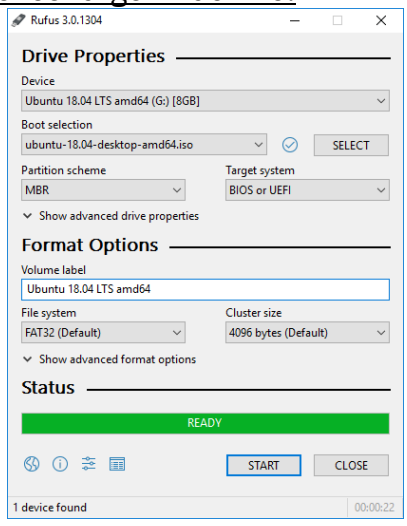
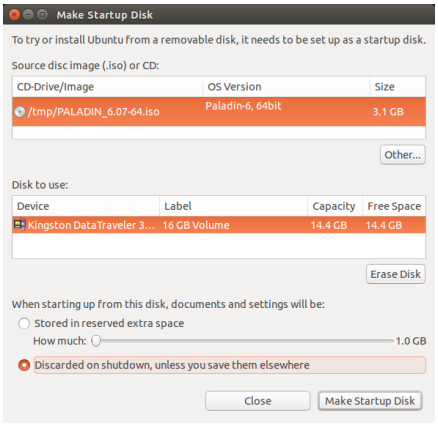
Preparation (on separate machine)

1. IBM X-Force IR recommends using Sumuri Paladin for disk imagining – below steps guide through this process. If using other tool, follow instructions of that provider.
2. Use Sumuri Paladin Edge Version 6 for 32-bit CPU target machines and Sumuri Paladin Edge Version 8 for 64-bit CPU target machines. This tool can be downloaded for free from the official website (there is an optional donation of 25$): https://sumuri.com/software/paladin/.
3. Once downloaded, either:
   a. Burn ISO to DVD using any disk burning software.
   b. Create bootable USB on Windows eg. with Rufus Portable (https://rufus.akeo.ie/) or any other software of your choice. Select appropriate partitioning scheme that matches target machine.



4. Create bootable USB on Linux Gnome/KDE - use Startup Disk Creator to create bootable USB drive. Don't enable USB persistence.

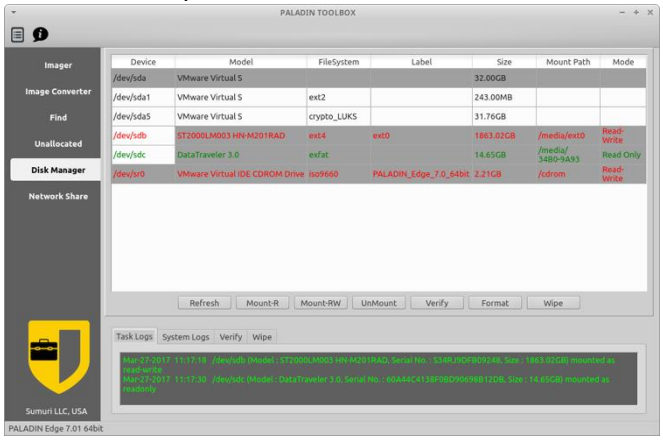


5. To avoid issues with boot device selection, consult manufacturer of your computer and/or motherboard on how to **reliably enable booting from DVD disk or USB flash drive** to perform forensically sound acquisition.
6. Prepare storage medium with at least the same size or amount of free space as media size in target machine. Tool allows forensic images to be stored on external hard drive attached to target machine or in file share over the network. Either:
   a. Quick-format external hard drive with NTFS file system.
   b. Prepare a file share with appropriate user rights.
7. Ensure that you have compression software capable of creating encrypted ZIP archives available in your system. If not, IBM X-Force IR recommends using 7-Zip Portable, available from official website: http://portableapps.com/apps/utilities/7-zip_portable or any other tool of your choice.

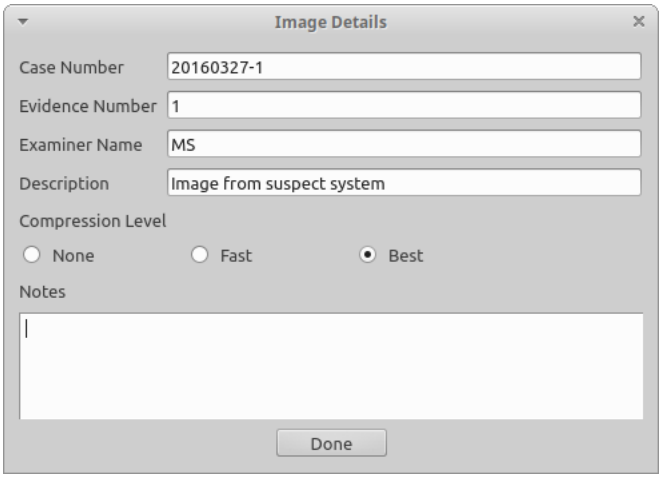
Information capture (on target machine)

1. Following instructions from manufacturer of your computer and/or motherboard, boot computer from previously created Sumuri Paladin DVD or USB drive.
2. Run 'PALADIN Toolbox' from the panel.

