Usability of Forensics Tools: A User Study

Hanan Hibshi
Carnegie Mellon University
Pittsburgh, PA,USA
hhibshi@andrew.cmu.edu

Timothy Vidas
Carnegie Mellon University
Pittsburgh, PA, USA
tvidas@cmu.edu

Lorrie Cranor
Carnegie Mellon University
Pittsburgh, PA, USA
lorrie@cs.cmu.edu

Abstract

Digital forensics has become a critical part of almost every investigation, and users of digital forensics tools are becoming more diverse in their backgrounds and interests. As a result, usability is an important aspect of these tools. This paper examines the usability aspect of forensics tools through interviews and surveys designed to obtain feedback from professionals using these tools as part of their regularly assigned duties. The study results highlight a number of usability issues that need to be taken into consideration when designing and implementing digital forensics tools.

Index Terms

Usability; Digital Forensics; Forensics; GUI; User Interface.

I. Introduction

Digital forensics tools play a critical role in providing reliable computer analysis and digital evidence collection to serve a variety of legal and industry purposes. These tools are typically used to conduct investigations of computer crimes by identifying evidence that can be used in a court of law. In addition to criminal investigation, these same tools are used for purposes of maintenance, debugging, data recovery, and reverse engineering of computer systems in private settings. Digital forensics (or "computer forensic") is rapidly becoming a substantial part of computer investigations all over the world, used by both law enforcement and private sector investigators.

Digital forensics tools are designed for use by forensics investigators. It is important to consider the background, computer expertise, workflow, and practices of these users. In practice, users might have any level of an IT background ranging from a veritable computer security expert to a criminal investigator possessing minimal computer skills. With this diverse range of computer expertise, practitioners need "usable" tools that will help them get results easily.

Humans prefer to focus on specific tasks for a finite amount time to achieve certain goals. When interrupted with distractions, individuals tend to become confused or complacent, and become distracted from their main goal [1]. In digital forensics, when examiners (or practitioners) conduct an investigation, they are typically seeking answers to specific questions they have in mind. Practitioners often do not care about any underlying technical details that will shift them away from their two main goals: investigative leads and conviction support. Even when giving testimony in court, practitioners may claim to be a certified tool user instead of an expert that understands how a tool works [2].

We have conducted a study to obtain feedback from users that interact with digital forensics tools on a daily basis. The rest of the paper is organized in the following manner: Section 2 contains background and related work. Our methodology is described in detail in Section 3, followed by the results in Section 4. Finally, we present our conclusions and future work in Section 5.

II. Background & Related Work

Usability is becoming a critical aspect of any technical product. The international standard ISO 9241-11 defines usability as: "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [3]. Usability of computer systems is considered an important area of research and is often a metric used to evaluate systems. Therefore, usable security is emerging as a strategic research area. The field of usable security aims to apply computer security metrics in a user-friendly fashion. The research in this area interests academia as well as professional practitioners; and serves government institutes as well as private organizations [4].

In the past 30 years, digital forensics has matured from a very ad-hoc, and possibly destructive, use of system administration tools to formal processes utilizing dedicated tools. Technological advances in court cases have created a need for dedicated digital forensics tools. Today these tools can be used to make best-evidence duplicates and perform non-destructive analysis. Contemporary analysis can recover deleted files, construct event timelines, attribute events to users, and much more. The American Society of Crime Laboratory DirectorsLaboratory Accreditation Board (ASCLDLAB) "recognized digital evidence as a full-fledged forensic discipline" in 2003 [5]. Moreover, the interest in training and education has grown causing a wide number of universities and training organizations to offer a range of computer forensics courses and degrees where students can gain in-depth expertise in the field of digital forensics [6], [7].

Users of digital forensics tools need to become very familiar with the tools to be able to use them efficiently. In order to make sense of the information these tools provide, users may need to attend professional training [6], [7]. As digital forensics is sufficiently difficult to understand, it has been suggested that it be taught as part of university curriculum[7]. Another reason many feel digital forensics should be incorporated into the university is that it generally requires book-length training materials in order to teach people how to use forensics tools. A 2005 Metropolitan State University study surveyed computer forensics higher-education programs in the US and concluded that computer forensics is a"growing multi-disciplinary field with increasing industry demand" [6].

Reith et al. propose an abstract model as a possible replacement for existing forensic models that were deemed too specific. The authors further observe that existing digital forensics tools are typically too technology specific in a way that tends to become an inconvenience for non-technical users. Such users have typically been trained to use a particular tool, but may not have any foundational education about the underlying technology employed by the tool [8].

Modern digital forensics tools use many specific, complex technologies. For example, modern tools must support a plethora of complex file systems. This complexity led to the creation of specialized classes [9] and books dedicated to the subject [5]. Even though the objective of these classes and books is to provide a technical foundation for forensics examiners to better use their tools, these information sources focus on very low-level topics that are commonly ancillary to an investigator.

Garfinkel discusses trends in forensics research and observes that the field is likely "to fall-behind" in the near future. Current forensics tools were designed in an "evidence-oriented" fashion. The author further explains that this way of designing digital forensics tools has created some of the challenges that users face today. Examples include: slow speed, inability to find non-ordinary information, lack of smart reporting functionality, and inability to construct a timeline that helps investigators in their analysis. These are a few of the problems explored by the author that cause investigators to perform some essential tasks manually because the tools they have do not provide a way for them to get obtain needed information[10].

In his Masters thesis, Farrell addressed a number of issues with forensics tools, including usability, and proposed a new approach to forensics reporting. Instead of the current manual method that relies on a trained human operator, the author has suggested a digital tool that will "perform automated analysis and reporting." Furthermore, he proposed design requirements for an automated reporting tool framework that takes into consideration three main categories: systems, user interface, and reporting intelligence. The thesis emphasized making the tool more efficient for untrained users by following a "user-centric approach that requires minimal human involvement thereby increasing usability and providing results with less time and effort [11].

III. Methodology

In this section we describe our study methodology, which included expert interviews and a survey of attendees at a forensics conference. The main goal of this research was to identify usability problems with forensics tools. In future work we plan to explore identified usability problems further through heuristic evaluation and user testing.

