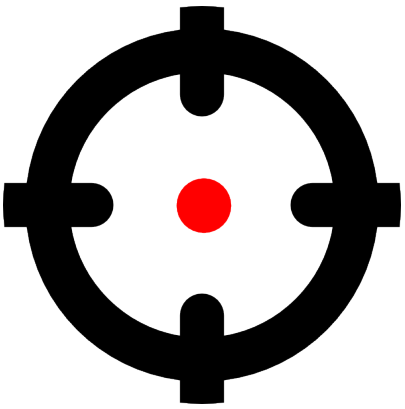
Instalog Requirements Document Version 1.0

Billy R. O'Neal III (bro4@case.edu)
Jacob Snyder (jrs213@case.edu)

Case Western Reserve University

February 29, 2012



Contents

1 Intended Users

Instalog is designed with three types of target users in mind. These “user classes” are listed in the following sections.

1.1 Home Users

For a typical home user, Instalog must not display a complicated interface, and must make it relatively difficult to misstep and take a wrong action. Few options need be presented, such as the ability to generate a default report and the ability to take a given script and run it on a target machine. Complicated features such as analysis must not be displayed; though they may appear as options that are, by default, deselected.

1.2 Administrators

Administrators are similar to home users in that they are physically working at a computer being examined, but they are different in that they have the intent of repairing their own computer or the computer of a client. They wish to see analysis features and more possible options. Instalog must provide a means for Administrators to use it’s analysis features without manual saving and reloading of log files.

1.3 Forum Experts

Forum Experts help typical end users repair their machines remotely over self-help forums such as BleepingComputer.com or GeeksToGo.com. These users work remotely, and likely will never see a given target machine. Instalog must produce log formats that are human readable in the vast majority of cases, but which can be passed through common forum software such as Invision Power Board, phpBB, or vBulletin without destruction of information. Unfortunately, this makes common data exchange formats such as JSON and XML unsuitable.

Moreover, as obtaining additional information from a machine may have lead times of several days, Instalog’s report must be unambiguous; that is, no two possible system configurations may produce the same output. Experts can also benefit from log analysis features. Finally, Experts need to be able to write simple, human readable scripts to perform actions to fix a user’s machine remotely.

2 Scripting Requirements

One of the main features of this tool is the logging capability. The log will be separated into multiple “sections,” where each section has similar information grouped under it. There will be a default script of actions that is provided with the tool that will be performed as the first part of this tool. There will also be additional script actions that a script can specify to gather more targeted information about a system.

3 Scanning Requirements

Below are the default log sections that should be presented after a default scan has been run.

1. Header
2. Running Processes
3. Machine PsuedoHJT Report
4. n User PseudoHJT Reports (One for each loaded user registry on the system)
5. Mozilla Firefox (if Mozilla Firefox is installed)
6. Google Chrome (if Google Chrome is installed)
7. “Interesting” files present on the filesystem based on date, time, location, etc.
8. Event Viewer (if any relevant events need be reported)
9. Machine Specifications
10. Restore Points
11. Installed Programs
12. Footer

3.0.1 Additional Log Sections

These log sections are not included in the default scan, but can be run optionally through a custom script.

1. DNS Check
2. Directory
3. VirusTotal
4. MRC Upload
5. Process Kill
6. File Quarantine
7. Security Center
8. Registry 32 Bit
9. Registry 64 Bit

4 Repair Action Requirements

A fix script is a textual representation of the actions that should be taken to clean up a system. Most of the log sections listed in the previous section will have fix actions associated with them. Again, the specifics about this are too detailed to include in a document of this scope, but will be explained in full in the specification document.

One very important requirement of fix script actions is that they MUST create a backup before they proceed so that the action taken can be reverted.

5 Graphical User Interface Requirements

The graphical user interface will be the only method for interfacing with this tool. The interface is designed such that it will enable all three of the user classes described in the “Intended Users” section to go through their appropriate workflows. As such, the GUI must bridge the gap between being simple enough for home users to use yet complicated enough for power users to build complex fix scripts. This balance is achieved by splitting the GUI up into several screens for completing various parts of the workflow.

Like the other sections, enumerating all of the requirements and specifications of this would be beyond the scope of this document. This being said, the GUI should include the following screens:

1. Main screen
2. Running screen
3. Run completed screen
4. Analysis screen
5. Analysis complete screen
6. Finished screen

This screens will be connected in the manner described in Figure 1.

6 Other Requirements

Instalog will support all Microsoft Windows NT variants released later than Windows 2000 for x86 and x64 based computers. Specifically, this tool shall support:

- Windows 2000 (x86, SP4 only)
- Windows XP (x86 and x64, RTM, SP1, SP2 and SP3 (on x85 machines))
- Windows Vista (x86 and x64, RTM, SP1, and SP2)
- Windows 7 (x86 and x64, RTM and SP1)
- Windows Server 2003 (x86 and x64, RTM, SP1, SP2)
- Windows Server 2003 R2 (x86 and x64, RTM, SP1, and SP2)
- Windows Server 2008 (x86 and x64, RTM, SP1, and SP2)
- Windows Server 2008 R2 (x64, RTM, and SP1)