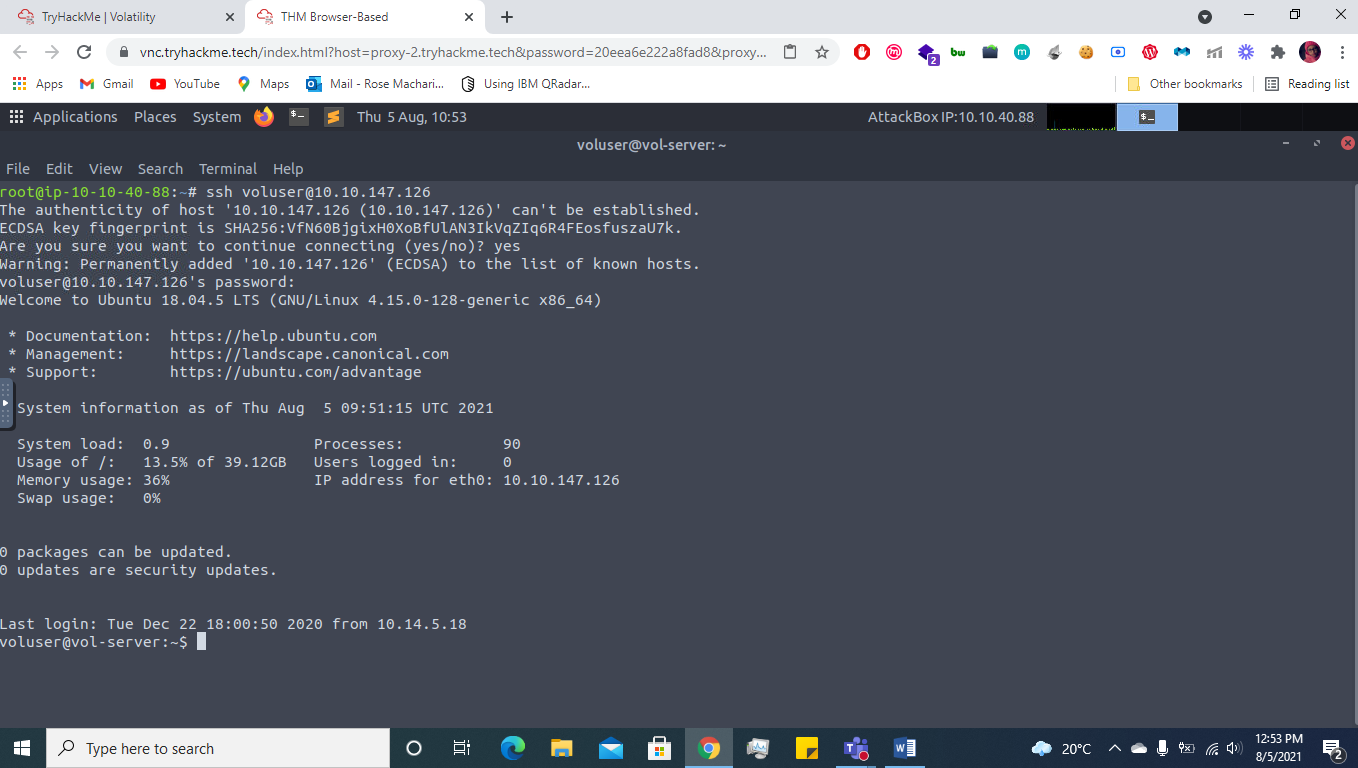
**Volatility room**

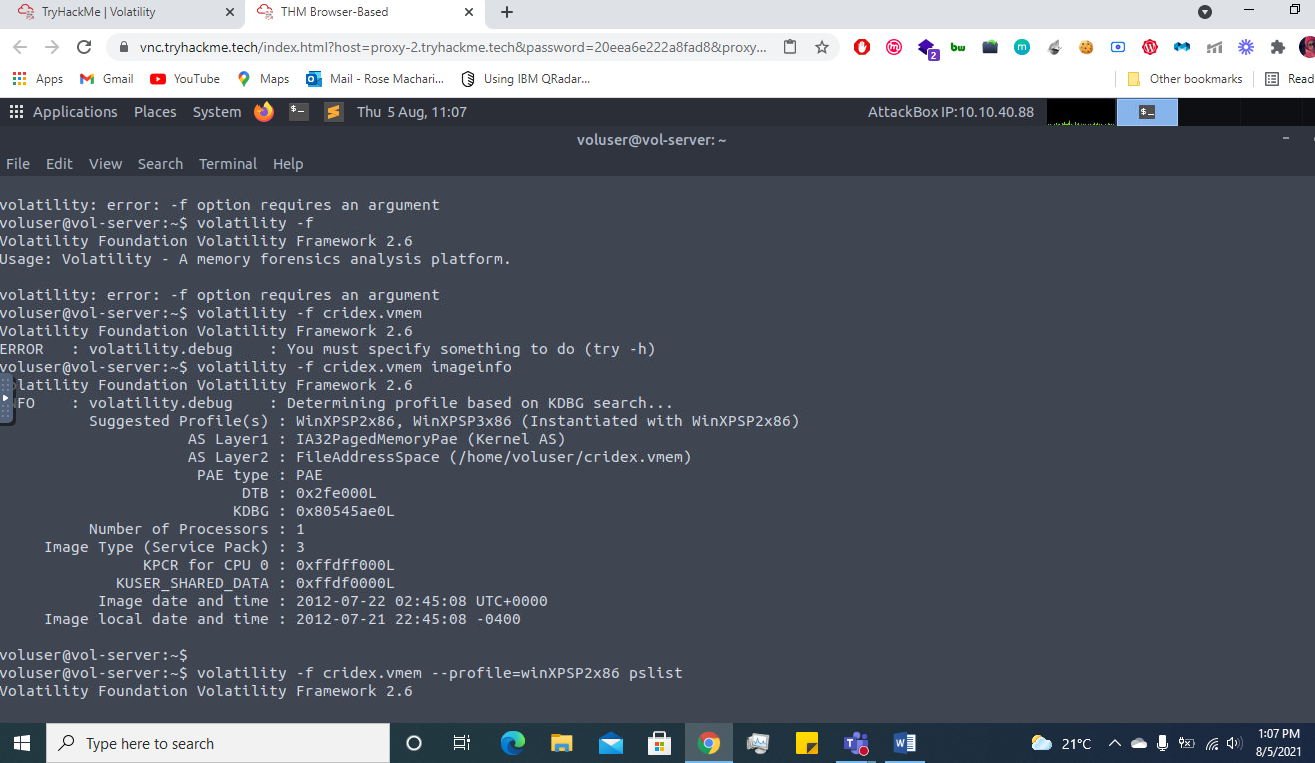
1. What memory format is the most common? .Raw
2. The Window's system we're looking to perform memory forensics on was turned off by mistake. What file contains a compressed memory image? hiberfil.sys
3. How about if we wanted to perform memory forensics on a VMware-based virtual machine? .vmem

Install Volatility onto your workstation of choice or use the provided virtual machine. On Debian-based systems such as Kali this can be done via `apt-get install volatility`