A. Interviews

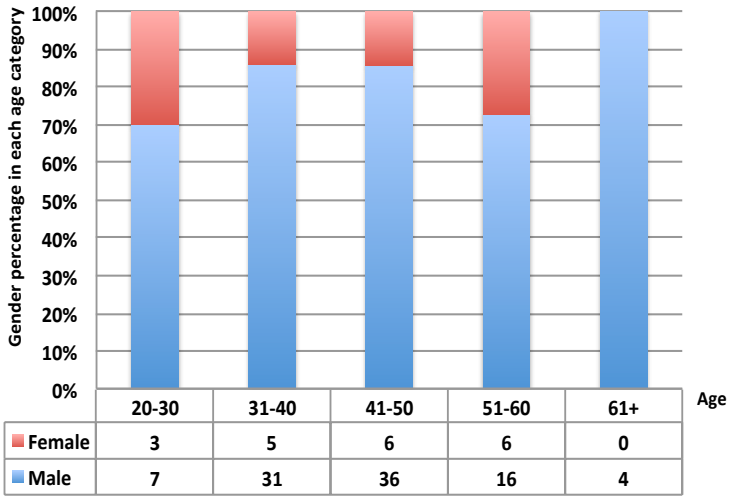
We first conducted two informal interviews with forensics experts in order to better understand the problem space. We used information gathered during these two informal interviews, plus information from our own review of the major forensics tools available on the market to develop an interview protocol.

We interviewed eight additional law enforcement and industry forensics experts in a series of 45-90 minute interviews. We encouraged interviewees to qualify answers by demonstrating everyday use cases with tools they use and issues they face. The experts are very familiar with digital forensics tools as they vocationally support several large law enforcement entities. In particular, they assist their clients by conducting training sessions or helping them solve case-related requests that are complicated or that require advanced technical skills. Our eight experts have a variety of backgrounds, including private-sector forensics and law enforcement field agents.

Digital forensics is often a complex application of computer science to legal settings. We had preconceived notions regarding tool usability in the space, but the interviews provided us with valuable insight into the usability problems as experienced by experts in the field. The interview notes and feedback not only helped us form informed theories regarding tool usability, but also greatly assisted the development of our survey.

B. Surveys

Using the information gathered from the interview process, we developed a survey to assess usability problems with digital forensics tools. Survey questions were shaped to determine if the observed usability issues held with a larger population and to address specific issues not suited for the interview process. Before addressing a larger population, a pilot version of the survey was given to five students enrolled in graduate programs with a focus in digital forensics. We revised and modified the survey questions based on feedback from the pilot. We conducted the survey at the High Technology Crime Investigation Association (HTCIA) 2010 international conference. HTCIA hosts a wide range of practitioners, academics, and policy makers



	20-30	31-40	41-50	51-60	61+
Female	3	5	6	6	0
Male	7	31	36	16	4

Fig. 1. Gender and age data from the survey. The table shows the total count of each gender in each age category.

all with varying backgrounds working in different sectors. Paper surveys were distributed to attendees who were encouraged to participate via an immediate reward of a $10 Amazon gift card. This approach garnered 115 responses.

IV. Results & Analysis

A. Demographics

Our survey participants ranged between 20 and 61+ years old. Most participants were between 31 and 50 years old and only 4% were over 61. Male participants represented 83% of the overall participants. This was expected as both the IT and Law Enforcement fields are highly dominated by males (see Fig. 1). Given that the survey was conducted at a conference, we expected that most participants would hold at least a bachelors degree. The survey results were as expected: only 23% of our sample had an education level lower than bachelors. Bachelors degree holders were 42% of the sample, masters holders were 30%, and PhD holders were 5% (see Fig. 2a). Most participants had majors related directly to the computer forensics field: 37% computer science or IT-related, 21% criminal justice related, and 16% computer forensics. However, 26% of participants had other majors such as: business, accounting, biology, science, engineering, history, law, and behavioral science.

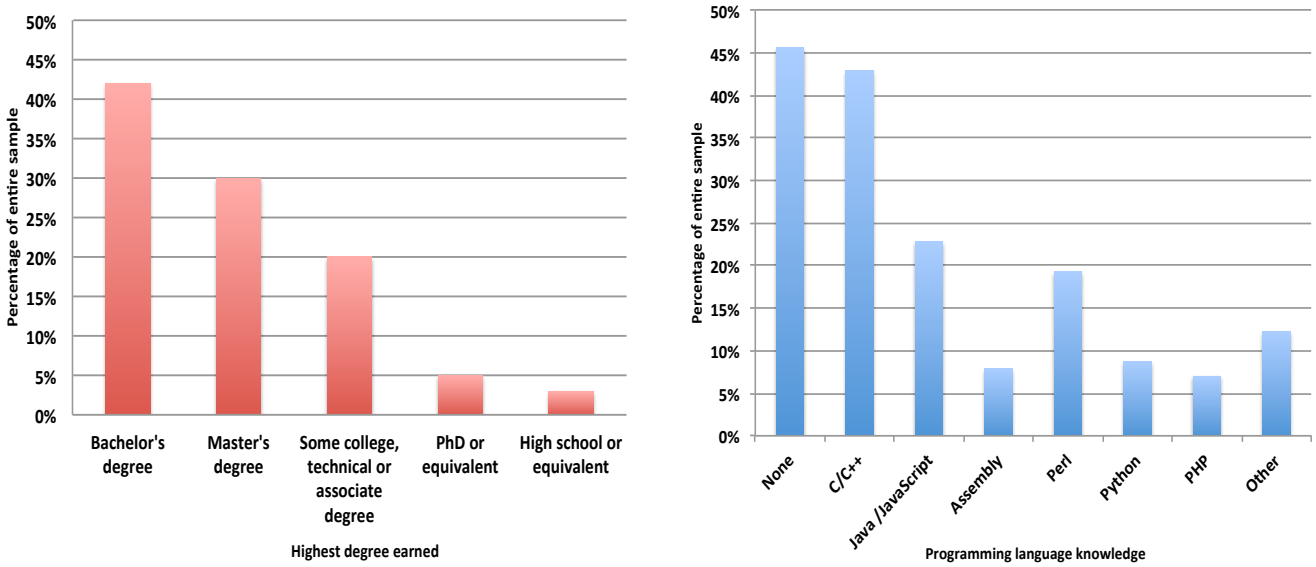
The occupation categories for the participants were: 43% law enforcement, 29% private sector, 19% other government sectors, and 10% other. These other fields were either related to academia, or related to both government and private sector such as retired law enforcement personnel who work as consultants for the private sector.

