

## ABSTRACT

The use of software systems has played an integral role in DNA analysis for years. Recently, LIMS and expert systems have been validated and adopted into the workflow of forensic DNA laboratories. Audit trails are being introduced as part of the implementation of automation and advances in paperless systems. As DNA data analysis becomes more automated in processing, the evaluation of proper documentation and user tracking is essential. For quality assurance purposes, it is crucial that any changes an analyst makes to an allele call can be traced to the analyst who made it. When looking at software systems, security features such as analyst login, administrative control, and audit trails should also be evaluated to ensure they meet the laboratory's quality assurance requirements.

The NIJ Expert System Testbed (NEST) Project Implementation Team has evaluated several single source expert systems and mixture deconvolution tools including: DNA\_DataAnalysis Software (U.S. Army Criminal Investigation Laboratory, Fort Gillem, Georgia); FSS-i<sup>3</sup>TM Expert Systems Software version 4.2.2 (Promega Corporation, Madison, Wisconsin) in conjunction with GeneMapper® ID Software version 3.2 (Applied Biosystems, Foster City, California); GeneMapper® ID Software version 3.2 (Applied Biosystems); GeneMapper® ID-X Software version 1.1 (Applied Biosystems); and TrueAllele® Databank version 2.9 (Cybergenetics, Pittsburgh, Pennsylvania). All of these software systems offer different tracking and administrative control features. When launching the software, some systems have unique user login and password requirements, while other software programs require entering a user identification name at an alternate point during sample analysis. There are also programs that track the Windows® user login and associate that user with a data set imported into the software. These features may dictate which software program a laboratory chooses to implement into its workflow.

Audit trails document the time periods that the user is logged in, changes made by the user, and the rules that are fired, to name a few examples. Each software package reports different information in its respective audit trails. Another security level that was examined is the accessibility of settings to various users. Some software packages allow the administrator to limit access to custom settings, while others do not. For example, if the laboratory's quality assurance program states that only an administrator or a technical leader can modify settings and thresholds, access to these settings can be controlled in some software packages.

The intent of this poster is to inform the forensic community of the differences in security and audit features in single source expert systems and mixture deconvolution tools. The information presented in this poster may assist a laboratory in choosing not only a software program that meets its analytical needs, but its security needs as well. Comparisons between the software packages will be discussed, highlighting the benefits as well as possible areas for improvement for each program assessed.

## INTRODUCTION

As laboratories are becoming increasingly dependent on software systems for forensic DNA analysis, analysts and administrators should be cognizant of the associated quality assurance requirements, including the audit trails and security features offered both within the software applications and the operating systems. The emphasis on quality assurance is leading laboratories to choose software systems that will seamlessly integrate into their standard operating procedures and also have the ability to properly document user information and changes made to the analysis parameters. When gaps in documentation surface, it leaves the analyst vulnerable and could potentially devalue his or her case. Because of quality assurance considerations, the resulting software systems utilized for forensic DNA analysis have various audit trails and security features built into them. This research assessment project has been designed to inform the forensic science community about available software systems and the type of security and audit features each one offers.

A checklist was created by the NIJ Expert System Testbed (NEST) Implementation Team to encompass the most significant security and audit functions of each software system. Samples were processed through each system and, in addition to the checklist, detailed information was noted on unique security and audit features within each software system. Electronic signatures (e-signatures or eSig) used in software systems were also evaluated. Results from this study as they relate to the purchase of software for forensic DNA analysis will be discussed.

## MATERIALS & METHODS

### Data Collection

•86 samples and 10 controls were processed through each of the following software systems:

- DNA\_DataAnalysis Software
- FSS-i<sup>3</sup>TM Expert Systems Software version 4.2.2
- GeneMapper® ID Software version 3.2
- GeneMapper® ID-X Software version 1.1
- TrueAllele® Databank version 2.9.

- Security and audit trail features were recorded when encountered during sample processing.
- Output files were examined for security features.

