IMAGING WITH CAINE

CONTENTS

BOOTING TARGET DEVICE FROM CAINE AND ACQUIRING A FORENSIC IMAGE

EQUIPMENT REQUIRED

1. USB key (16 GB or larger) (USB 2.0 or better is fine)
2. USB hard drive (size depends on the size of the drive being imaged)
    a. USB 3.0 or better if you have it as it will be faster. USB 2.0 will work fine. It will take longer to image.

OPTIONAL EQUIPMENT

3. USB hub (only required if the laptop being imaged only has 1 USB port)
    a. Optionally, you can boot CAINE into RAM allowing you to remove the USB key and connect the hard drive. Thus, this is very much optional. Don't worry if you don't have one even if there is only 1 USB port on the laptop.

CREATING BOOT DEVICE

4. Download CAINE from https://www.caine-live.net/ and create a bootable USB drive with it. See "**Appendix A –Create A Bootable USB**" for instructions.

NOTE TAKING

5. **IMPORTANT**
    a. Throughout this process it is imperative that you keep detailed notes of your actions, including the date/time you took those actions, and the outcome of those actions (especially if the outcome was not what you expected). You will want to date/sign your notes if on paper, or note your name at the bottom if electronic, and provide them to the investigator at the conclusion of this process.
    b. If the matter goes to court or a disciplinary hearing in a year or two, you will need to explain what you did, and any issues you encountered in the process. Acquiring electronic evidence is **THE MOST IMPORTANT** step in the forensic process. If there are concerns that the imaging process was not done correctly impacting the integrity of the image and its reliability, all subsequent analysis of that forensic image will suffer the same scrutiny as the image itself. If the tribunal deems that the image was done incorrectly, or not preserved correctly after collection, they can deem that it is not admissible, thereby rendering any analysis of it worthless. The burden is on us to show that it was done correctly, which is why your notes are critically important to demonstrate to the tribunal that it was done correctly and can be relied upon. And why it's imperative that a trained/experienced digital forensic examiner provides oversight of the imaging process.
    c. The best way to demonstrate this is to have the digital forensic examiner on a video call with the camera pointing to the computer you are imaging so that they can record everything, or at minimum make notes of what you did and provide direction where needed to ensure it's done correctly.

PREPARE TARGET LAPTOP/PC

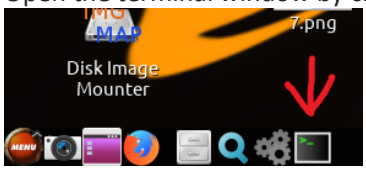
6. Go into the BIOS and check for Secure Boot - See "**Appendix B – Secure Boot**" to check and deal with Secure Boot.
7. See "**Appendix C – Fast Boot**" to deal with FastBoot.
8. Note the date/time in the BIOS vs actual date/time
    a. BIOS date/time: {date} {time}
    b. Actual date/time: {date} {time} {time zone}
        i. It's important to note your time zone.

BOOTING TARGET PC WITH CAINE

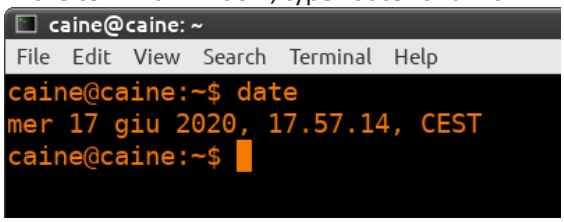
9. Connect the CAINE USB key.
10. Boot the laptop. As the laptop boots, press the appropriate key to change the boot device and select to boot from CAINE.
11. If you only have one USB port on the device, choose the option to boot CAINE into RAM. If you have at least 2 USB ports, you can hit ENTER to select the default boot option.
12. Once CAINE is booted, connect the USB drive you will be using to store the forensic image.

DATE/TIME AND TIME ZONE

13. Click on the Menu button (bottom left – red circle), and select System (not System Tools), Administration, Time and Date. A window will pop open where you can change the date/time, and time zone settings. Set the time zone to your time zone and set the date and time to your local date and time. Click on Close to exit out of the menu.
14. Open the terminal window by clicking on the terminal icon near the bottom left.



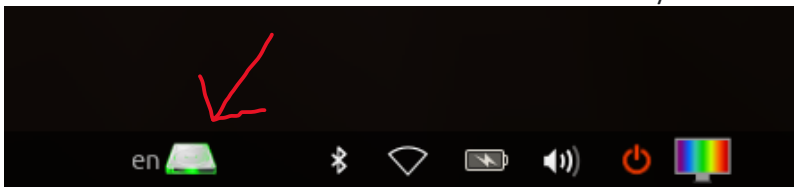
15. In the terminal window, type “date” and hit <ENTER>.