B. Level of Expertise & Major Tools

We asked participants to rate their overall level of expertise with forensics tools. 43% of participants reported being experts, 39% reported being intermediate, and 18% reported being beginners. Then, we asked participants to rate their level of expertise by application. The results indicate that the commercial software FTK and Encase dominate the field as they are easily the most widely used. Out of 114 users, only 7 had never used FTK and only 6 had never used Encase. No users reported using neither FTK nor Encase. Among open source tools, Autopsy and the Sleuth Kit were the most common. This is not a surprising result for major tools in the market, and is consistent with existing literature. A team of researchers in California State Polytechnic University had compared the performance of open source tools to commercial ones using the same disk images. The researchers specifically compared common market tools: Encase, FTK, The Sleuth Kit and Autopsy[12].

The frequency with which participants used open source tools was as follows: always 18%, sometimes 51%, rarely 26%, and never 5%. We further inquired about the reasons that participants use open source tools. 54% reported that they use open source tools when these tools do a certain function better than the commercial framework and 43% reported that they use open source tools if there is no way to do that function in a commercial framework. Following this question was an opposing question: why would the participant not use open source tools. 31% of participants responded that they are not familiar with these tools in general, 29% responded that their organizations already provide licenses for commercial products, and 20% believe that open source tools do not have reliable user support.

In addition to the reasons mentioned above for favoring commercial tools over open source, another reason emerged: FTK and Encase are believed to be court approved. Some of the law enforcement users added comments that they avoid the use of open-source tools because they are not sure whether or not their results are admissible in court. We expected to see that



(a) Participants education level percentages

(b) Participants programming languages background percentages

Fig. 2. Education level and programing background of survey participants

kind of comment because in our interview process, we encountered comments about "court blessing" several times. "Court blessing" was the term that many of our experts used to describe the importance of court admissibility of evidence. Our experts emphasized that to have a stronger case; they need to verify their analysis. If the analysis was done using some open source tools, they told us that it is essential to go back and find the same result using commercial tools that are "court-blessed." This is a common belief, that may actually be a misconception. Carrier reviewed open source tools and examined them against the "Daubert test" guidelines that courts use to measure the admissibility of scientific evidence. Carrier showed that open source tools meet all the known guidelines of the Daubert procedure, which makes their admissibility at least as good as closed source tools [13].

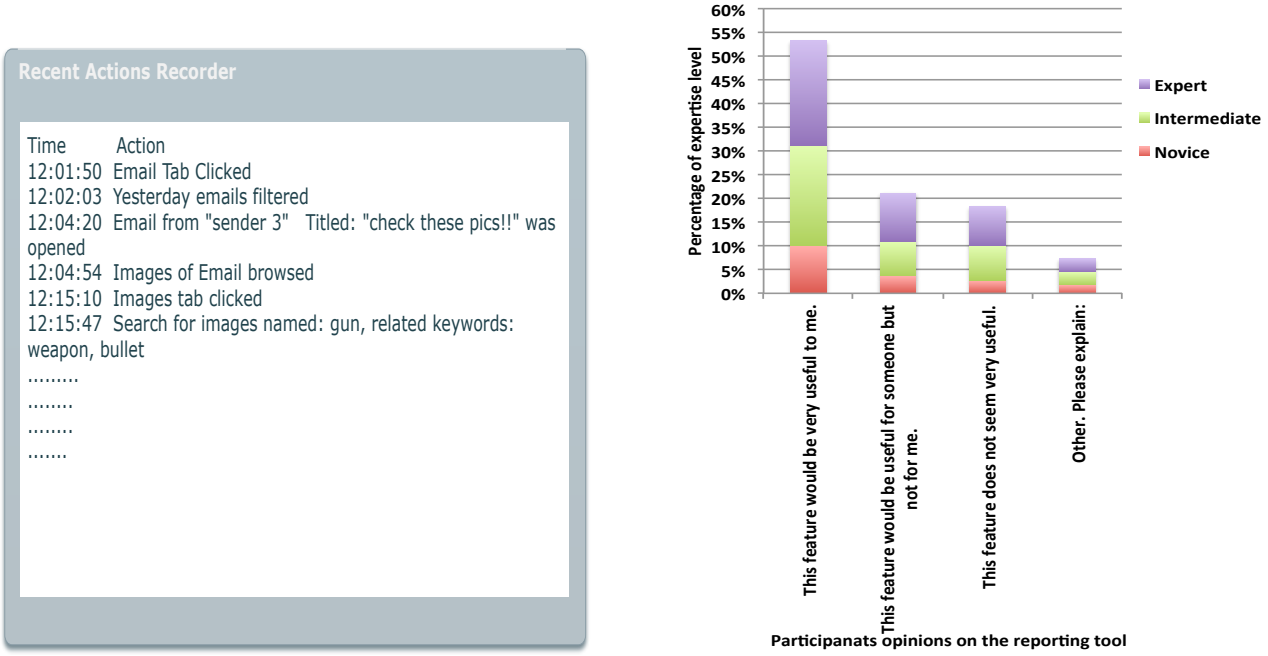
C. Use of GUI vs. Scripts and Command Lines

We asked respondents directly about the frequency of using command line forensic tools as opposed to GUI forensic tools. The results were as follows: always: 13%, sometimes 42%, rarely 35%, and never 10%. Our results suggest that the users we surveyed are more satisfied with the GUI interface and they try to avoid the use of command line tools as much as possible. Generally, users use the command line in situations where a certain task can be done better or if there is no way to do that task through the GUI interface.

