Justin Coleman  
IA455  
03/25/2021  
Assignment Six: Disk Forensics

## Forensics tools

Autopsy (4.12.0):  
“Autopsy® is the premier end-to-end open-source digital forensics platform.”  
<https://www.autopsy.com/download/>

FTK Imager (4.5.0.3):  
“FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool is warranted.”  
<https://accessdata.com/product-download/ftk-imager-version-4-5>

Certutil (10.0.19041.1):  
“Certutil.exe is a command-line program, installed as part of Certificate Services.”  
<https://man7.org/linux/man-pages/man1/sha1sum.1.html>

Virustotal.com (April 4th, 2021):  
“Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.”  
<https://www.virustotal.com/gui>

Hybrid-analysis.com (April 6th, 2021):  
“A free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.”  
https://www.Hybrid-analysis.com

MiTeC Windows Registry Recovery (3.1.0)  
“This application allows to read files containing Windows 9x, NT, 2K, XP, 2K3, 7, 8, and 10 registry hives. It extracts many useful information about configuration and windows installation settings of the host machine.”  
<http://www.mitec.cz/wrr.html>

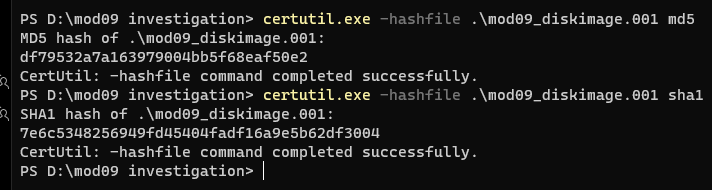
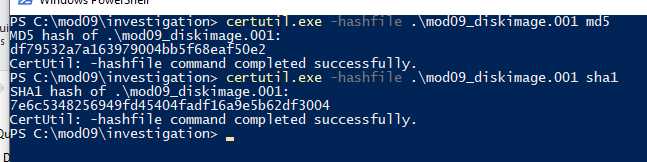
## Create a digital forensics workstation

|  |  |
| --- | --- |
| Windows 10 Pro 1909 | Build 18363.1440 |
| CPU | 2 with 1 Core |
| RAM | 7 GB |
| Hard Drive | 160 GB |

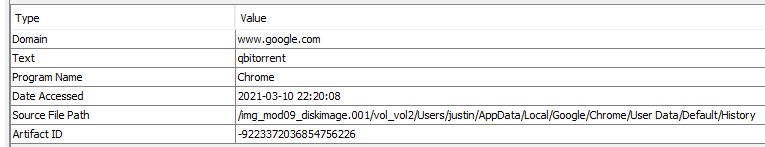
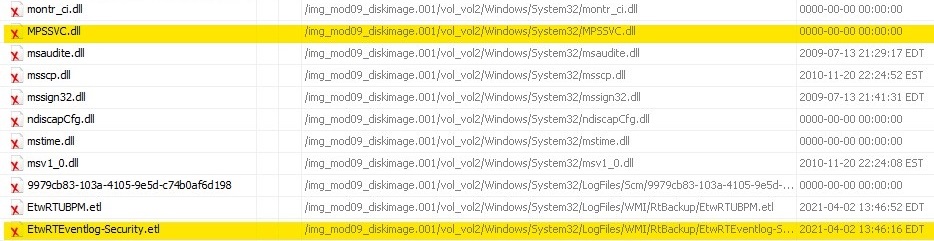
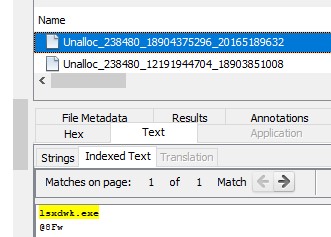
I installed a Windows 10 Pro VM with the above specs using otherwise default options. From this point manually installed Autopsy 4.12.0 using the default options from a known good installer.