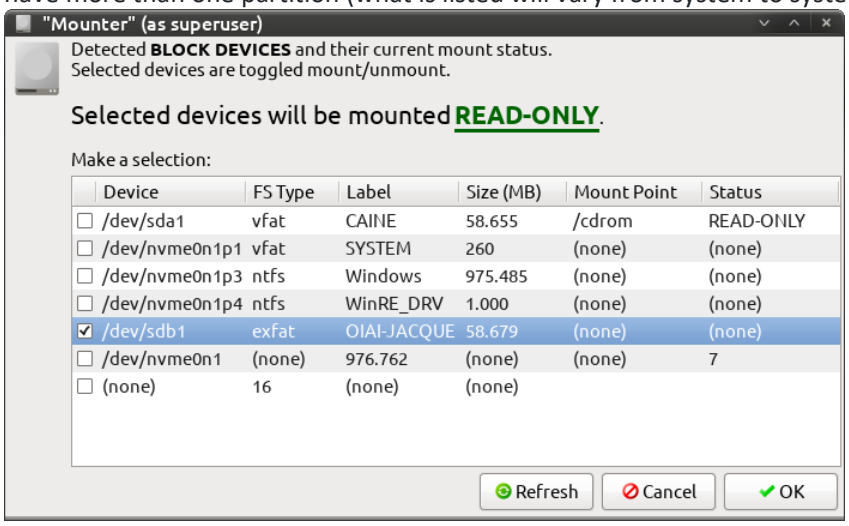
16. Note the date/time and time zone and compare it to the date/time and time zone where you are. If they do not match, return to step 13 to re-configure the date/time.
17. Once you have it properly configured, note it in your notes and photograph the screen. If you are unable to configure it correctly, photograph it, and make a note of the displayed date/time and time zone along with the actual date/time and time zone where you are located.

CONNECTING AND MOUNTING YOUR TARGET USB DEVICE

18. Connect the USB drive you will be using as the target for the image.
19. Mount the USB drive Read-Only by clicking on the drive icon with a green hue at the bottom of the screen around the middle of the status bar as indicated by the arrow in the image below.

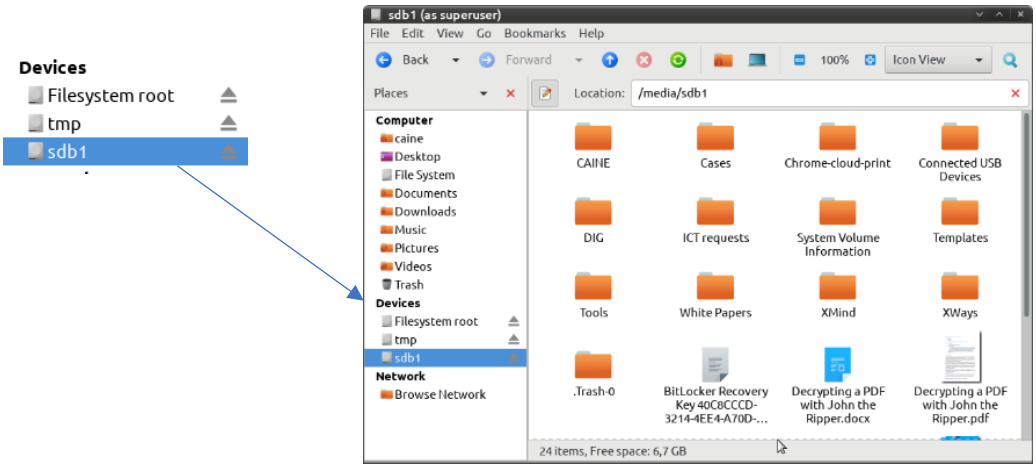


20. This will open the following screen which lists all available partitions, noting that a single drive can have more than one partition (what is listed will vary from system to system).

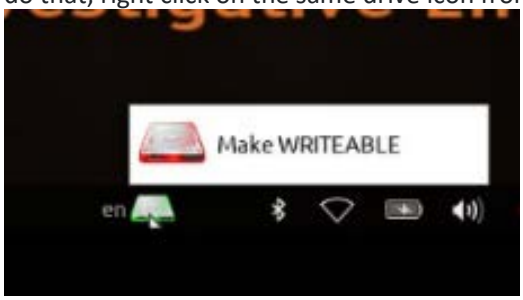


   a. In a typical setup you will see an internal NVMe (with several partitions) or mSATA drive, and your USB drives (CAINE and destination one). Above we see /dev/nvme0n1 and three partitions (p1, p3, p4). That is the internal drive. If you see two unique /dev/nvme0n#, or another drive in addition to the NVMe and the two USBs, either something else is connected to the laptop, or there is a second internal drive (which some laptops will have).
      i. Notify the forensic examiner if you see more than the single NVMe and the two USBs (or one USB if you booted CAINE in RAM and removed it to plug the destination drive).
   b. Your USB devices will most likely be /dev/sda1 and /dev/sdb1. In the screenshot above we see that /dev/sda1 is CAINE, and it's already mounted Read-Only. Note that /dev/sdb1 is the destination drive in this case. You should recognize the label as being the volume name you gave the drive when you formatted it.
      i. **NOTE**: If the laptop has a mSATA drive, it will be /dev/sda. CAINE will be /dev/sdb1, and your USB destination drive will be /dev/sdc1.
   c. As in the screenshot, click on the checkbox for the USB drive you wish to mount Read-Only (your destination drive), and then click **OK**.
21. Open the file explorer (Caja-Root on the desktop).