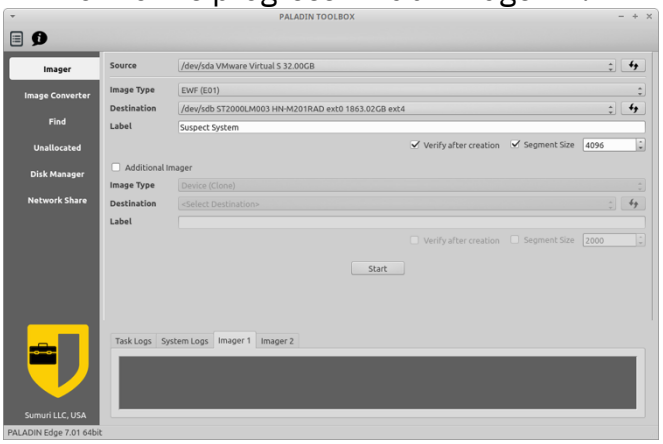
3. Mount storage for forensic image by following one of below steps, depending on option you have chosen:
   a. Attach previously formatted external hard drive, choose ‘Disk Manager’ tab, click ‘Refresh’ button, choose **partition** on the device that will appear in the list, and mount it in read-write mode by clicking on the ‘Mount-RW’ button.
   b. Enable networking, choose ‘Disk Manager’ tab, choose ‘Samba/Window Share’ tab, click ‘Mount’ button, fill in details in ‘Network Share’ window (switch ‘Read Only’ to ‘No’), and click the ‘Mount’ button.
4. Entries marked in green color are mounted with read only access and entries marked in red color are mounted with read/write access.



5. Set PALADIN Toolbox to store logs on previously mounted storage for forensic image by clicking ‘Logs’ button in upper left hand side corner, choosing previously mounted storage for forensic image in ‘Select Paladin logs media’ window and clicking ‘Select’ button.
6. Choose ‘Imager’ tab, select source **device** in ‘Source’ dropdown menu, select ‘Image Type’ as ‘EWF (E01)’ in ‘Image Type’ dropdown menu. In the ‘Image Details’ window provide ‘Case number’, ‘Evidence Number’, ‘Examiner Name’, ‘Description, and choose ‘Best’ as ‘Compression Level’, and click ‘Done’.



7. Choose previously mounted storage for forensic image in ‘Destination’ dropdown menu, enter unique and descriptive name in ‘Label’ field, tick ‘Verify after creation’ checkbox, tick ‘Segment Size’ checkbox and enter 4096, and click ‘Start’ button to start forensic image acquisition. You can monitor its progress in tab ‘Imager 1’.

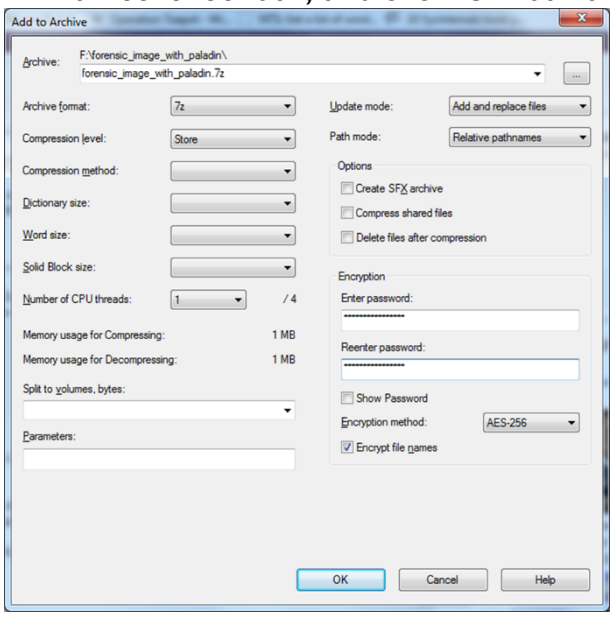


8. After forensic image acquisition and verification completes, scroll down in the popup window ‘Imager1 Logs’ and **confirm** that MD5 and SHA1 values in ‘Imager Logs’ section match respective values in ‘Verification’ section for both ‘hash stored in file’ and ‘hash calculated over data’. Close the popup window.

9. Unmount previously mounted storage by choosing ‘Disk manager’ tab, choosing ‘Device’ tab, selecting previously mounted storage for forensic image and clicking ‘UnMount’ button. Close PALADIN Toolbox.
10. Shut down computer by clicking on ‘App Menu’, clicking on power button in upper right hand corner and clicking on ‘Shut Down’ button.
11. When prompted, remove Sumuri Paladin DVD or USB drive, press ‘Enter’ key, and after computer has completely switched off remove any attached external USB drives containing forensic images and logs.

Preparation for delivery to IBM IR team (on separate machine)

1. Attach external hard drive with previously acquired forensic image or mount file share containing previously acquired forensic image.
2. Create compressed encrypted archive with below options, eg. using 7-Zip Portable.
3. Open the folder matching value provided as ‘Label’ during the imaging process and select the **file** with the same name as the folder and **extension E01** and click ‘Add’ from toolbar. **ONLY** add **file** with E01 extension to the archive.
4. In ‘Add to Archive’ window choose ‘7z’ from ‘Archive format’ dropdown menu, choose ‘Store’ from ‘Compression level’ dropdown menu, enter complex (16 characters, mixed case letters, numbers, and special symbols) password in ‘Enter password’ and ‘Reenter password’ fields, choose ‘AES-256’ from ‘Encryption method’ dropdown menu and tick ‘Encrypt file names’ checkbox, and click ‘OK’ button.



5. After encryption is completed, use 7-Zip to open newly created file with 7z extension, provide password and click ‘OK’ button, then click ‘Test’ from toolbar. If test completes without errors, encryption was successful.
6. Use method approved within your organization to securely erase file with previously chosen unique and descriptive name and extension E01.
7. Files in the folder matching value provided as ‘Label’ during the imaging process and in the folder ‘PALADIN_LOGS’ on the external hard drive or within the file share are now ready for delivery to IBM IR team via agreed method of delivery.
8. Share complex password used to encrypt file with E01 extension with IBM IR team using different communication channel then used to share forensic image.