## Capture disk image with FTK Imager

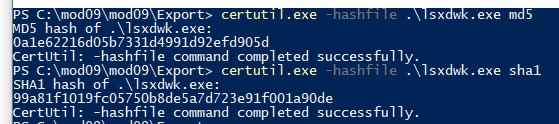
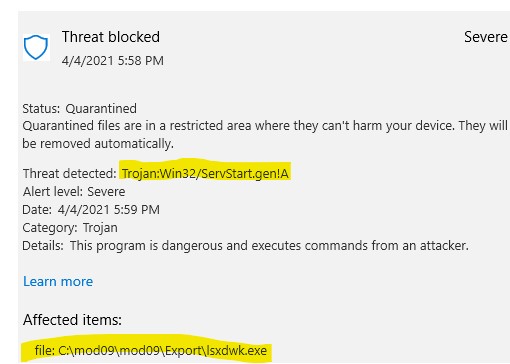
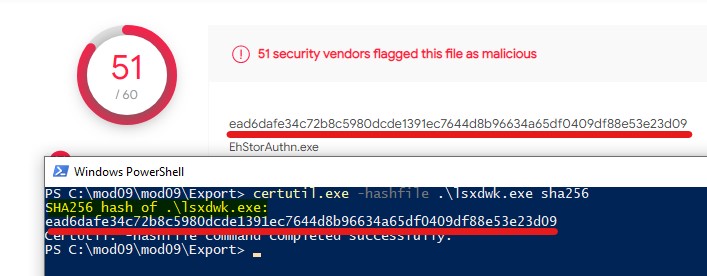
I installed FTK Imager on a USB drive using the following steps:

1. Installed FTK Imager on my host machine.
2. Inserted an NTFS formatted flash drive.
3. Copied the entire "**FTK Imager**" installation folder located at "**C:\Program Files\AccessData\FTK Imager**" to my flash drive.
4. Copied msvcp120.dll, vcruntime140.dll, and all MFC\* files located in **C:\Windows\System32**
5. Attached the flash drive to the Win7-VICTIM VM.
6. Run FTK Imager.exe (as Administrator) and used: File > Create Disk Image
7. On the Select Source window, I chose Logical Drive
8. From Select Drive options, I chose C:\ - [NTFS]
9. I verified the sha1 sum of the disk files before and after transfer to the forensics VM.  
     
   

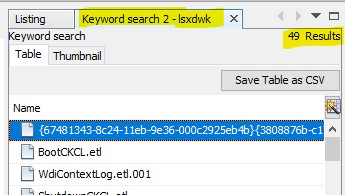
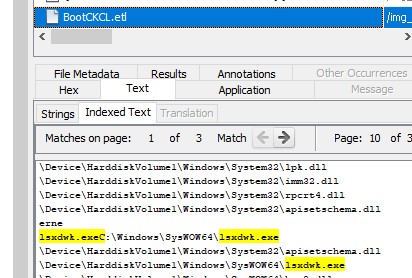
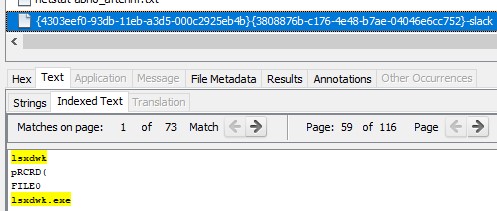
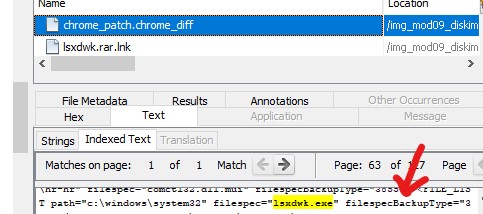
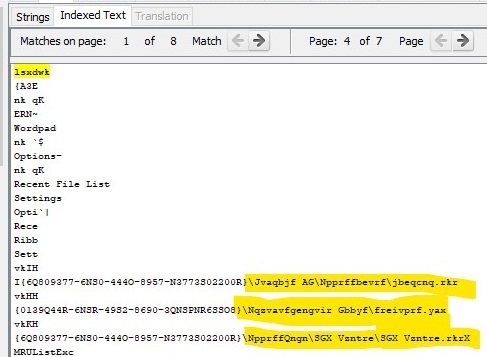
## Analyze disk image