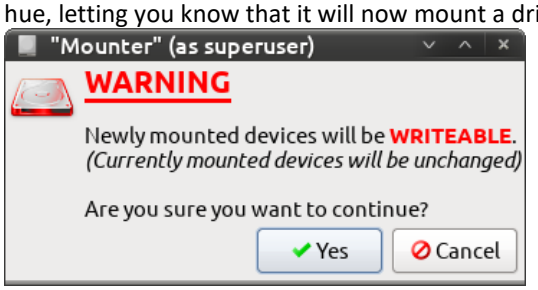
22. Navigate to the newly mounted USB drive. It will be mounted at /media/sdb1 (if you mounted /dev/sdb1), but you should also see it listed under “Devices” in the left pane of the file explorer.



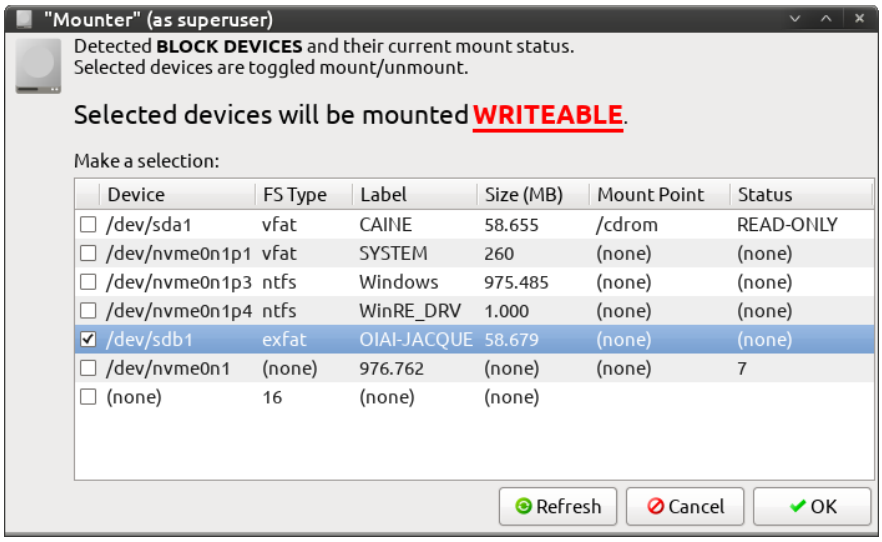
23. In the above example we see several files/folders on the USB drive. In your case, it will normally be a blank/newly formatted drive so you should see no files there. This step is to safely confirm which is our destination drive (/dev/sdb1 in this case) before we mount it Read-Write. We do this so that we don’t accidentally mount Read-Write a partition that is evidence and cause changes to it.
24. Unmount the partition by clicking on the eject icon ⏏ in the file explorer located to the right of the partition listed under Devices.
25. If the partition you mounted was not your USB destination drive, return to step 19 to mount another partition until you safely identify the one that is your USB destination drive. Once you’ve properly identified your destination drive, continue to the next step.
26. Now we want to mount the partition Read-Write, as we will be writing the forensic image to it. To do that, right click on the same drive icon from step 19 and choose to Make Writable.



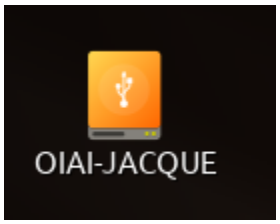
27. You will get a warning prompt. Click on Yes. This will now change that icon from a green hue to a red hue, letting you know that it will now mount a drive Read-Write rather than simply Read-Only.



28. After you’ve clicked on Yes in the previous step, click on the drive icon at the bottom that is now read instead of green. You will see a very similar window to earlier but note that now it’s letting you know it will mount your selection as writable.



29. Click on the checkbox for the partition you identified earlier as your destination partition (/dev/sdb1 in my case) and click on OK. You should now see an icon appear on your desktop showing the drive is available. It will have the volume name as the name of the drive.



