**Tips for before opening the image**

* Make sure VMware is fully updated to the latest software
* Have sufficient time to actually download the images -- this may take several hours
* Allocate more RAM to the image before you run it -- this will make it a lot faster/smoother
  + <http://kb.mit.edu/confluence/pages/viewpage.action?pageId=148602892>
* Make sure you have a stable internet connection, as well as a power source (if you’re using a laptop)
* Have all materials prepared before beginning the competition
* **DO NOT open the image before the competition time under any circumstance**

**Resources for Cyberpatriot**

* Official Cyberpatriot resources: <https://www.uscyberpatriot.org/competition/training-materials/windows>
  + The training modules alone should be sufficient for the first round
* Microsoft documentation (great for research): <https://docs.microsoft.com/en-us/>
* General crypto resource for forensics: <https://gchq.github.io/CyberChef/>
* Practice Images: <https://magistrate.shiversoft.net/>
* <https://www.google.com>
* I suggest creating your own checklist to aid in the competition

**Competition Checklist - Quick Start**

* **Open the README first and skim/read it first**
* **Open up the Scoring Report and verify the network status of the image**
  + If the messages are still red after a while, there is something wrong with your network:
    - Internet Connectivity Check: Checks an image’s ability to connect to Google. If it fails, there is a problem with the image’s connection or something on the network is blocking access.
    - CCS Server Connection Status: Checks an image’s ability to connect to the scoring server. If it fails, you will need to troubleshoot your network connection.
    - CCS Server Score Upload Status: This checks an image’s ability to upload scoring data to the scoring server. A failure is usually the result of a proxy server or other security measure.
* **Complete the Forensic Questions next**
  + If any of the forensic questions involve physical files, make sure to KEEP those files if you haven’t completed the questions yet
    - If you decide to give up on a forensic question and the file is a vulnerability issue, record the location, properties, and other details of the files before doing so, in case you decide to work on it later.
* **Begin Windows Updates** - this might take a while, so it is a good idea to start the updates early
* **Configure users accordingly to the README**
* **Run through control panel items (Firewall, virus protection, etc.)**
  + Using Godmode: <https://www.online-tech-tips.com/computer-tips/enable-god-mode-control-panel-windows/>
* **Uninstall unwanted software (Wireshark, Nmap, etc.) and update other software (Firefox, Internet Explorer, etc.)**
* **Find and delete unwanted files (suspicious text files, media files)**
  + Software to quicken search process: <https://www.voidtools.com/>
* **Update security policies**
  + gpedit.msc, secpol.msc
  + Follow CIS Benchmarks: <https://www.cisecurity.org/cis-benchmarks/>
* **Disable/Enable/Configure services**
  + You will (in later rounds) likely need to configure the critical services mentioned in the README
  + <https://www.blackviper.com/service-configurations/black-vipers-windows-10-service-configurations/>
* **Restart to fully update Windows**