It is important to note that 45% of the participants reported that they do not know any programming languages. The remaining participants had experience mostly with languages such as C, C++, Java or Perl. Only a small fraction reported knowing JavaScript, Assembly, Visual Basic, Python, or PHP. The percentages of participants with knowledge of each programming language is shown in Fig. 2b.

We asked users of different expertise levels about Encase's special "Enscript" proprietary scripting language. Although the frequency of use was almost uniformly distributed (always: 21%, sometimes: 26%, rarely: 25%, and never: 28%), are results show that users usually search for pre-made scripts that are available online rather than understanding the syntax and writing their own scripts. About 58% of the respondents said they only search online for ready-made scripts and copy scripts into their workspace and 36% reported that they search for ready-made scripts first and if they don't find something helpful then they will attempt to write their own scripts. This observation is evidence that users of different backgrounds and expertise levels prefer not to write scripts, especially when they must be written in a language other than a common programming or scripting language.

Even experienced programmers like to reuse code and this fact might contribute to the results regarding the use of Enscript. In fact, it is also important to note that experienced programmers might prefer to use programming and scripting languages that they already know rather then going out of their way to learn a new language. Some experts during the interviews said that when they can't find results using FTK and Encase, they use open source tools where they can run scripts with a language that they are comfortable using such as Perl. When asked about Encase's Enscript language specifically, most of them said that they never or rarely use it, and if they did, they would use a ready-made script that was made available online. One interesting



(a) The reporting tool mock-up in Survey

(b) Responses to reporting tool by tools experience level

Fig. 3. Mock-up reporting tool presented in the survey and participants responses to it

example some interviewees pointed out was the Enscript script for credit card search. Searching for credit card numbers on examined computers is a very common task for many forensic examiners. Although there is a built-in Enscript script to search for credit card numbers, it is not really strictly searching for credit cards numbers. The script will capture any 16-digit number and display that in the query result without checking if these numbers match credit card patterns. It is not surprising then to see an Adobe software license key included in the search results. As a result, our experts stated that many examiners tend to use outside software tools and scripts that were written to give more refined search results and find numbers that are more likely to actually represent credit cards.

Our results suggest that many forensics tools users are not programmers; and almost all users, including those with programming experience, find it inconvenient to write code from scratch. Therefore, we suggest that forensic tools come packaged with more of the functionality used by practitioners. This approach will free users from having to learn the details of the scripting language. For example, Encase designers might want to look at the most popular downloaded online-scripts and work on embedding their functionality in their updates. Another suggestion is to make the process of building scripts more user-friendly, even for non-technical users. Instead of having users learn the Enscript language, the software can include a wizard interface, or a tool like "the formula builder" that is used in MS Excel and some other programs.

An important question regarding language should be addressed: is it necessary for Guidance Software to develop its own proprietary scripting language when other familiar, established scripting languages exist? What kind of functionality does Encase's Enscript provide? Is it possible to have these functionalities bundled in libraries that are compatible with common programming languages? Enscript is one reason that Encase is difficult to use. In [12], the author describes using Perl in Autopsy and The Sleuth Kit as an advantage because of the ease of customizability. Garfinkel states that forensics tools lack "frameworks that enable cross-language and cross-platform development" that we already see in other development communities [10]. To achieve the kind of interoperability between tools suggested by Garfinkel, we believe that it is essential for these tools to use interoperable scripting languages.

D. Reporting & Documentation

One critical step for any forensics investigation is reporting. The experts that we interviewed described this part as "not very easy." They further explained that while performing an examination, the investigator concentrates on analyzing the case and going in every direction possible to reach a conclusion. Once the conclusion is made, now the investigator must go back and try to remember all the steps taken to reach that result. We asked several questions about documentation in our survey.

We asked the participants to respond to the following question: "When it comes to documentation and reporting, I usually...." Bookmarking key points in the program itself, was the most common response, with 75% of responses. The second most

TABLE I
PREFERRED REPORTING AND DOCUMENTATION METHODS.

When it comes to documentation and reporting, I usually...	Number	Percentage
bookmark some important points in the program itself	86	75.4%
use a pen to write down some of my findings and brain storm my ideas	59	51.8%
have MS Word opened on another screen while I am working and I will be typing some key points	55	48.2%
use MS Word on the same screen	6	5.3%
use some note taking software	14	12.3%
never document while working on the case – I concentrate on solving the case, and after that is done I will sit and worry about documentation and reporting	3	2.6%
brief a colleague about the findings and let them write the document	1	0.9%
only fill the standard forms, I don't tend to write a thorough report	1	0.9%
other	10	8.8%

common responses were the traditional pen and paper method (52%) and using Microsoft word on another screen for note taking (48%). Note that we gave participants the option of selecting multiple answers, hence the sum of the percentages is above 100%. We summarize the responses for this question in Table I.

We showed survey participants a screenshot of a sample reporting-assistant tool (shown in Fig. 3a) that records the actions of the investigator while working on a case. Over half of the users (55%) responded that this tool would be very useful to them, and 20% reported that they would not find it useful but they think it would be useful to users other than themselves. The breakdown of these responses by participant job categories is shown in Fig. 3b. Although current tools already have some built-in reporting features, these features do not collect user logs automatically and do not provide the level of detail needed for users to review their actions and remember what steps they took in order to write their reports.

When we asked participants to write their comments about how to make forensics tools more usable, we had 64 responses (greater than 50% response rate). Twelve users explicitly suggest having better reporting tools. We intentionally placed this question before the question that showed a sample tool so we could collect their feedback prior to influencing them with this idea.

E. Training needs

During the interviews, experts explained that forensics tools require users to have special knowledge and acquire a number of skills. For this reason, they emphasized the need to continuously train their clients on new tools and techniques. They also stated that no agent could start conducting forensics examinations in the field without proof of taking proper training. Therefore, we included some questions to get user feedback regarding training. Fig. 4 shows how frequently users undergo training, broken down by job category.