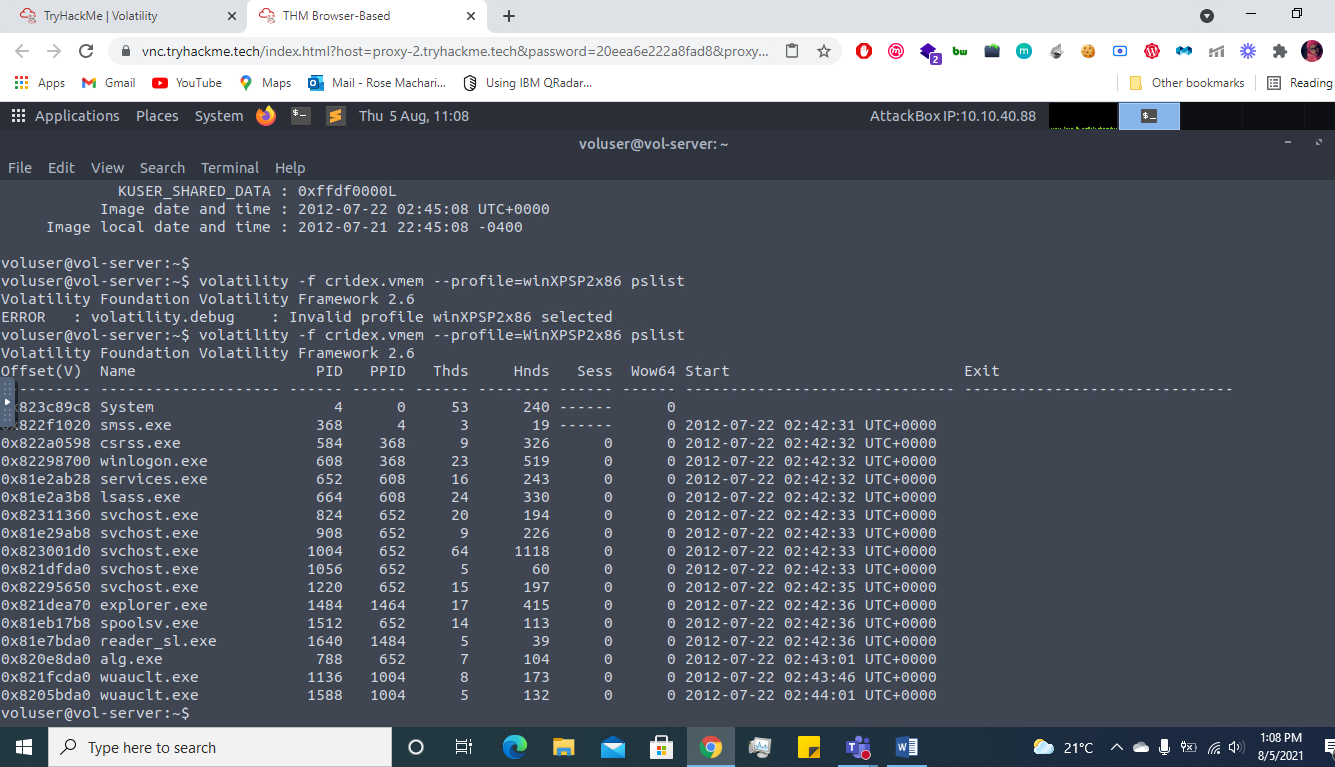
First, let's figure out what profile we need to use. Profiles determine how Volatility treats our memory image since every version of Windows is a little bit different. Let's see our options now with the command `volatility -f MEMORY\_FILE.raw imageinfo`

Volatility -f cridex.vnem



Running the imageinfo command in Volatility will provide us with a number of profiles we can test with, however, only one will be correct. We can test these profiles using the pslist command, validating our profile selection by the sheer number of returned results. Do this now with the command `volatility -f MEMORY\_FILE.raw --profile=PROFILE pslist`. What profile is correct for this memory image? WinXPSP2x86

