Triage - Hiren USB Key HD cleanup form

This checklist form is useful for when booted off a Hiren Boot USB key. It is quite easy to remove unneeded temporary files and folders from a customer's hard drive when booted off a Hiren key. File permissions restrictions that may restrict you from deleting a file when booted off a hard drive are not active when booted off a Hiren key.

Over the course of time, using this form before running other utilities will save you considerable bench time.

When booted off the Hiren Win XP environment:

For computers that have Windows VISTA or 7 installed

1. _____ Delete c:\Quarintine folder (but do not open it) if it is there. (It may not be there) .
2. _____ Delete c:\pagefile.sys (swap file) incase it is corrupted. It will rebuild upon restart.
3. _____ **Restore Point deletion – Restore Points can take up many Gigabyte of space and may have malware or virus in them. -** *(know when to NOT delete restore points at this point in the service to the computer)*
    a. *For example, if a client reports that a problem recently started then restoring the computer to an earlier point may fix the issue in a matter of minutes*
    b. *You can always delete the restore points later on from within Windows.*
    c. *When service to the computer is complete, I like to create a restore point and name it "Repair Center work completed"*
    d. *If the problem is not related to anything a Restore Point may fix….*
        i. Open c:\System Volume Information folder and delete all the entries in it
4. _____ Remove files in c:\windows\temp folder
5. _____ Migrate to C:\ Users folder. Open customer's profile folder. Navigate to Appdata\Local\temp folder and delete all entries
6. _____ Migrate to C:\ Users folder. Open customer's profile folder. Navigate to Appdata\Local\Microsoft\Windows\Temporary Internet Files folder and delete all entries
7. _____ Open 'HBCD Menu' icon on Hiren desktop. Select Programs. Select Hard Disk / Storage ----→ HD Tune option. When HD Tune is open, click on 'error scan' tab and select 'start'. If any Red blocks appear, make a note of it as this indicated a bad sector(s) on the hard drive. All green blocks means the hard drive likely does not have any bad sectors.
8. _____ This step is optional – ***Know when to run it*** - If HD tune finds no bad blocks, Open 'HBCD Menu' icon on Hiren desktop, Under 'Programs', select Optimizers → Defraggler. Run the utility on the correct drive (should be the largest one). This can take quite a while if the hard drive is large. If near end of day, under 'Defraggler Settings' tab select "shutdown when done" before starting defraggler. *This is a good feature – whoever added the shutdown after scan feature had common sense.*

End of this section -

6-2015 – **Difficult virus removal ? -** If you are dealing with a virus that is proving difficult to remove: it seems as if the best course of action after triage in these situations is to:

1. If the problem started recently, use a system restore point to see if you can fix the issue BEFORE deleting the restore points in triage.

2. Slave the HD into a work station to run specific utilities before running utilities from the customer's computer itself. Suggested utilities to run on the slaved HD are: Superantispyware, Avaste antivirus, malawarebytes (yes, you can do custom scans)
3. Now, reinstall the HD into client's computer and start the computer boot in safe mode with network support as the infection is likely to not be running in safe mode In safe mode, recommended utilities to run on client's system are: . (Run them in order given (*based on previous level of success*) - stop when you feel the malware / Trojan / Virus is removed)

1. TFC – removed more temp files	4. Superantispyware	7. Hitman Pro
2. Ccleaner or PC decrapifier to remove junk programs	5. MalawareBytes	8. May need to research if s deep infection
3. ADwCleaner	6. Spybot	9. If needed, and if possible, a root kit utility may need to be run

Step 3- boot the computer in normal to determine if you have been successful . – Open all the browsers and navigate to multiple pages – Open different applications to see that they work

Step 3 – Remember to remove all the utilities you just installed and ran

Notes: _____