## RESULTS

Table 1: Checklist of Security and Audit Features

SOFTWARE SYSTEM	Does the software ask for a user ID?	Does the software ask for a password?	As an administrator, do you have access to change ALL settings?	As a user, do you have security limitations to make changes?	When a change is made to an allele call, is an annotation required and/or available?	Do the output files track who made the changes?	Are the output files locked for editing?	Will the software "Time Out" if the computer remains on or in sleep mode?
DNA_DataAnalysis	✗	✗	✓	✗	✗	✗	✗	✗
FSS-i <sup>3</sup> ™	✗	✗	✓	✓	✓	✓	✗	✗
GeneMapper® ID	✓	✓	✓	✗	✓	✗	✗	✗
GeneMapper® ID-X	✓	✓	✓	✓	✓	✓	✗	✗
TrueAllele® Databank	✓	✗	✓	✓	✓	✓	✗	✗

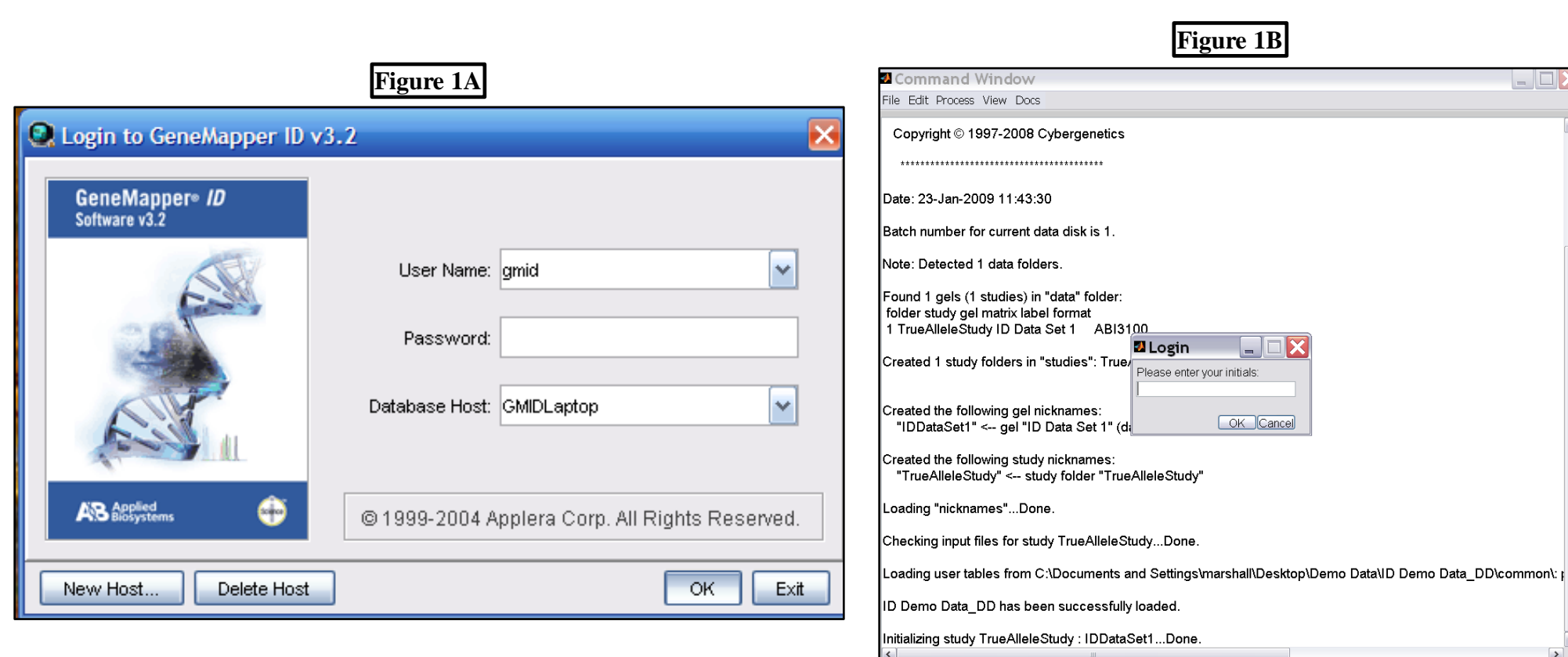


Figure 1A: Applied Biosystems requires a user to enter a specific User Name and Password to enter the GeneMapper® ID software. Without these, the software will not open. In GeneMapper® ID-X (not pictured), different security levels are accessible depending on the user name entered.