To analyze the disk image more quickly and efficiently, I loaded it into Autopsy 4.12.0 using the Add Data Source button. Given that I performed a full disk capture, it took over twelve hours to fully ingest the 60 GB image into Autopsy. Note that it is possible to begin work within Autopsy while still ingesting evidence, but I prefer to wait until the entire image is loaded, as this prevents missing artifacts or needing to redo aspects of the investigation. My first point to check was the recent web searches, which revealed searches for a BitTorrent client (qBitTorrent) and searches for a popular file-sharing website, piratebay:  
  
Given the potential threat this combo presents, I knew that I needed to look for signs of malicious behavior. I next looked through the deleted files and noticed several important Windows files, including security event logs and MPSSVC.dll (Windows Firewall file). This is highly suspicious because I know for a fact that this machine has never installed any Windows updates, so there’s no reason for any of these types of files to have been deleted:  
  
Next, I looked through the files carved from unallocated space and came up with a suspiciously named file that doesn’t appear to be a built-in Windows executable:  


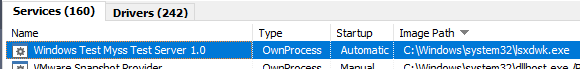
## Extract and analyze malware

To test my hypothesis that this was malware, I searched and found the file located in C:\Windows\SysWOW64\lsxdwk.exe which I then extracted:  
  
and immediately it was picked up by my forensic machine’s anti-virus:  
  
To get a more thorough examination I next checked it on Virustotal.com:  
  
The consensus on virustotal is that this is a Remote Access Trojan – a file that allows an attacker to take control of the machine and execute commands from their home system(s).

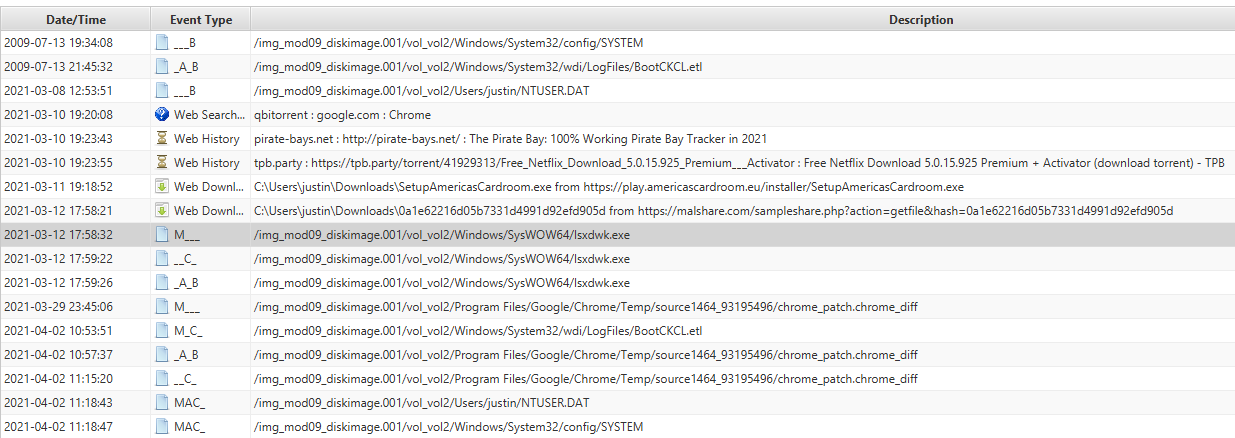
## Further information gathering

With this established, I next needed to attempt to determine the extent to which the system had been compromised, so I ran a search for the string ‘lsxdwk’ in all files  
  
Some of the most notable were BootCKCL.etl, which provides a high-level boot trace of the system showing that lsxdwk.exe had achieved persistence by some as yet undiscovered method:  
  
It appears to have created and deleted a SID for itself (recovered from slack space):  
  
I also found what looks to be an infect Google Chrome update process:  
  
This could be a way to get the file back on the system should it get deleted or perhaps a method to apply updates to the malware.  
  
Finally, there’s mention of both lsxdwk.exe along with several strangely named files in the SYSTEM and ntuser.dat registry hives:  
  
This suggested a possible source of the persistence mechanism employed by this malware.