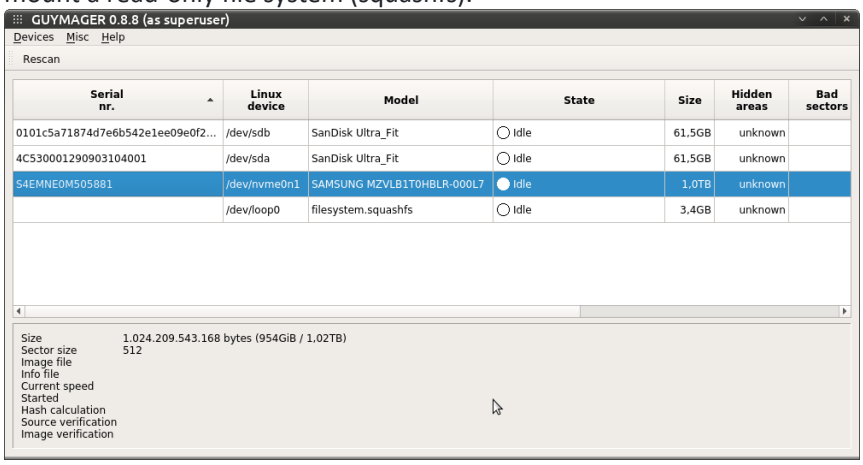
30. If you mounted the incorrect one, make note of the one you did mount (important to document potential changes you may have made), and then right click on the icon and eject it, then go back and mount the correct one. You can always right click on the drive icon at the bottom (now with the red hue) to switch it back to Read-Only if you need to go back to step 19 to safely figure out which one is your destination drive for the forensic image.
31. Congratulations! Your destination drive is now ready to receive the image. You can move on to imaging now.

IMAGING THE INTERNAL DRIVE(S)

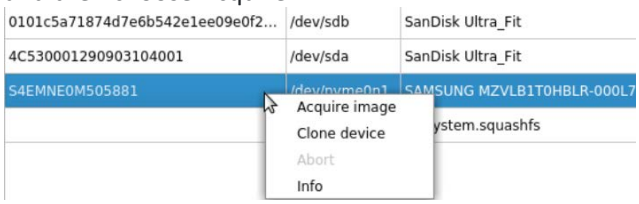
32. Launch Guymager (Menu, Forensic Tools, Guymager).

33. You should now see physical devices (not all the partitions on each device). In this scenario we see /dev/sda (CAINE as we saw in this example) on a 64GB SanDisk Ultra_Fit drive, /dev/sdb (our destination drive as we saw earlier in this scenario) which is another 64GB SanDisk Ultra_fit drive,

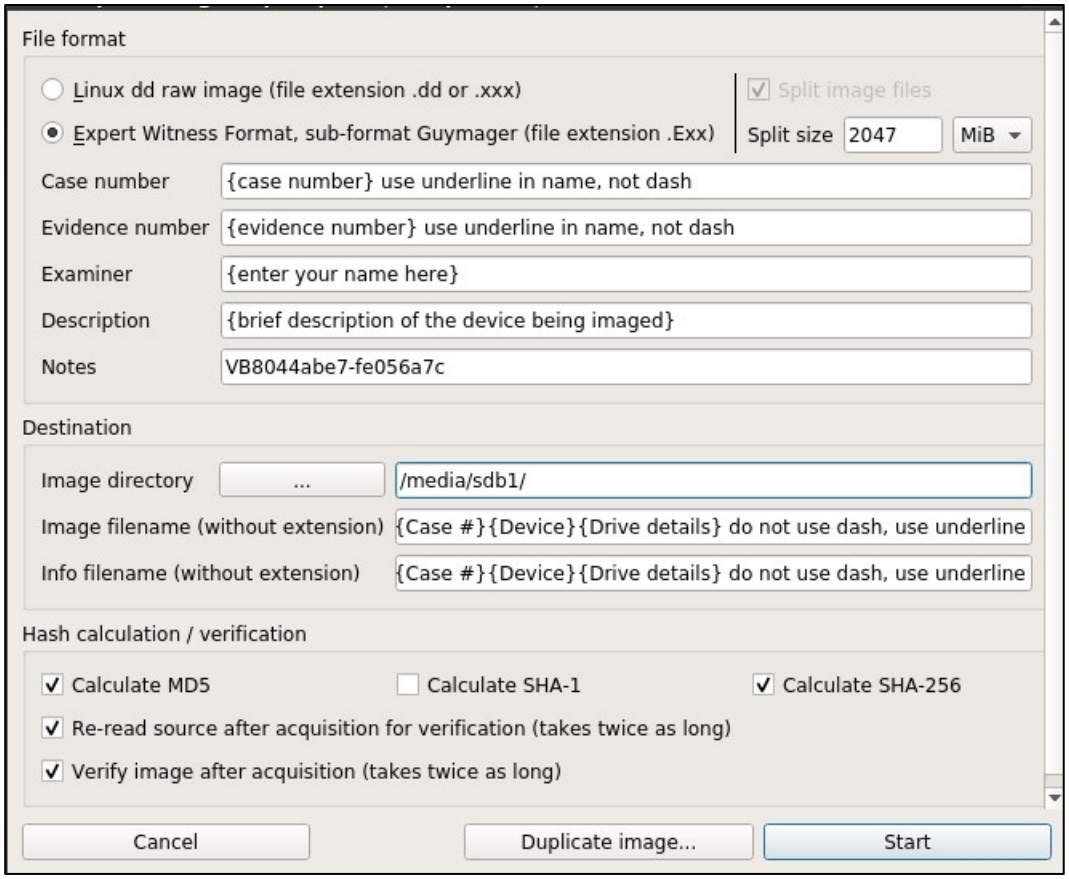
and /dev/nvme0n1 (a 1.0 TB Samsung drive), the internal hard drive in this example. You will also see /dev/loop0. You can ignore this, as it's not a physical drive. It's used as part of the live distro to mount a read-only file system (squashfs).