Figure 1B: When operating TrueAllele® Databank, a user's initials are required for those steps that allow changes to be made. In this figure, the box requesting the user's initials is required because the analyst is trying to view and edit his or her control samples in the Control Check window. Only approved user initials may be entered.

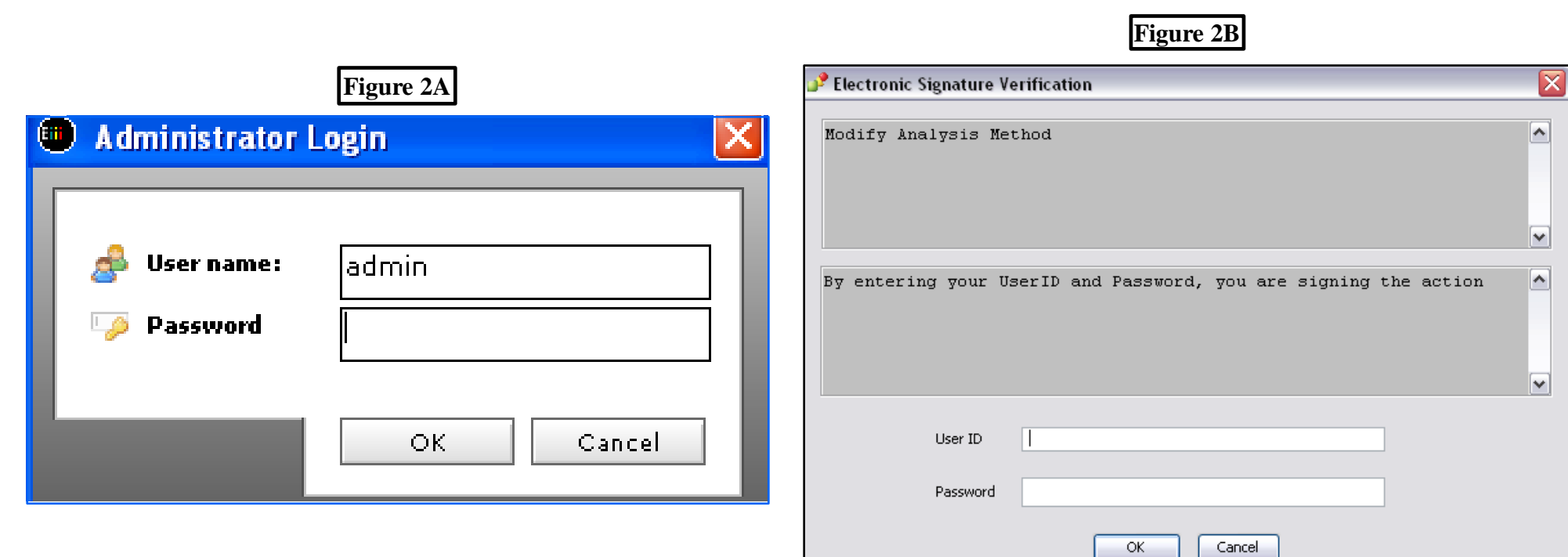


Figure 2A: Some software systems document access to different features for specific users as part of the audit trail. In FSS-i<sup>3</sup>TM, the administrator can make permanent changes to settings. Other users, such as the analyst, can be restricted to making changes to certain parameters.

Figure 2B: GeneMapper® ID-X has an integrated network of security access levels and tracking features. When the user tries to save a change to an analysis method, the Electronic Signature Verification window appears and requires a User ID and Password. The change will only be made if the user has permission to edit an analysis method. This change, as well as the user making it, is recorded in the eSig Administration Event Log.