When asked about how they prefer to learn how to use forensic tools, 68% of respondents reported that they prefer going to intensive training. This is a strong indicator that users are still not confident about their capabilities regarding new tools and that they find them difficult to understand without in-depth training. 24% preferred to use tools with a better GUI interface that would require less training. 1% of the sample think that the tools are very complicated and they would rather have a third-party do the analysis. The remaining 7% suggested other options such as online training, reading manuals, and attending training sessions.

Users were also asked how strongly they would agree or disagree with the following statement: "I can learn how to use these tools on my own, the learning curve is similar to programs like MS Office." The response percentages were as follows: strongly disagree: 9%, disagree: 31%, neutral: 26%, agree: 28%, and strongly agree: 5%. However, when looking at the whole picture of the survey results, it is important to note that most of our sample (77%) have a bachelors degree or higher and 53% of the sample have a degree in a computer-related field. This kind of a background will affect the judgment on difficulty level of learning the tools. Usually, expert users who are already very familiar with using the tools will tend to find the learning curve easier. With this education background, one might expect to see the results of this Likert-scale question lean towards agree. Instead, our result had shown that overall users are neutral on this question with slight leaning towards disagree.

F. User Interface Issues

Participants provided several categories of comments that all reflect user interface problems. We identified six categories of user interface issues.

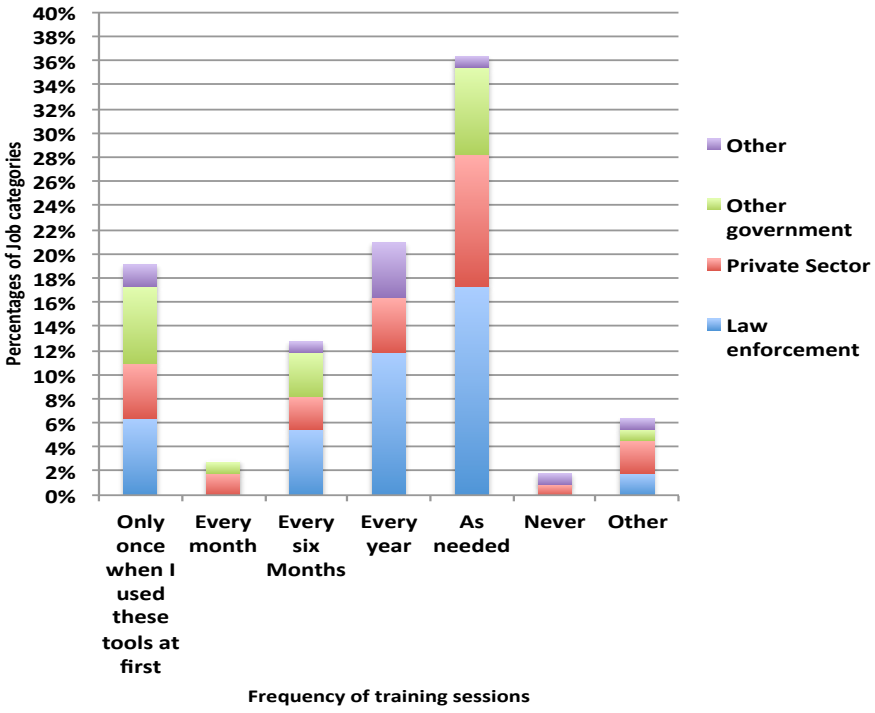


Fig. 4. Training frequency for survey participants overall and by job category

1) Consistency: Some participant comments relate to "consistency" among interfaces. This is a reasonable issue to comment upon because from our assessment of the tools and from the expert interviews, it is obvious that there is no consistency among the different tools. A respondent suggested an interface that has the "Windows" look and feel, which suggests the user would prefer an interface that is more like an interface with which the user is already familiar. To illustrate the issue, let us examine the interfaces of two major tools, FTK and Encase, which are shown in Fig. 5 and Fig. 6. While FTK has a look and feel closer to "Windows Explorer," Encase has a different interface implementing a tree structure that is not very intuitive. If users click in the wrong place in this special structure they can end up displaying a recursive view where they might be confused because they see unexpected results. One participant complained about the inconsistencies between versions of the same product: "Settle on an interface and improve on it. Quit making wholesale interface changes..." the user wrote.

2) An "intuitive" interface: Having a more "intuitive" interface was another participant suggestion. For users to find interfaces intuitive means that they should be consistent with something users are familiar with such as other common programs or common workflows for the task they are trying to accomplish. During the interviews all the experts agreed that when they first used FTK and Encase, they found the Encase interface "less intuitive" because it uses a non-standard tree view when compared to the tree view found in FTK that is similar in looks and functionality to the Windows classic tree view. Furthermore, when we asked our interview participants to rate FTK and Encase, all participants rated FTK to be easier. When asked about reasons, they commented that the FTK interface is more intuitive and Windows-like, which will ease the learning curve of the program itself compared to Encase's non-standard way of displaying things. Accordingly, in their comparison of forensics tools, Manson et al. stated that Encase's user interface in general is "difficult for almost anybody to use" [12].

3) Information overload: Another user interface issue mentioned by our participants is information overload. In other words, the amount of information presented to the user is very dense. When we asked about the screen space, we found that 69% of our participants prefer to use at least two monitors not less than 17" each. This result is consistent with what we observed in our interviews. Upon entering the workspace of a participant, the first thing we observed was large screen space: dual monitors of not less than 19" each. When we asked the participants about the monitors they described such a working environment as essential in order to have a more efficient view of the large quantity of dense information. Our participants had also noted that without this type of set-up, the amount of time and effort needed to investigate a case would increase. In fact, one interviewee demonstrated to us the significant impact on time and effort when examining the same file using multiple large screens vs. a traditional laptop screen. He used Encase to examine a number of MS Word documents using a dual monitor screen set-up, and then repeated the same process using his laptop. The difference in time and effort was so significant that he find relying