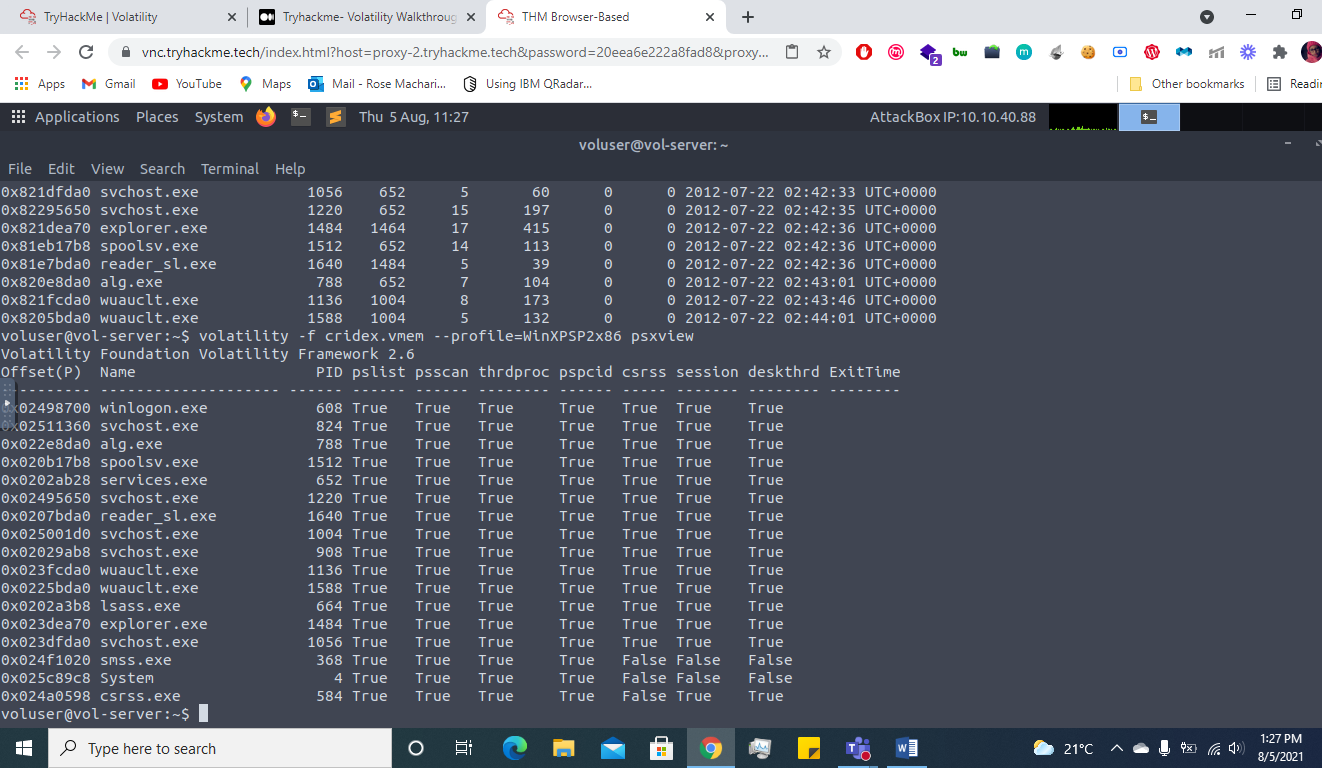
Volatility -f cridex.vnem –profile=WinXPSP2x86 pslist



Take a look through the processes within our image. What is the process ID for the smss.exe process? If results are scrolling off-screen, try piping your output into less: 368

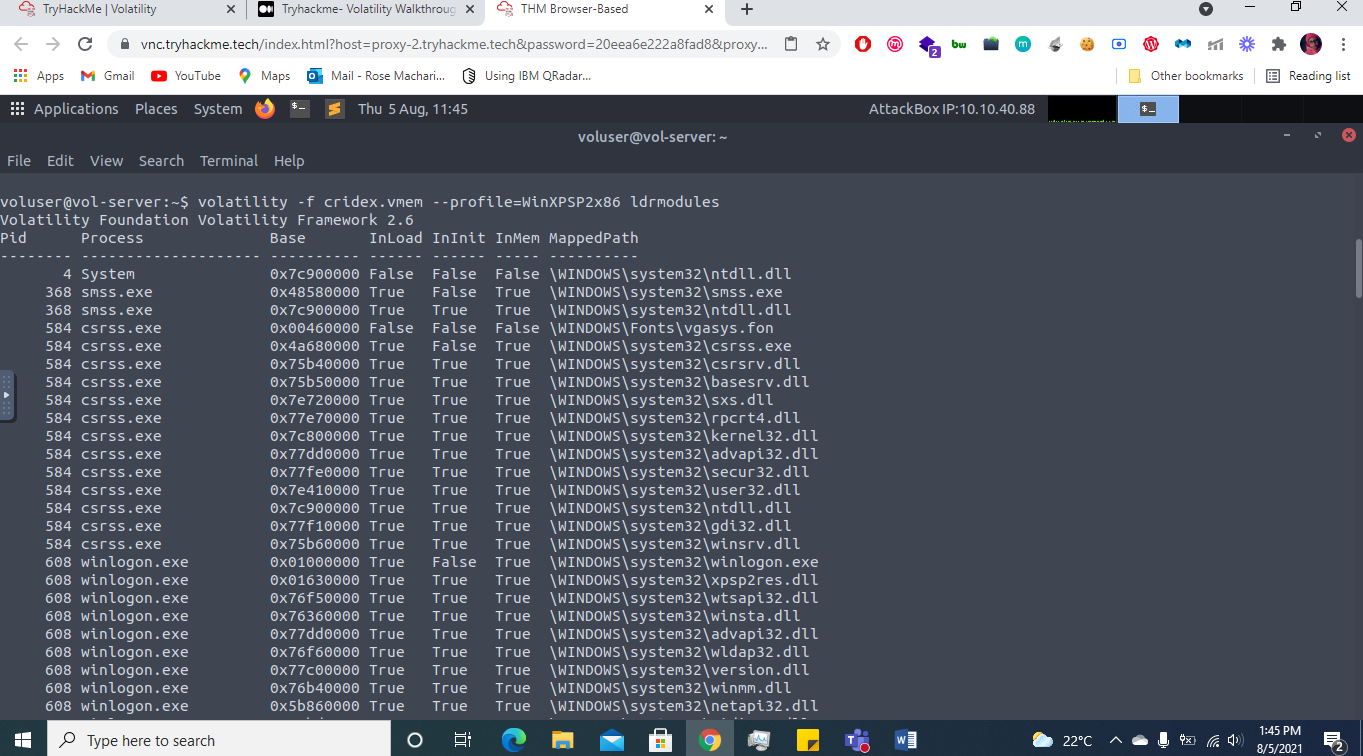
It's fairly common for malware to attempt to hide itself and the process associated with it. That being said, we can view intentionally hidden processes via the command `psxview`. What process has only one 'False' listed? csrss.exe