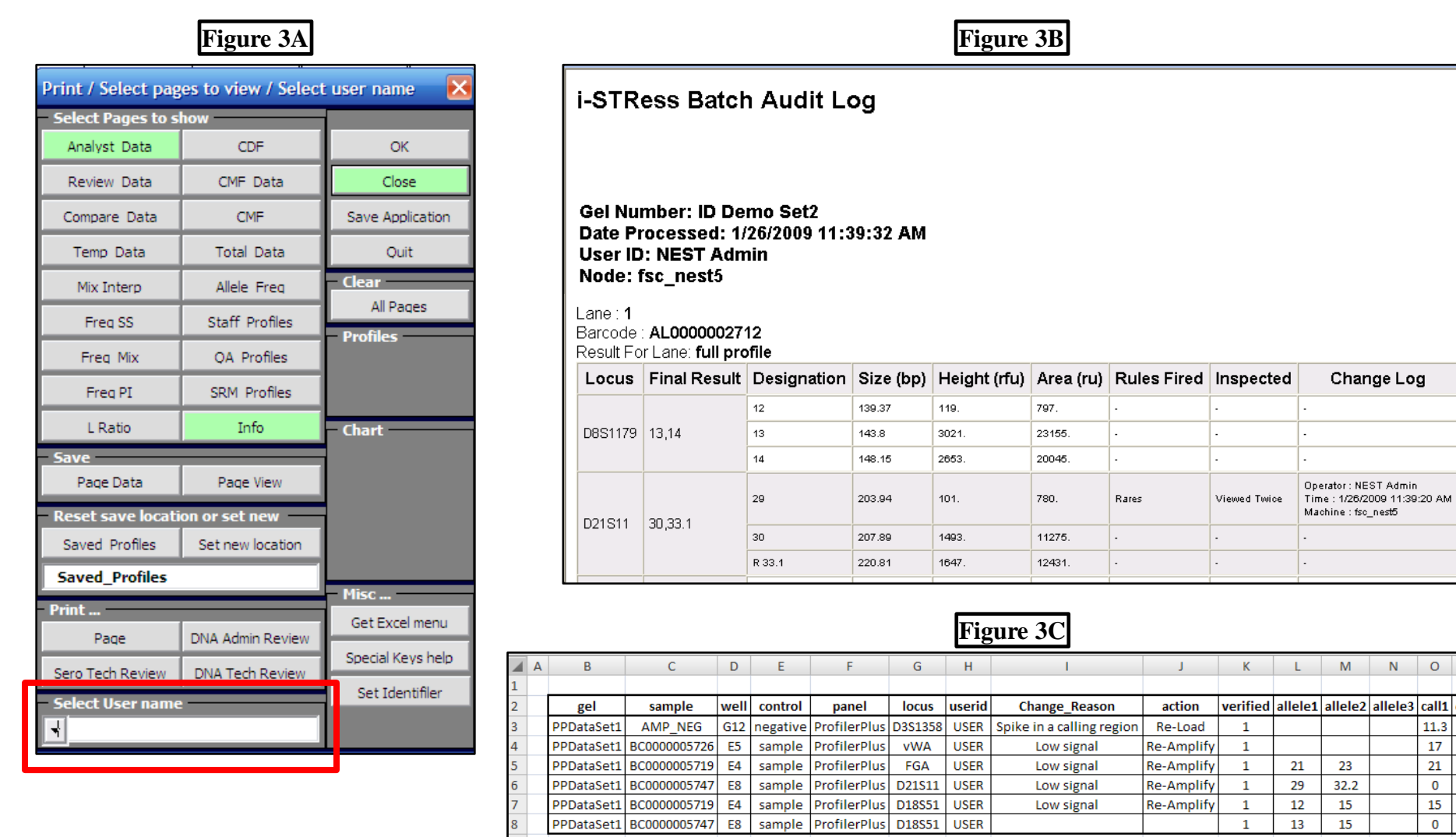


Figure 3A: DNA\_DataAnalysis allows for the entry of all users and their corresponding CODIS identification. When the user opens a printout, he or she can select his or her user name (highlighted in red box) which will be found in the header of all pages of the printout.