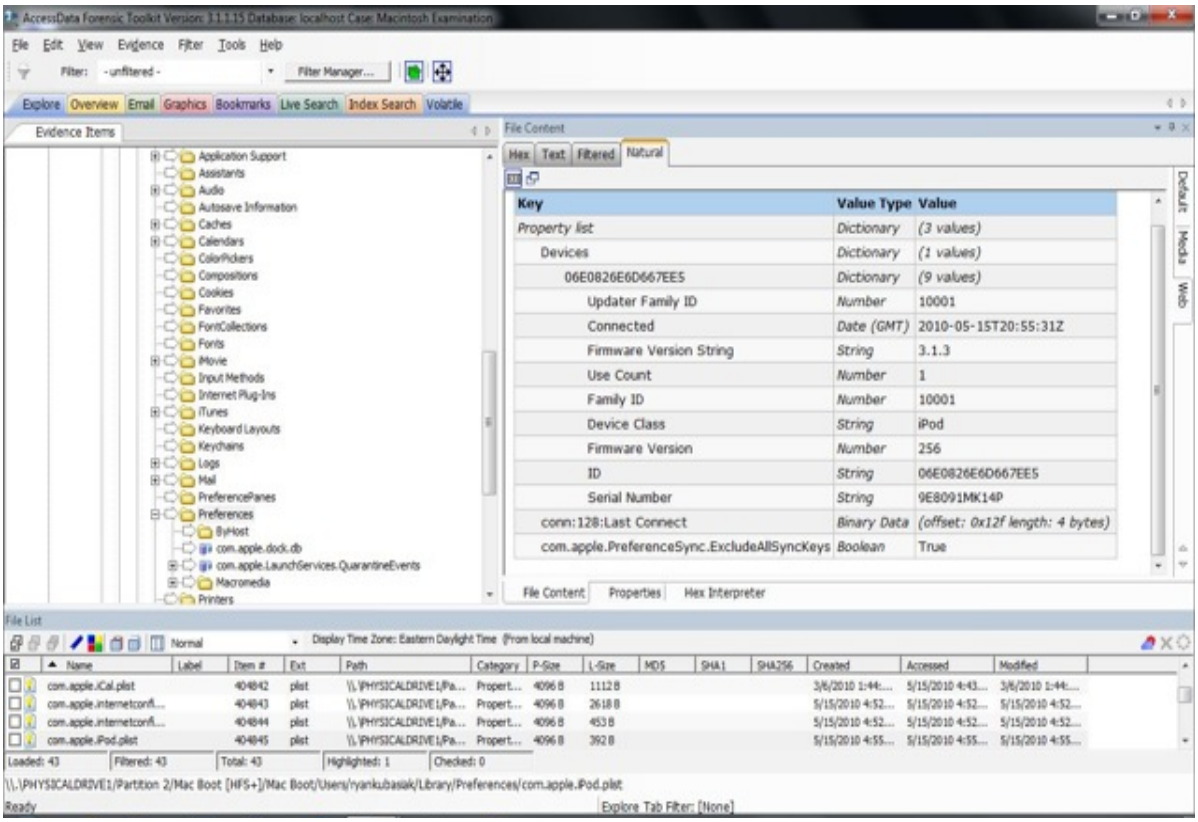


Fig. 5. FTK screenshot (source: www.appleexaminer.com)

on a small laptop totally impractical for a forensics examination. It is an open question as to whether all of the information needs to be shown on screen simultaneously. A better designed interface might contain less information, but focus on the information most useful to the investigator.

4) Use of icons : Icons are often used to represent complicated concepts and thus may be confusing to novice users. One expert that we interviewed acknowledged that many concepts are difficult to represent with icons: "How would you make an icon describe: Extracting a string from a Hard-Drive?" We asked users to rate the understandability of the icons used in forensics tools on a five-point Likert scale where five is very user-friendly. 32% of participant gave icons a rating of 3 and 42% gave icons a rating of 4. Thus, icons were not a major concern for most of our survey participant. However, one user drew a picture of a square (representing the icon shape) and an arrow pointing to that icon. The respondent used the term "icon referencing" to suggest having some explanatory text that will appear when pointing to an icon. We assume this user is suggesting more use of "tool tips" or "hover text."

5) Picture presentation and image clustering: For picture presentation, 54% of respondents reported that they are "satisfied" with the way pictures are presented in FTK and Encase. The next question was to choose among a number of different picture representation methods where they can choose more than one method. Most participants preferred gallery/organizer view and large thumbnails with percentages of 75% and 50% respectively. Apparently, this is a functionality the users are satisfied with in forensic tools. However, we had one comment from a law enforcement expert that it would be more efficient to have the gallery search implemented in a more efficient way; for example, one suggestion was "image clustering" that is already available in some applications and online gallery websites. Image clustering could speed up the image search process because once an investigator selects a picture; the software would re-organize the other images according to its relevance to that picture. In a similar context, a paper by Beebe [14], suggested applying clustering to text searches in forensic tools and explained the advantage investigators could get if this smarter search algorithm were to be applied into forensic tools.

G. Relationship between the User Interface and the Forensic Process

Based on the initial interviews and our own assessment, one theory we wanted to test in the surveys was that current user interfaces do not match the workflows used in forensic investigations. 43% disagreed with this theory while the others either agreed or were neutral. One user explicitly suggested having tools that are workflow related. Another user suggested tools that are "more mission-oriented."

