## D34 Comparative Analysis of Computer Forensics Software on IBM Compatible and Macintosh Media

*Ismail M. Sebetan, MD, PhD* and Gloria A. Stafford, MS, National University, Forensic Sciences Program, La Jolla, CA 92037; Luis Salazar, MS, Department of Justice, 110 West A Street, San Diego, CA 92101*

The goal of this presentation is to provide the forensic community with a sampling of the Computer Forensics software tools available for imaging and analyzing computer hard drives and storage media. The given information in this presentation will help Computer Forensic Examiners and others working in this field to gain knowledge of applications, advantage and disadvantage of three specific software programs researched during this study and help them determine which program may work best for their needs in searching for evidence of a crime.

This presentation will impact the forensic community and/or humanity by aiding the forensic community in understanding the different forensic software available and will help them choose the best software for their cases.

This study attempts to answers three important questions when choosing software tools: 1) Can the program recognize and therefore image a particular type of storage media? 2) Can the examiner view or execute the specified test files and documents either from within the program or with an external program? 3) Can the program recognize and therefore image a Macintosh formatted storage media? The programs evaluated, scored and then subsequently rated on the aforementioned criteria.

The results shown in the Tables 1 and 2 indicate the total number of test documents and files each program was able to open, view, or execute either from within the program or with an external program.

In conclusion the present study will provide a very useful guide for the suitable program choice and proper application of the forensics software.

**Table 1**

| | PC ZIP DISK | |
|---|---|---|
| **RATING** | **SOFTWARE TESTED** | **NUMBER OF OPENED FILES** |
| 1 | Forensic Toolkit (FTK) | 26 out of 26 |
| 2 | ProDiscover | 23 out of 26 |
| 3 | EnCase | 20 out of 26 |

**Table 2**

| | MACINTOSH ZIP DISK | |
|---|---|---|
| **RATING** | **SOFTWARE TESTED** | **NUMBER OF OPENED FILES** |
| 1 | EnCase | 7 out of 26 |
| 2 | Forensic Toolkit (FTK) | 5 out of 26 |
| 3 | ProDiscover | 0 out of 26 |

**Computer Forensics, Software Tools, Comparative Analysis**

 ** Presenting Author*