**Intro to Malware Hunting**

**Offline approach**

This is when the system isn’t active and the code of the threat isn’t running

Might examine this by

* Booting of a Live CD into another OS and examine the file system
* Remove hard drive and mount in different machine and examine file system that way
  + Maintains integrity of the disk (used in forensics to maintain evidence)
* Clone system and place in virtual machine
  + Threat is then active and online but isolated and you can monitor its activity/behaviour

How to clean the system after a threat has been confirmed

* First, shut off the infected machine and analyse on another machine
* System rebuild, wipe and restart or use a snapshot
  + Complete wiping is good as you know all of the threats have been removed
* System clean
  + Delete the executables that make up the malware
  + Less guarantee that system is clean but less destructive to system if no backup is available

**Always have backups of file system and registry**

**Automated Malware Removal Tools (Online approach)**

Kaspersky

* Portable and free

MalwareBytes

Hitman Pro

RogueKiller

* Best with online as it analyses active behaviour

AdwCleaner

* Adware and browser extensions

When using an online approach, often the malware can either send back false information or commands in the code can stop the tools from even running

Boot into OS that supports these tools and analyse file system

Can boot into safe mode, maybe doesn’t start the malware and you can use the tools

* Sometimes even renaming the tools works

Rkill

* Attempts to kill malware processes to allow you to run the tools

Choco / Curl / Wget / Home(brew) / Apt-get

* For when browser is compromised or you can’t download the tools via browser