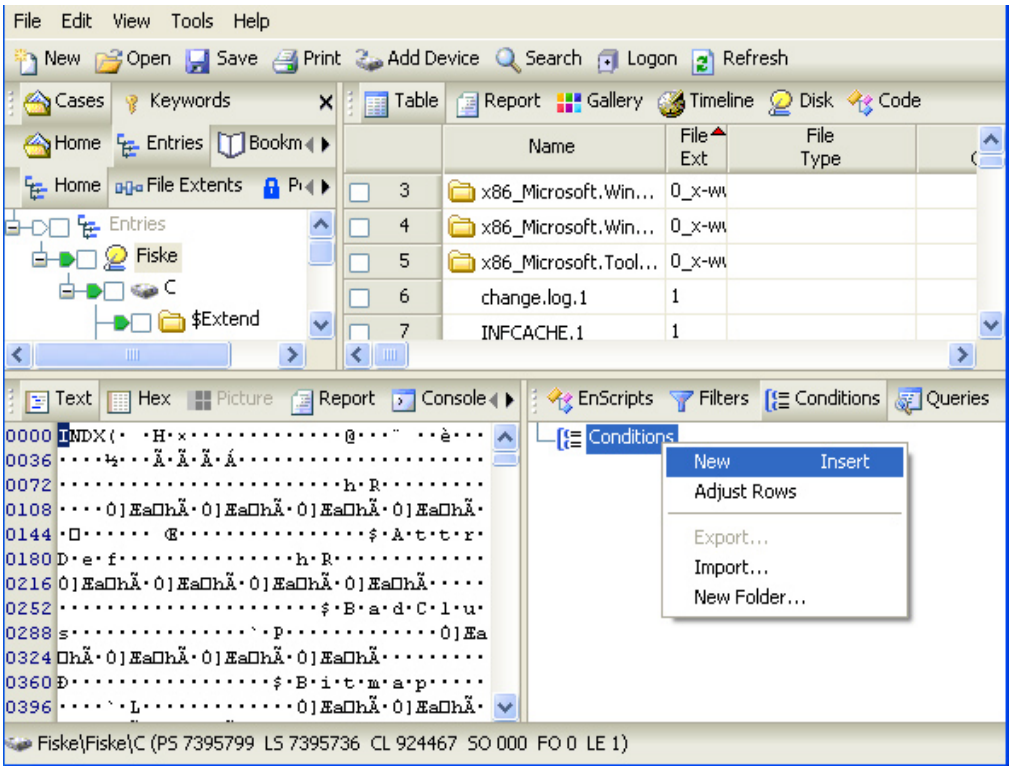


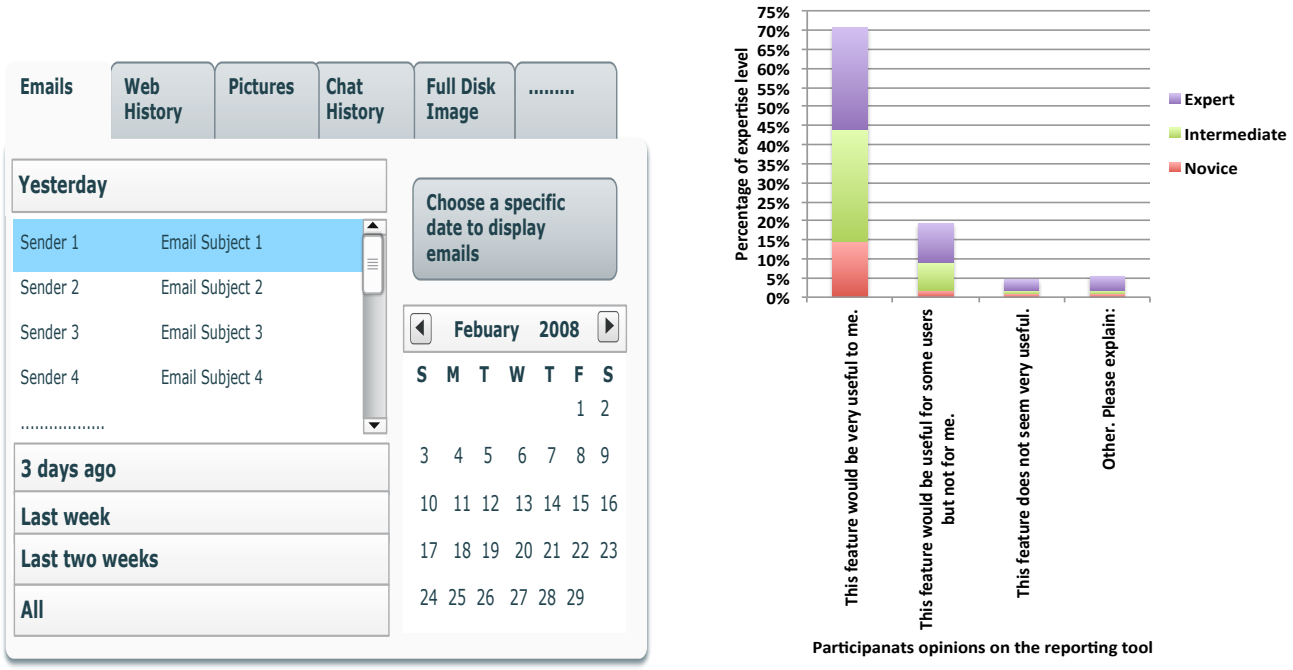
Fig. 6. Encase screenshot (source: http://www.encaseenterprise.com)

TABLE II
INVESTIGATION FREQUENTLY ASKED QUESTIONS

Question	Always	Usually	Sometimes	Rarely	Never
What web sites were visited and when?	47.4%	36%	14%	1.8%	0.9%
What email was exchanged with whom and when?	52.6%	33.3%	11.4%	0.9%	1.8%
What other things did the person of interest do on their computer system(s)?	39.5%	41.2%	14.9%	3.5%	0.9%
What, if any, other devices could evidence reside upon (USB drives, on-line backup providers)?	55.3%	26.3%	14%	2.6%	1.8%
Was a wiping tool used?	31.6%	28.9%	23.7%	11.4%	4.4%
Was there any encryption involved?	37.7%	26.3%	22.8%	9.6%	3.5%
How many users are using this machine, and what are their privileges?	50%	28.9%	14.9%	2.6%	3.5%
What type of file system is on this machine?	72.8%	14%	6.1%	3.5%	3.5%
What is the content of the photos on this machine?	41.2%	35.1%	20.2%	2.6%	0.9%
What kinds of documents are on this machine?	51.3%	36.3%	9.7%	1.8%	0.9%

We presented a set of questions to participants and asked them about the frequency that the questions occur in an investigation. The results are shown in detail in Table II. With even a cursory view of the results, it is obvious that most of the questions occur frequently and the percentage of "rare" or "none" is very low. Our results suggest that investigators have a standard set of investigative questions in mind for which they are trying to find answers without paying much attention to the underlying technical details. We asked users to list any additional questions they had and the result came as expected: high level questions most of the time such as what was communicated through email or chat, what information was transferred, who is responsible, why, etc. Currently, the forensic tools are not designed in a manner that facilitates answering these questions. Investigators need to go out of their way through a lot of technical details in order to obtain answers. This may have been the motivation behind one user suggestion to implement tools with "Wizard" functionality where users can go through a process of answering a set of questions to build their case.