Volatility -f cridex.vnem –profile=WinXPSP2x86 psxview



In addition to viewing hidden processes via psxview, we can also check this with a greater focus via the command 'ldrmodules'. Three columns will appear here in the middle, InLoad, InInit, InMem. If any of these are false, that module has likely been injected which is a really bad thing. On a normal system the grep statement above should return no output. Which process has all three columns listed as 'False' (other than System)? csrss.exe

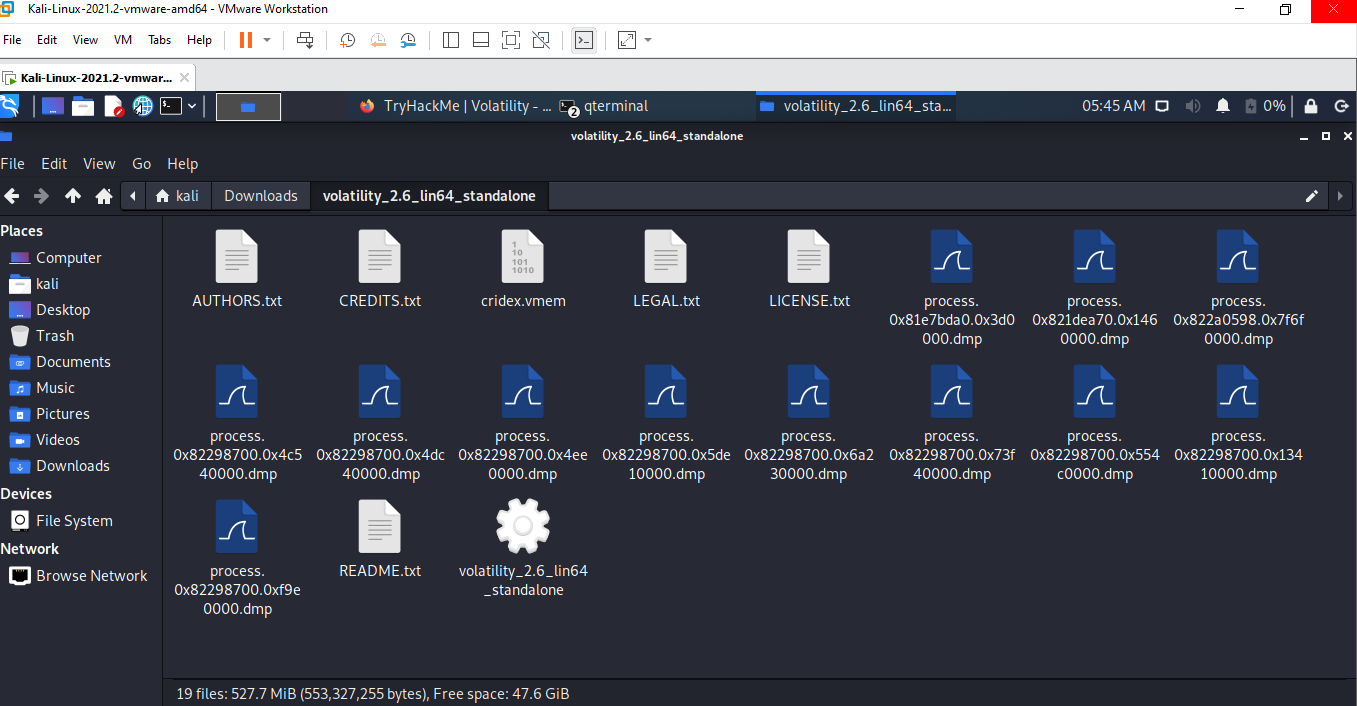
Volatility -f cridex.vnem –profile=WinXPSP2x86 ldrmodules

