CCSI460 Forensic Lab Report

**Investigator’s Name:** *Matt Ferry*

**Date of Investigation:** *September 8, 2013*

**Lab Number and Title:** 1 Survey of Forensic Toolkits

**Summary of Findings:**

All of the links provided go to forensic software packages that are readily available for use by the computer forensics industry. I was aware of Sleuthkit/Autopsy, FTK, and Encase, but did not know about STD and Helix

I particularly like that there are at least two open source packages available Sleuthkit /Autopsy and STD, although STD is more of a Linux live distribution than an individual software package.

In regards to these programs uses in the corporate world, I would think that because Sleuthkit/Autopsy, STD are free to use, that these software packages would be a great launching point for a small business or independent investigator that cannot afford the costs of FTK, Encase, or Helix. A larger corporation can afford FTK, Encase, and Helix. The use of these programs not only provide stronger features and more product support, but they will also allow investigators to be more consistent with the work and reports that are produced, increasing the viability and credibility of those reports as these software packages are widely used and therefore trusted as accurate.

At a minimum Encase costs approximately $3,000 plus a one year Software Maintenance[[1]](#endnote-1) Service plan, and both FTK and Helix Enterprise only offer options for calling for a quote, which indicates that their costs are just as costly as Encase if not even more.

A couple of things to note about FTK and Helix is that they each offer separate products for “Live Response” or the capturing of volatile data. FTK’s version does not list the price, but Helix’s Live Response software is $500[[2]](#endnote-2).

The company behind the Helix software package also offers what I would call a hook package, in that they offer a particular version of their software for free[[3]](#endnote-3) (although this option is not as prominent, it is near the top of the page). This free software is not updated or supported by Helix developers in any way, but allows them to get their foot in the door. Once users of the software see exactly what the software is capable of doing, and since they are already using the Helix software they will be more likely to purchase/upgrade to the full version of Helix.

In specific regards to STD, while this would still be a good distribution to download and have as part of your software repository for use on older computers, it no longer appears to be being developed. As far as I can tell, the last official release was back in 2004, which means that the software packages in the release are more than likely going to be severely out of date. An alternate live CD option for forensic purposes might be Kali[[4]](#endnote-4), which is a newer version of Backtrack[[5]](#endnote-5), which is actively being maintained and developed.

Kali can also be configured to act as security/forensics workstation, or it can be configured as a Linux live cd while STD was only ever meant to be a Live CD, and never as a full Linux distribution. The Kali Live CD also has a boot option that is specifically labeled for “Forensic Mode”[[6]](#endnote-6), which is in contrast to STD. While STD can be used for forensics work, there is no clearly defined “Forensics Mode” outside of part of STD’s FAQ section where it says “[forensics folks note that you need to boot with the 'noswap' option to NOT touch an existing Linux swap partition.]” [[7]](#endnote-7).

Out of these software packages, I would use either Encase or FTK because they also offer software certifications that are specific to their software packages. Helix offers “training” as well, but based on what I am seeing in their website those training classes do not directly translate into certification (If it did I would think that that would be clearer)[[8]](#endnote-8). I would also use Sleuthkit /Autopsy, and a Kali Live CD/ Boot device, and potentially a full Kali install on a machine (or virtual machine). By using these particular software packages, you will have access not only to recognized and supported software that is used within the industry, but you will also have access to multiple tools that are capable of verifying the results of any work that you perform, which means you are also verifying the accuracy and validity of your work.

I have also successfully downloaded and installed FTK 1.81.6

**Details of the Investigation:**

September, 4 2013

 1:00 PM – Performed research on the requested programs and wrote the report for the above summary section.

September 8, 2013

 11:51 AM – Reviewed and revised the summary report.

1. <https://www.encase.com/Pages/EnCaseForensicConfirmation.aspx> [↑](#endnote-ref-1)
2. <https://www.e-fense.com/store/index.php?_a=viewProd&productId=4> [↑](#endnote-ref-2)
3. <https://www.e-fense.com/products.php> [↑](#endnote-ref-3)
4. [http://www.kali.org](http://www.kali.org/) [↑](#endnote-ref-4)
5. <http://www.backtrack-linux.org/> [↑](#endnote-ref-5)
6. <http://linux.softpedia.com/progScreenshots/Kali-Linux-Screenshot-97645.html> [↑](#endnote-ref-6)
7. <http://s-t-d.org/faq.html> [↑](#endnote-ref-7)
8. <https://www.e-fense.com/training/index.php> [↑](#endnote-ref-8)