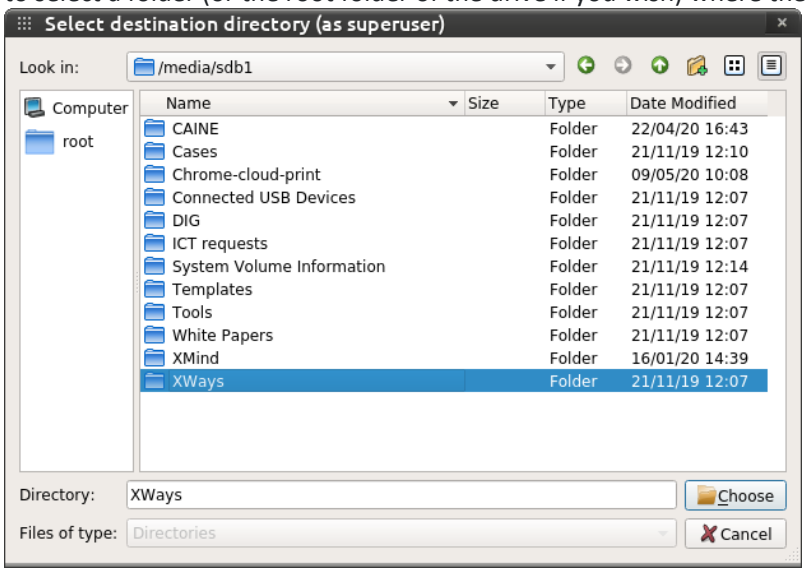
34. Right click on the internal hard drive (/dev/nvme0n1 in the above example) which will present you with a context sensitive menu giving you the option to acquire that drive you've right clicked on, clone it, or get more info on it. Info will give you way more information than you need, but feel free to click on it if you want to have a look at it. Then return to the above screen and right click again, and then choose Acquire.



35. You will now be presented with a screen where you need to fill out information about the acquisition. Some of this info will be saved in an info file along with the image files. You can leave the default Expert Witness Format, and the split size. The forensic examiner assisting you will provide you with the
    a. Case number and Evidence number
    b. Put your name under Examiner.
    c. Add a description, and notes.
    d. The Destination section will be covered in the next step.
    e. In the hash calculation/verification section, check off (if not already checked off):
        i. Calculate MD5
        ii. Calculate SHA-256 (not SHA-1)
        iii. Re-Read source after acquisition
        iv. Verify image after acquisition



36. Under Destination, you need to click on the ellipse (…) button and navigate to your destination USB drive. Note it will be under /media/sdb# (sdb1 in this example). You can create a folder from the file browsing interface if you wish to store the image in a sub-folder. You will want to do this if you have other content on this drive to keep things organized. In the screenshot example below, you see many folders listed, because the drive used in this example was not a blank drive. In your case you should see nothing under /media/sdb# as it's recommended you use a blank drive. Click on Choose to select a folder (or the root folder of the drive if you wish) where the image will be saved.



37. Finally, you need to give the image a file name, and the info file a file name. The screenshot below provides a suggested nomenclature for each, but your forensic examiner will likely tell you how to name these files. If they do not, feel free to use the suggested nomenclature. If it was case 2020-1234, and you were imaging a 1TB Samsung drive in Jacques Boucher's laptop, it could look something like:
    a. 2020_1234_Jacques Boucher laptop_Samsung 1TB NVMe
    b. You can copy/paste the name you put under the image file name to use the same for the info file. They will have different extensions so no need to worry about overwriting.