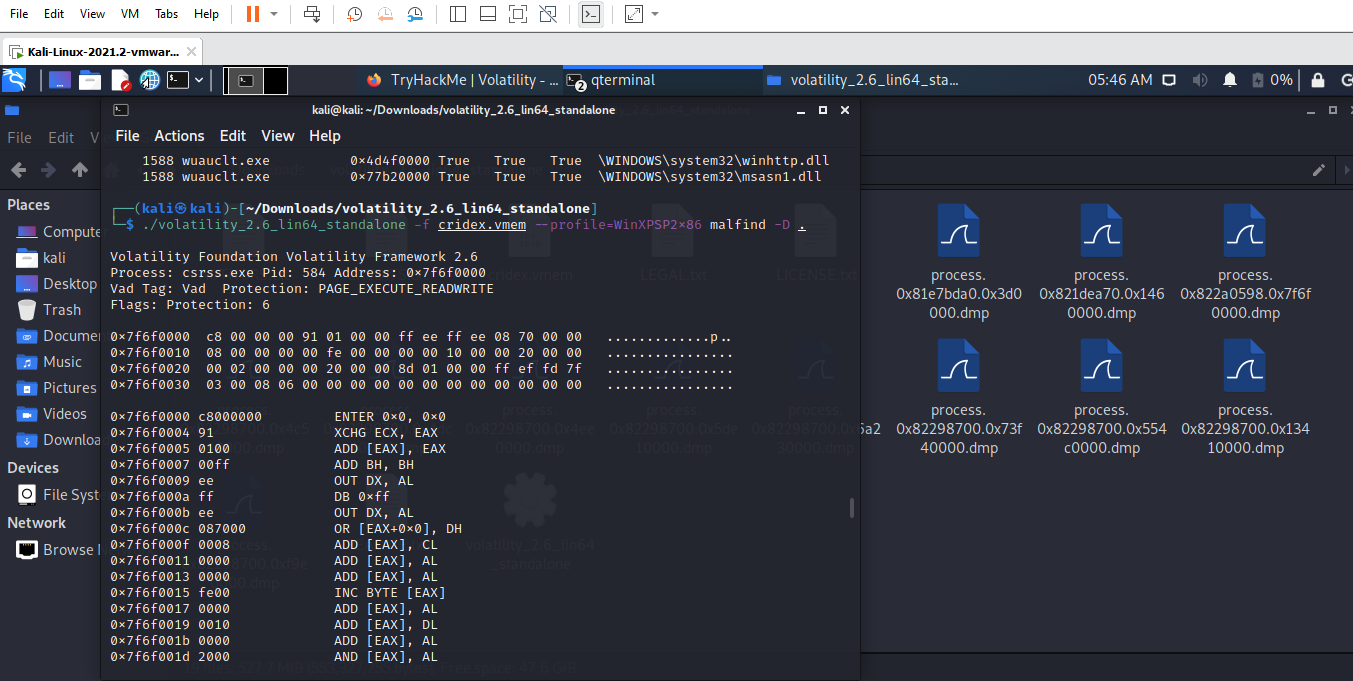


Injected code can be a huge issue and is highly indicative of very very bad things. We can check for this with the command `malfind`. Using the full command `volatility -f MEMORY\_FILE.raw --profile=PROFILE malfind -D <Destination Directory>` we can not only find this code, but also dump it to our specified directory. Let's do this now! We'll use this dump later for more analysis. How many files does this generate? 12

Volatility -f cridex.vnem –profile=WinXPSP2x86 malfind -D .