Figure 3B: FSS-i<sup>3</sup>TM Expert System Software allows a user to customize output files based on information and file type (text vs. HTML). In addition to output files, a number of audit files are automatically generated for each project analyzed. The i-STRESS Batch Audit Log reports information such as: a User ID, the computer used to analyze the project (Node), sample information (Barcode), final allele calls (Final Result), all peaks identified at each locus (Designation), Rules Fired, and Change Log.

Figure 3C: Audit and output files generated by TrueAllele® Databank are exported into text files. An "Edit" output file is shown. This file provides information such as: the sample number (sample), locus where an edit was made (locus), the user who made the edit (userid), and his or her reason for making the edit (Change\_Reason).

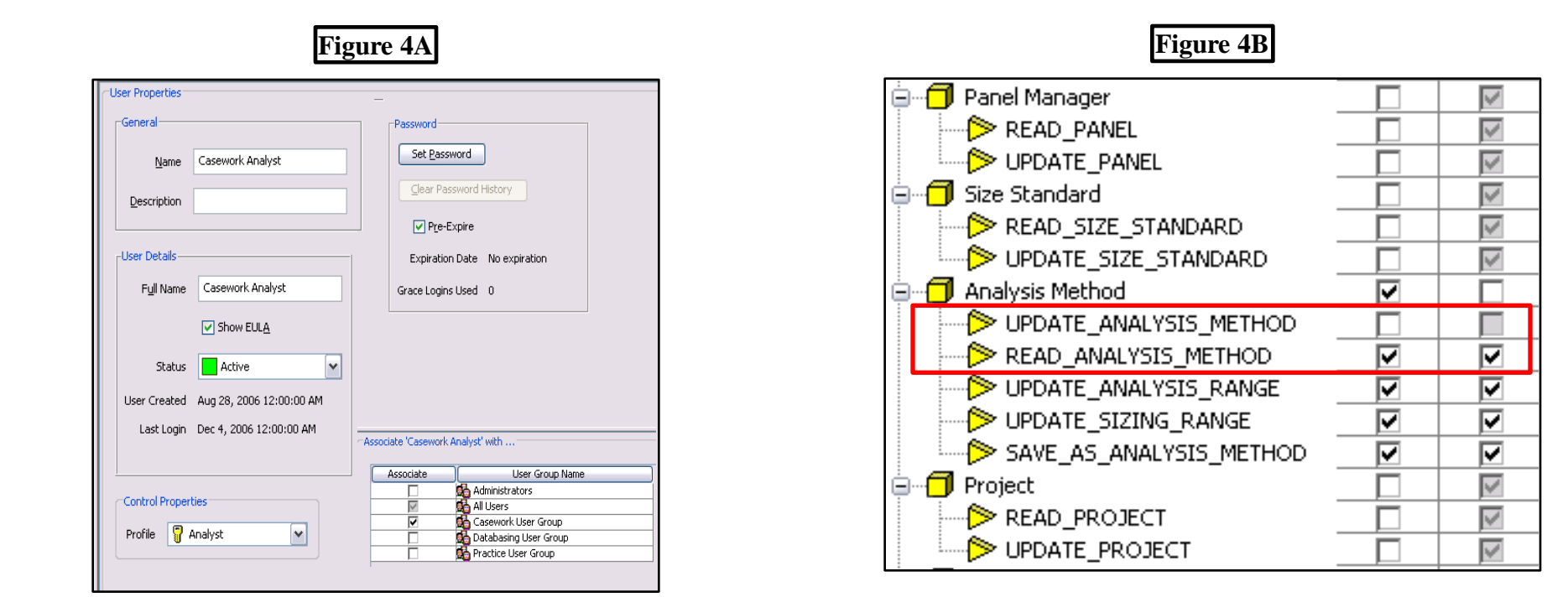


Figure 4A: GeneMapper® ID-X allows an administrator to create a unique profile for each scientist. In the User Properties window, the user's name and password are entered. The user is associated with one or more User Group Names and a profile is chosen.