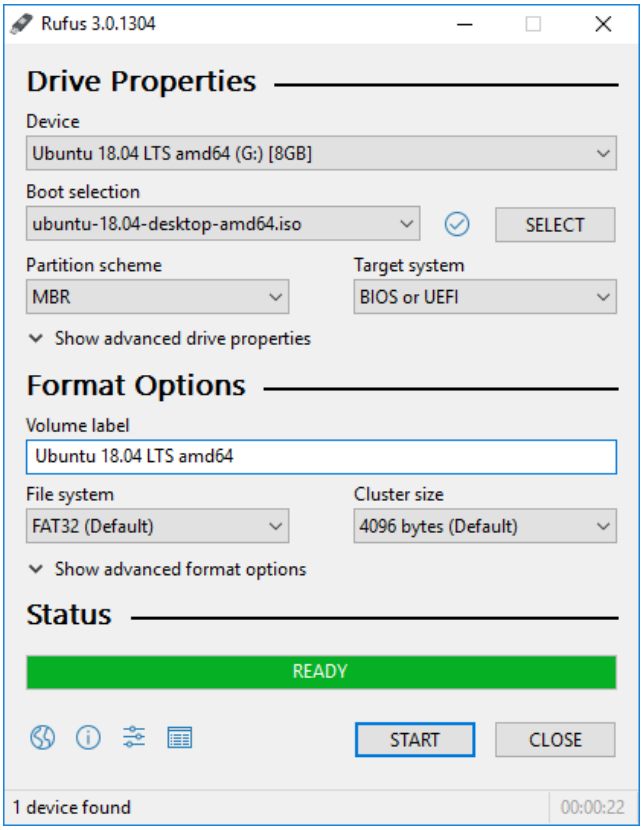
38. Click on the Start button at the bottom of the acquire screen and imaging will start.
39. You are done for now. The drive will now image. How long it takes will vary depending on the size of the drive in the laptop, the speed of that drive, the speed of your USB device, and the processing power of the laptop. A 512 GB drive will likely be done in about 2 hours.
40. Once it's done, document the results and leave it on screen in case the forensic examiner wants to see it by having you share video with them during a video call.
41. Once the forensic examiner has confirmed that the image is good, she/he will instruct you how they want the image delivered to them (mailing the destination drive or uploading to a corporate share).
42. Secure the laptop and the USB drive with the image and make note of the date/time you secured it, and where you secured it (e.g. personal locked desk or office).
43. Do not delete the image from the USB drive until such time as the forensic examiner tells you it's OK to do so. And do not return the laptop to service yet. This is usually done after the forensic examiner has confirmed that they received the image, and that it validated correctly.
44. Once everything validated, the forensic examiner will advise you if you can return the laptop to service, or if they wish to keep it as evidence. Same for the image, if they require it, they will have you preserve it and ship it to them along with the laptop if requested. If they do not require the copy you made, they will instruct you to wipe that key (hence why it's recommended to use a blank one).

RETURNING LAPTOP TO SERVICE

45. **If** the forensic examiner has authorized you to return the laptop to service, you will need to re-enable secure boot if you had to initially disable it. Then boot up the laptop to ensure it is working correctly. If it prompts you for a BitLocker recovery key, you will have to obtain it from IT. Once the laptop boots up correctly, it can be returned to service (or returned to the pool if the individual was issued a replacement when this one was taken).

APPENDIX A –CREATE A BOOTABLE USB

The free utility Rufus (http://rufus.ie/) is a suitable tool to create a bootable USB key.



1. Select the device from the first pull down menu. The device is the USB key onto which you will be installing CAINE.
2. Select the CAINE ISO by clicking on "SELECT" and navigating to the ISO image.
3. Partition scheme: MBR
4. Volume Label: CAINE
5. File system: FAT32 (Default)
6. Cluster size (4096 (Default)

Once all the options are selected, the READY bar at the bottom will change from grey to green.

Click on START to begin creating the bootable USB drive.

APPENDIX B – SECURE BOOT

Secure boot will stop you from booting a USB drive with a non-Microsoft OS on it. If you disable secure boot on a BitLocker encrypted drive, you will be prompted for the BL Recovery key when you reboot into the OS on the system drive.

*****If Secure Boot needs to be disabled, it's important to have the BitLocker recovery key in order to recover after turning off secure boot and trying to boot into the OS of the device. Without the recovery key, you will not be able to boot back into the laptop.**

If you are unsure if BitLocker is enabled or not, refer to **Appendix D – Checking for BitLocker**.

APPENDIX C – FAST BOOT

If the device uses FastBoot, it doesn't shut down, but rather goes into hibernation when you "shut down" the device. Because of this, when rebooting the device and either trying to get into the BIOS or booting from a USB, it will fail and boot to the OS.

To get around this, you need to do a full shutdown of the device. This can be accomplished by holding down the shift key while clicking on Shutdown. Once the device starts shutting down, you can release the shift key.