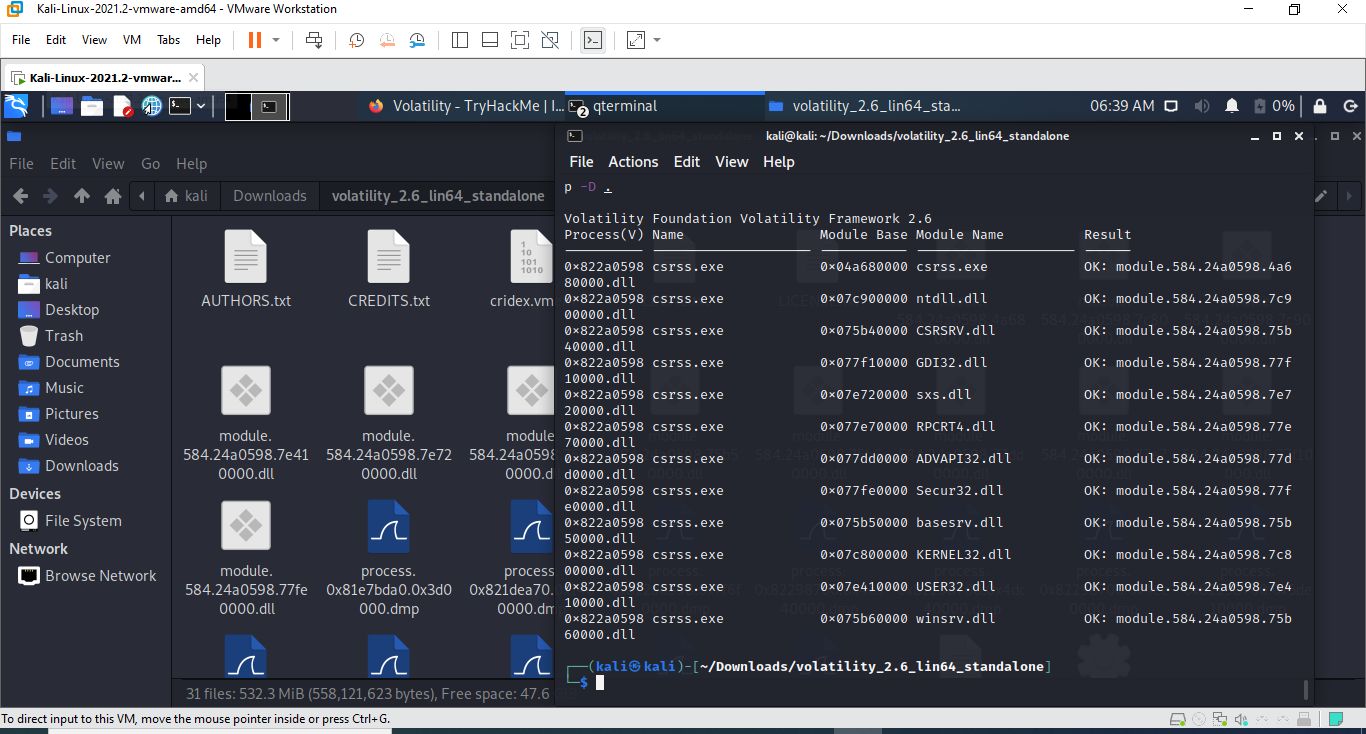
Last but certainly not least we can view all of the DLLs loaded into memory. DLLs are shared system libraries utilized in system processes. These are commonly subjected to hijacking and other side-loading attacks, making them a key target for forensics. Let's list all of the DLLs in memory now with the command `dlllist`