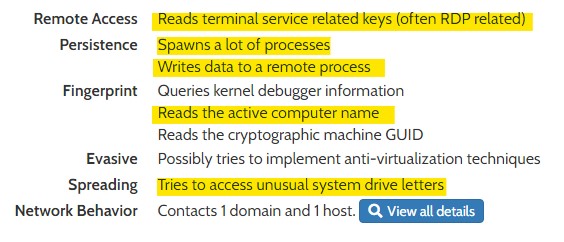
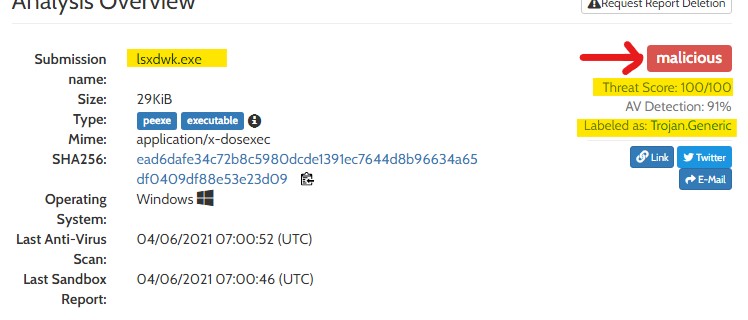
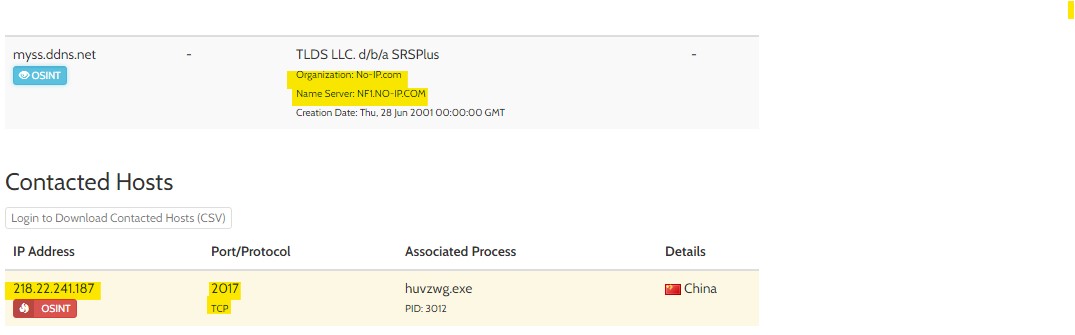
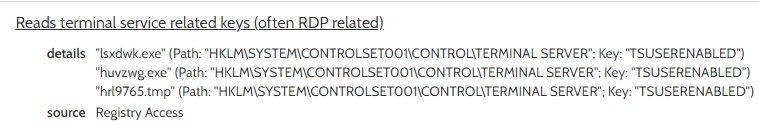
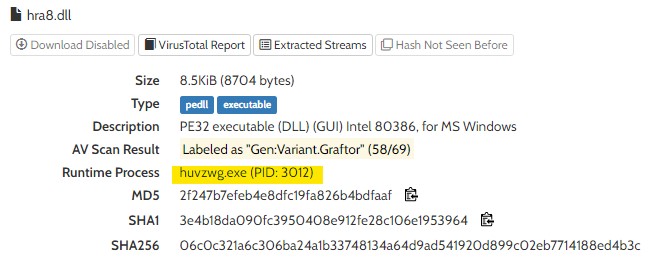
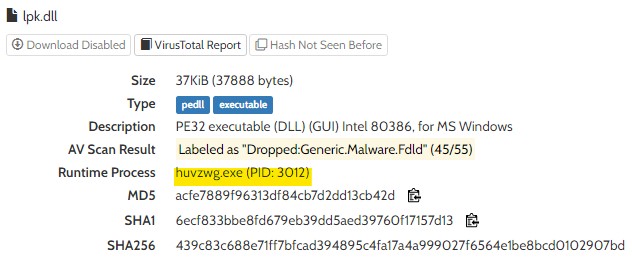
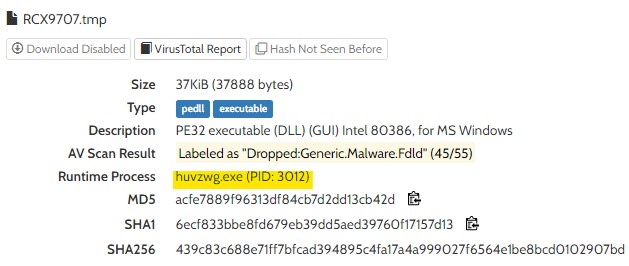
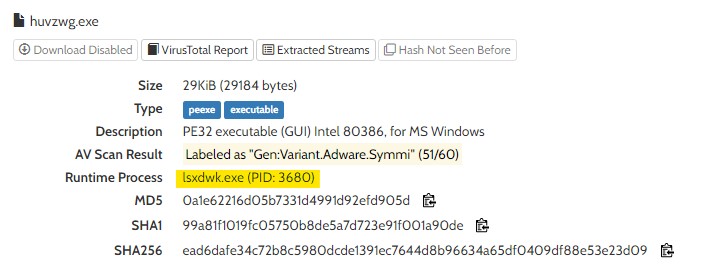
## Finding persistence mechanism:

I used MiTeC Registry Recovery to explore the extracted registry files, as I know that one of the prime targets of malware to maintain its access to the system is the registry. Loading the SYSTEM and ntuser.dat registry hives, I did not find anything in the Startup Applications sections, but I was able to find lsxdwk.exe in the Services and Drivers section:  
  
From this it’s clear that this Windows Test Myss Test Server 1.0 service is automatically loaded on Windows start up, achieving persistence on the infected machine.

## Timeline

Based on the above-mentioned files, here is a rough timeline of when they were created:  
The full report is included in the attached ia455-justincoleman-diskanalysisfiles.zip

## Appendix 1: Hybrid-analysis

I wanted to get a more thorough understanding of the malware that I discovered, so I ran it through Hybrid-analysis, which is a sandbox environment created to automatically determine malware functionality. The initial analysis:  
  
From this, a general understanding of the malware began to form. It is reconfirmed that this is a RAT trojan that spawns processes, writes data to remote processes, and attempts to reconnoiter the local networking environment via RDP-related keys and mounted network resources. Next, I took a look at the DNS and IP address of the remote attacking system:  
  
From this, it was easy to see that this was located in China, IP address 218.22.241.187 using port 2017. The attacker had registered a Dynamic DNS-based domain through no-ip.com: myss.ddns.net. The artifacts discovered previously by hybrid-analysis tied to this address:  
  
This tracks with the earlier investigation: attempting to grab RDP keys and enumerating shared drives are methods a worm might use to propagate itself across networks.   
  
Next, it was discovered that lsxdwk.exe also spawns several additional files:  
  
First, lsxdwk.exe spawns huvzwg.exe, which then spawns RCX9707.tmp, lpk.dll, and hra8.dll for additional functionality. Finally, we can see a wide range of hooks that the malware opens and writes to:

## Appendix 2: File list

|  |  |
| --- | --- |
| File Name | SHA1 Hash |
| Mod09\_diskimage.001 | 7e6c5348256949fd45404fadf16a9e5b62df3004 |
| lsxdwk.exe | 99a81f1019fc05750b8de5a7d723e91f001a90de |
| mod09\_diskimage.001-FullFileList.csv | 9460fd2b71f101b8ae74cc1b79b9a75934ae3015 |
| {67481343-8c24-11eb-9e36-000c2925eb4b}{3808876b-c176-4e48-b7ae-04046e6cc752}-slack | 4c65cf917ea42ff514af73f89dc58f9a7581eb3a |
| Unalloc\_238480\_18904375296\_20165189632 | 3bf74eea581e39c766e37d602fab54f7576d927e |
| 96352-SYSTEM | 76d8e3f1ba05352c3426c81f8f60b0cc5069bcf9 |
| Ntuser.dat | e85df945f4f1f5adb8ee8cf4826ac22b66c79814 |