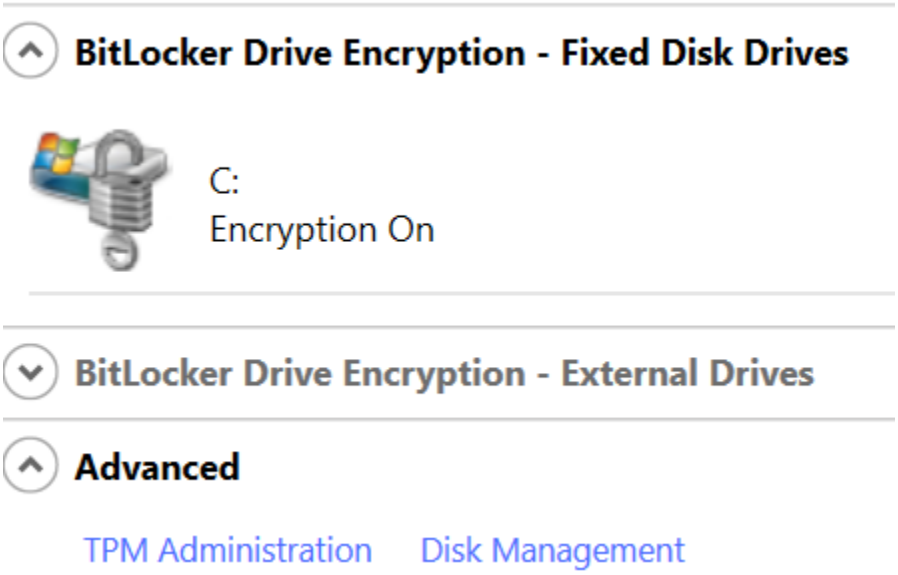
If you boot to the OS of the laptop by accident due to Fast Boot or for any other reason, make note of the date/time it happened, and do a full shutdown as noted herein. Booting into a laptop will cause changes to some of the content of the drive, hence why it's important we note each time it happens so that we can account for any artefacts arising from our interaction with the device.

APPENDIX D – CHECKING FOR BITLOCKER

From the command line (as administrator): manage-bde -status

In PowerShell (seem to need admin rights): Get-BitLockerVolume

Via GUI - Control Panel (can be done without admin rights): BitLocker Encryption Options



APPENDIX E - TROUBLESHOOTING

Linux commands you may be instructed to run as part of troubleshooting steps.

1. List all devices
    a. ls /dev/*
        i. List all devices in /dev folder.
    b. sudo lsblk
        i. List all block storage devices.
2. Check what partitions are mounted
    a. sudo mount
3. File System Layer Tools
    a. sudo fsstat
        i. "Shows file system details and statistics including layout, sizes, and labels."[1]
4. Volume System Tools
    a. sudo fdisk -l
        i. Displays partition layout of a disk.
    b. sudo df -h
        i. Displays mounted volumes and space available on them in human readable format.
    c. sudo mmls
        i. "Displays the layout of a disk, including the unallocated spaces."[2]
    d. sudo mmstat
        i. "Display details about a volume system (typically only the type)."[3]
5. Disk Tools
    a. sudo disk_stat
        i. Checks if an HPA exists.
    b. sudo disk_sreset
        i. "Temporarily removes the HPA if one exists. After the disk is reset, the HPA will return."[4]
6. Guymager commands
    a. sudo guymager EwfCompression=BEST
        i. Will launch guymager using BEST compression instead of the default, FAST, as specified in the guymager config file at /etc/guymager/guymager.cfg. According to the config file, using BEST will normally only achieve slightly better compression than FAST, but it will be much more demanding on the CPU. The author of guymager does not recommend using BEST, but the option is available if a reduced image size is what is most important.

[1] https://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview
[2] https://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview
[3] https://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview
[4] https://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview

APPENDIX F – PRINTABLE CHECKLIST

EQUIPMENT REQUIRED

1. ☐ USB key (16 GB or larger) (USB 2.0 or better is fine)
2. ☐ USB hard drive (size depends on the size of the drive being imaged)

OPTIONAL EQUIPMENT

3. ☐ USB hub (only required if the laptop being imaged only has 1 USB port)

CREATING BOOT DEVICE

4. ☐ Download CAINE from https://www.caine-live.net/ and create a bootable USB drive with it. See "**Appendix A –Create A Bootable USB**" for instructions.

NOTE TAKING

5. It is imperative that you keep detailed notes of your actions, including the date/time you took the actions.

PREPARE TARGET LAPTOP/PC

6. ☐ Go into the BIOS and check for Secure Boot - See "**Appendix B – Secure Boot**" to check and deal with Secure Boot.
7. ☐ See "**Appendix C – Fast Boot**" to deal with FastBoot.
8. ☐ Note the date/time in the BIOS vs actual date/time

BOOTING TARGET PC WITH CAINE

9. ☐ Connect the CAINE USB key.
10. ☐ Boot the laptop. As the laptop boots, press the appropriate key to change the boot device and select to boot from CAINE.
11. ☐ If you only have one USB port on the device, choose the option to boot CAINE into RAM. If you have at least 2 USB ports, you can hit ENTER to select the default boot option.
12. ☐ Once CAINE is booted, connect the USB drive you will be using to store the forensic image.