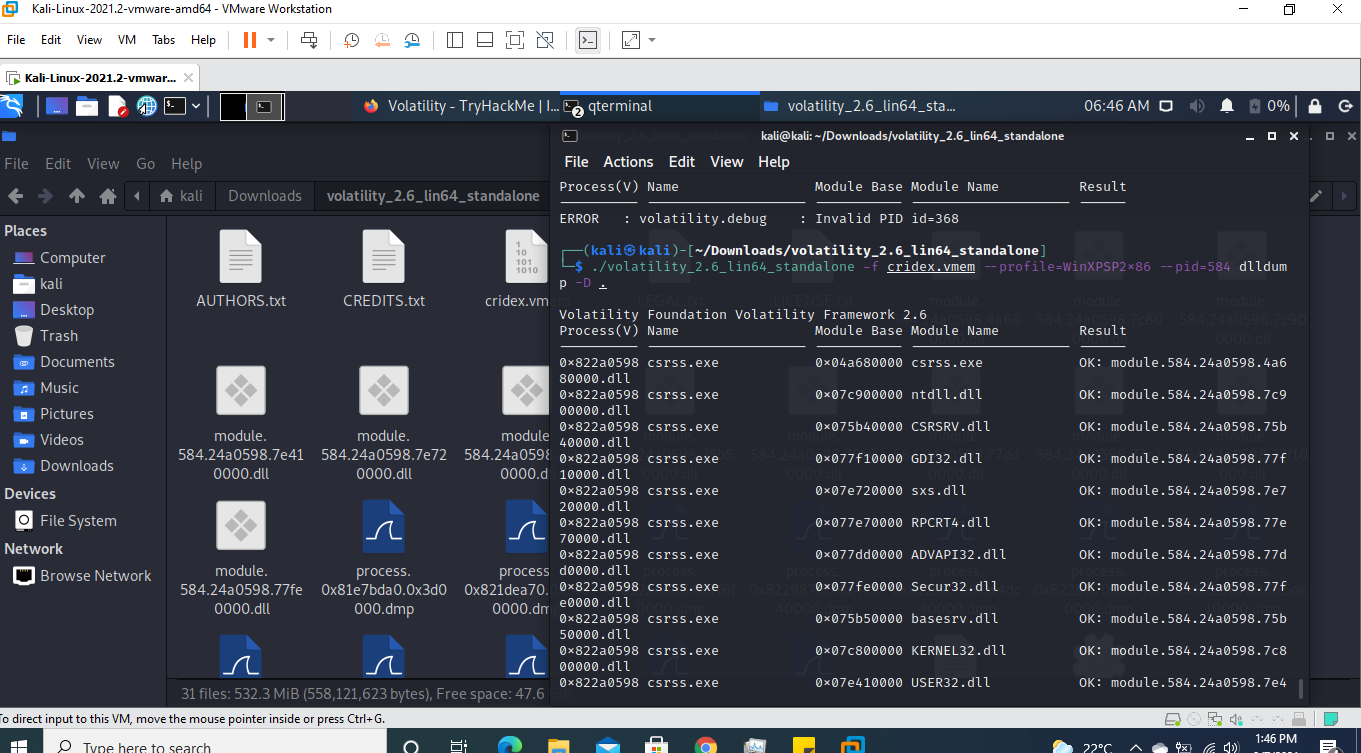




Now that we've seen all of the DLLs running in memory, let's go a step further and pull them out! Do this now with the command `volatility -f MEMORY\_FILE.raw --profile=PROFILE --pid=PID dlldump -D <Destination Directory>` where the PID is the process ID of the infected process we identified earlier (questions five and six). How many DLLs does this end up pulling? 12

Volatility -f cridex.vnem –profile=WinXPSP2x86 –pid=368 dlldump -D .





Upload the extracted files to Hybrid Analysis for examination - Note, this will also upload to VirusTotal but for the sake of demonstration we have done this separately

*In the terminal calculate the has of the modules,,,(Md5sum module.584.24a0598.7e410000.dll) then copy the hash to virus total and hybrid then analyse it*

What malware has our sample been infected with? You can find this in the results of VirusTotal and Hybrid Anaylsis. Cridex

