Widows 8/10 Checklist

1. **Review the scenario and all forensics questions:** Ensure that you have created a good record of what the readme is telling you, and what the forensics questions are asking for.
2. **Search for forensics questions answers:** I like to do this first because sometimes the forensics questions deal with malware, incorrect settings, or other items you would change. If you remove malware that the forensics question is asking you about, you're not going to be able to find the answer. This is an easy way to earn points.
3. **Go through the User Accounts section of the Control Panel:** Look through all of the users. Make sure that they are at the level that they need to be at, are adhering to password policies, and are actually supposed to be there. Disable the guest account unless the readme specifically tells you not to. Verify the al group assignments are correct.
4. **Set the security policies in secpol.msc:** Go through **secpol.msc** and set the Password and Audit log settings. They should look something like this:
    - Enforce Password History: 5 passwords remembered
    - Maximum Password Age: 30 to 90 days
    - Minimum Password Age: 5 days
    - Minimum Password Length: 8 characters
    - Password must meet complexity requirements?: Yes
    - Store passwords using reversible encryption?: No.

    You should also go through and **turn on auditing** for failed and successful log-ons while in **secpol.msc.**

5. **Enable UAC (User Account Control):** Turning UAC up to the highest level is generally a good practice and will earn you points in most cases.
6. **Enable Windows Firewall:** Turning on the Windows Firewall is a requirement in most images. The level of protection for your system may vary, and some exceptions in the firewall may apply. Be sure to check that the firewall is still up periodically after you do it the first

time.

7. **Check the Windows Scheduled Tasks:** If you've been experiencing any unexplained settings changing, pop-ups, or any other odd behavior, check the Scheduled Tasks. Look for anything that runs suspicious programs, opens error messages, etc. This is tedious, but is a good way to earn some extra points. Figuring out how often the nuisance occurs is a good way to nail down exactly what scheduled task is causing your problem.
8. **Look at Windows features in Programs and Features:** Look for anything that you know that your computer shouldn't have. Telnet is usually a no-no, but sometimes the Readme tells you to leave it on, or even enable it. Make sure your computer isn't running a web server if it shouldn't be.
   - Disable IIS and FTP
9. **Look for junk programs, malware, and hacking tools:** The Programs and Features section of the control panel will display a list of programs that are installed.
10. **Ensure that all required programs are running correct versions:** Note that the latest version is not always the correct version. The readme will usually tell you what version of a program to have. Standard fix is to **update Firefox version.**
11. **Install/Enable Antivirus Software:** Free antivirus software like AVG or Avast will do, but it has to be a free trial version for the competition. Scanning the system with **MalwareBytes** is a good idea, too.
12. **Use Process Explorer to see what's running on your computer:** Look for anything suspicious. Remove. Repeat.
13. **Use Autorun to see what's running when you first start up your computer:** This will help you locate pop-ups, and speed up start times.
14. **Make sure any important Windows Updates and Patches are installed:** This can be a long and tedious process, so see what you can bring in on removable media to help speed up the process.
15. **Verify that your browser is in good, working, uncluttered order:** Make sure that there are no unauthorized add ons, plug-ins, un-needed toolbars, etc. The process for removing these items varies by browser. Review security settings.

16. **Make sure your image doesn't contain any unauthorized media files:** Things like .mp3, .mov, have to go. Using the Windows search bar (*.mp3 searches the selected area for .mp3 files) is a good place to quickly find these media files.
17. **Use netstat -abq to look for listening ports:** Make sure nothing is listening that shouldn't be.
18. **Go through everything more than once, and document everything:** Going back through and making sure everything is exactly how you left it and how you want it is a good way to find errors that you might have missed. Documenting everything helps identify errors that you may have caused.
19. **Check for shared drives.** Best bet is to first check that C: drive is not set as a shared drive.
20. **Review the running Services.** The list of common services that are standard for for Windows 10.: https://www.winhelponline.com/blog/windows-10-default-services-configuration/. Use these to compare to shat's currently running.
21. **Turn off File and Print sharing** : https://www.isunshare.com/windows-10/turn-on-or-off-file-and-printer-sharing-in-windows-10.html
22. **Disable Remote Desktop Connections** : https://www.thewindowsclub.com/remote-desktop-connection-windows

Couple of extra things :

How do you create a MD5/SH1 Hash for a file in Windows:
https://support.microsoft.com/en-us/help/889768/how-to-compute-the-md5-or-sha-1-cryptographic-hash-values-for-a-file

This is a good thing to have in your back pocket for future forensics querstions : get-filehash -algorithm md5 <file_to_check>
https://www.howtogeek.com/67241/htg-explains-what-are-md5-sha-1-hashes-and-how-do-i-check-them

Bit Locker on Windows 10
https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10