DATE/TIME AND TIME ZONE

13. ☐ Configure the date/time and time zone to local time.
14-16. ☐ Verify the date/time and time zone and compare it to local time.
17. ☐ Note/photograph the date/time and time zone.

CONNECTING AND MOUNTING YOUR TARGET USB DEVICE

18. ☐ Connect the USB drive you will be using as the target for the image.
19-20. ☐ Mount the USB drive Read-Only
21-23. ☐ Confirm that the mounted partition is your external USB drive.
24. ☐ Unmount the partition.
25. ☐ If the partition you mounted was indeed your external USB drive, continue to the next step. If it was not the correct one, return to step 19.
26-29. ☐ Remount the same partition, but this time Read/Write.

30. ☐ If you mounted the incorrect one, make note of the one you did mount (important to document potential changes you may have made), and then right click on the icon and eject it, then go back and mount the correct one. You can always right click on the drive icon at the bottom (now with the red hue) to switch it back to Read-Only if you need to go back to step 19 to safely figure out which one is your destination drive for the forensic image.
31. Congratulation! Your destination drive is now ready to receive the image. Continue to the next step.

IMAGING THE INTERNAL DRIVE(S)

32. ☐ Launch Guymager (Menu, Forensic Tools, Guymager).
33. ☐ Confirm that you can see the laptop's internal hard drive in the list.
34. ☐ Right-Click and choose "Acquire image".
35. ☐ Complete the fields as directed in this guide.
36. ☐ Select the destination where the image will be saved (USB drive you mounted Read/Write in steps 26-29).
37. ☐ Enter the file name and info file name as directed in this guide.
38. ☐ Click on the Start button at the bottom of the acquire screen and imaging will start.
39. ☐ You are done for now. The drive will now image. How long it takes will vary depending on the size of the drive in the laptop, the speed of that drive, the speed of your USB device, and the processing power of the laptop. A 512 GB drive will likely be done in about 2 hours.
40. ☐ Once it's done, document the results and leave it on screen in case the forensic examiner wants to see it by having you share video with them during a video call.
41. ☐ Once the forensic examiner has confirmed that the image is good, she/he will instruct you how they want the image delivered to them (mailing the destination drive or uploading to a corporate share).
42. ☐ Secure the laptop and the USB drive with the image and make note of the date/time you secured it, and where you secured it (e.g. personal locked desk or office).
43. ☐ Do not delete the image from the USB drive until such time as the forensic examiner tells you it's OK to do so. And do not return the laptop to service yet. This is usually done after the forensic examiner has confirmed that they received the image, and that it validated correctly.

RETURNING LAPTOP TO SERVICE

45. ☐ **If** the forensic examiner has authorized you to return the laptop to service, you will need to re-enable secure boot if you had to initially disable it. Then boot up the laptop to ensure it is working correctly. If it prompts you for a BitLocker recovery key, you will have to obtain it from IT. Once the laptop boots up correctly, it can be returned to service (or returned to the pool if the individual was issued a replacement when this one was taken).

If you printed and used this checklist, initial the first page, and sign the second page. Include the date & location. Provide a scanned copy to the digital forensic examiner for their file along with a copy of your notes.

_____ _____ _____

(Signature) (Date) (Location)

REVISION HISTORY

July 2020	Initial release
December 2020	• Added title page and ToC • Minor grammatical corrections. • Added paragraph 21.b.i to note what a user will see if a laptop has a mSATA drive instead of an NVMe. • Added "Appendix E - Troubleshooting" o #1-5
February 2021	• Added "**Appendix A –Create A Bootable USB**"on how to create a bootable USB drive. • Other Appendix were renumbered from B to E. • Yellow highlight emphasis added in "**Appendix B – Secure Boot**" to draw attention to the fact that the BitLocker Recovery key will be required if Secure Boot needs to be disabled. • Removed the step to change boot sequence in BIOS, as that is not necessary since we control the boot sequence later. • Added checkbox for "Re-read source" for step 35.e.iii • Minor grammatical corrections.
March 2021	• Added paragraph 1.b in "**Appendix E - Troubleshooting**" • Added paragraph 4.b in "**Appendix E - Troubleshooting**" • Added paragraph 6 in "**Appendix E - Troubleshooting**" • Updated the acquire screenshot in step 35.e. • Added "**Appendix F – Printable Checklist**" • Minor grammatical corrections.