Item	Details
VirtualBox	You should have a running VirtualBox test lab
Kali	You should have a running Kali virtual system
Windows	You should have a running Windows virtual machine that can be isolated
Wireshark	You should have wireshark running on your test system
X32dbg	You should have x32dbg running on your system
IRMA	Download the IRMA VirtualBox appliance from Irma.quarkslab.com and load it into VirtualBox. Note the credentials vagrant/vagrant
nmap	Install nmap on IRMA by using the command: sudo apt-get install nmap
Comodo	Load the Comodo anti-virus into IRMA wget download.comodo.com/cis/download/installs/linux/cav-linux_x64.deb sudo apt-get install binutils ar x cav-linux_x64.deb sudo tar xvf data.tar.gz –C /
SysInternals	Load the Microsoft SysInternals set of tools from: https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite Download and extract
ProcessHacker	Download the Process Hacker zip archive from http://processhacker.sourceforge.net/
ProcessRevealer	Download and install Process Revealer from: http://www.tothepc.com/archives/view-all-active-hidden-processes-on-computer/
PE Explorer	Download and install PE Explorer down from http://www.heaventools.com/download/pexsetup.exe
PE Studio	Download and install PE Studio from https://www.winitor.com/binaries.html
LordPE	Download the LordPE archive from: https://appdb.winehq.org/objectManager.php?sClass=version&iId=14290