Figure 4B: The GeneMapper® ID-X profile indicates what functions each user can perform. In this figure, the scientist has permission to read the analysis method, but does not have permission to update the analysis method.

## E-SIGNATURES

The forensic science community is making advances towards a paperless system. As this movement progresses, the idea of electronic signatures (e-signatures) has come to the forefront. At nearly every point during DNA analysis a computer software program is involved, especially during the final allele calling step. Laboratories are critically evaluating the currently available software to determine which security features they may need. One component to consider is e-signatures.

The U.S. Food and Drug Administration (FDA) has released a document addressing e-signatures (21 CFR Part 11). This document sets forth criteria for an e-signature, and under certain circumstances deems them "trustworthy, reliable, and generally equivalent to...handwritten signatures executed on paper" (U.S. Food and Drug Administration, 2008). As the forensic science community depends more and more on audit trails in data analysis to link analysts to changes, the need for similar regulations for e-signatures may arise. If enough security measures are implemented, then those signatures could be important for quality assurance purposes.

The expert systems and mixture deconvolution tools evaluated by the NEST Project Implementation Team have features that associate a user with a change to an allele call. There is variation between the software systems for e-signature designations. Some programs associate the user ID used at login with a change, while others actually have an e-signature window that appears when a signature is required. Each laboratory should evaluate the software system it is considering to determine if the e-signature function meets its needs. As this technology advances, the forensic science community should continually assess the security and audit features of software systems.

## DISCUSSION & CONCLUSIONS

Results of this study indicate that software systems designed for analysis of DNA sample data offer a wide variety of security and audit feature functions. A common feature found in most software systems is the accessibility of an administrator to change all settings. If the administrator has control of the settings, then changes in protocols and procedures in data analysis may be better managed. Our evaluation of the different software systems demonstrates a great deal of variation in the actions that require a user name or initials. Some systems ask for a user name and/or password to login to the software; other programs require the user's name or initials when performing a certain step in the process; and some do not require any identification of the user to be entered, but instead use the Windows® user login to associate changes to the data. Each of these software systems may suit a different laboratory setup. Laboratories should take this into consideration when purchasing a software system.

We identified two possible areas for improvement across all the software systems. When any software program evaluated was left for any length of time, it did not time out while the computer remained on or in sleep mode. It would be an added security benefit if, after a set length of time, the software would time out and would require reentry of the user name and password by the analyst. Also, it was determined that output files from all software systems could be edited. Some systems offer generation of HTML files rather than text files. While HTML files are more complicated to edit, it is still possible.

Every DNA laboratory has numerous standard operating procedures in place to ensure that each analyst follows the same protocols so that the results are reproducible to satisfy a quality assurance system. Security and audit features within DNA analysis software programs are important and useful to document the authenticity of results. Each user can track various aspects of the analysis, but ultimately the integrity of the analyst matters most. When determining which software system meets the needs of a specific laboratory, the analysts' and quality assurance requirements should be taken into account in addition to the security and audit features that the software offers.

## REFERENCES

U.S. Food and Drug Administration. "Electronic Records; Electronic Signatures," 21 Code of Federal Regulations Part 11, Title 21, Volume 1. 1 April 2008.

## ACKNOWLEDGEMENTS

The authors of this poster would like to acknowledge all members of the NEST Project Implementation Team for their support and assistance with this project, specifically Chuck Heurich, Program Manager to the NEST Project.

This project was supported by Award No. 2007-MU-BX-K008 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice to the Forensic Technologies Center of Excellence (FTCoE) administered by the National Forensic Science Technology Center. Marshall University Forensic Science Center is a partner with the FTCoE as the host site of the NEST Project.

The opinions, findings, and conclusions or recommendations expressed in this presentation are those of the authors and do not necessarily reflect those of the Department of Justice.