We included a mock-up design of a simplified tabular-style GUI in the survey, shown in Fig. 7. We chose the following tab titles: email, web History, pictures, chat history, and full disk image. This way a disk image will have different organized views depending on what kind of information investigators are looking for, with the full disk image view option still available.



(a) Tabular-style mock-up user interface

(b) Participants responses for tabular GUI

Fig. 7. Mock-up tabular-style GUI presented in the survey and participants responses to it

The results of the survey (see Fig. 7b) showed that 72% of the users are in favor of having such a GUI and 18% think it will be useful to users other than themselves.

H. Other Usability & Technical Issues

The experts we interviewed believed that most users desire a tool that has a "Get Evidence Button." This means that the user wishes to click on a button that describes what he is looking for: credit cards, pictures, emails, etc. Then, the tool should act intelligently by getting the results the user requested. One interviewee mentioned that in one of the training sessions that they conducted for their clients, they started with introducing an in-house implemented tool that has a very simple graphical interface, but uses a complicated algorithm to find credit card numbers stored in a machine. When the training proceeded with other tools, users kept commenting that they didn't want any of these other tools that requires too much "brain power." They only want something similar to that simple interface they saw in the credit card tool. Survey participants expressed similar sentiments. One requested to "Be able to set-up common search that I do press a button to get a common information."

Another interesting concern that we learned about from the interviews was the lack of an integrated collaborative environment. 43% of the survey respondents also reported that they lack an integrated collaborative environment. A collaborative environment is helpful for investigators to work simultaneously on cases rather than relying on email, phone, or face-to-face communication. Furthermore, This kind of an environment helps non-expert users communicate with experts and ask them about any concerns or questions they might have.

Respondents to our survey provided a number of different suggestions for improving usability and functionality. In addition to all the comments that we mentioned in the previous sections, users commented on a number of features that they either find confusing or completely absent. In addition, some noted that they use open source or e-discovery tools when those tools are better able to meet their needs.

Many user comments mentioned aspects that we have already covered in the survey. Some of the other interesting suggestions included: better modular design, interoperability between different tools (currently the major tools are not interoperable) as well as version backward compatibility (FTK versions, for example, are typically not backward compatible with existing case files), better menu navigation, better help tools, improved installation process, better display of data, better error messaging, less frequent crashes, more software stability, add functions provided by the smaller specialized tools, faster processing speed, and more streamlining.

V. Conclusions & Future Work

The survey results provide strong evidence that current digital forensics tools are not considered user-friendly and that they lack intuitive interfaces. It is a challenge for investigators to directly find answers to their high level, case-related questions.

Usability is a critical issue in these tools because misunderstanding that leads to false interpretations may impact real-life cases.

Currently, users are overwhelmed with the amount of technical background required to use these tools. It is true that there are cases where an investigator needs to have a deep understanding of computer systems and networks to be able to interpret evidence correctly. However, this is not always required. According to the experts we interviewed, it is usually the case that field agents are conducting the investigation to be able to get answers to simple investigative questions such as: "Did person A contact Person B on that date? What websites did he visit? What kind of emails did he exchange and with whom?" When field agents are faced with cases involving technically savvy criminals, they generally ask more experienced personnel to examine evidence. Therefore, it is important to keep all levels of users in mind. Designers of these tools should keep the Microsoft Office example in mind, where users of different expertise levels can make the best use of the software: a novice user can easily find his way into writing a letter or report, and at the same time, a more sophisticated user will make use of advanced features the program offers (such as writing macros or connecting to an online collaborative repository).

Two conflicting suggestions written in the survey drew our attention: "I like to have a tool that does it all" vs. "The tools are too complicated. They do everything. It was a better environment when a tool did one job." These conflicting statements are a clear indicator that having one solution to please all user categories is not an easy task.

In our user study, we have reviewed some of the areas that need improvement: reporting, graphics, user interface, and collaborative environment among others. We plan to expand our research to explore many of these areas and conduct more user testing that will give us a better insight into these problems. In addition to user testing, we are also planning to apply heuristic evaluation to certain tasks that are accomplished with these types of software. We also intend to conduct a larger survey in order to better understand the digital forensics tools landscape. Our goal is to outline a set of usability guidelines for designing digital forensics tools. Designers and software engineers can use these guidelines to implement software solutions that meet the needs of digital forensics practitioners.

ACKNOWLEDGMENTS

We would like to thank the forensic experts who participated in interviews for this study, and and the HTCIA conference organizers for allowing us to survey conference participants. We also thank Simson Garfinkel for his valuable feedback and suggestions. This material is based upon work supported by the Naval Postgraduate School under Award No. N002441010055 and by NSF IGERT grant DGE0903659.

REFERENCES

[1] D. Crenshaw, *The Myth of Multitasking: How" Doing It All" Gets Nothing Done*. Jossey-Bass Inc Pub, 2008.
[2] "Williford vs. State of Texas," Court Case No. 11-02-00074- CR, 127 SW 3d 309, Texas Appeals Court, January 2004.
[3] Usability Net: International standards for HCI and usability. Usability.Net. [Online]. Available: http://www.usabilitynet.org/tools.htm
[4] L. Cranor and S. Garfinkel, *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Inc., 2005.
[5] B. Carrier, *File system forensic analysis*. Addison-Wesley Professional, 2005.
[6] L. Gottschalk, J. Liu, B. Dathan, S. Fitzgerald, and M. Stein, "Computer forensics programs in higher education: a preliminary study," in *Proceedings of the 36th SIGCSE technical symposium on Computer science education*, ser. SIGCSE '05. New York, NY, USA: ACM, 2005, pp. 147–151. [Online]. Available: http://doi.acm.org/10.1145/1047344.1047403
[7] A. Yasinsac, R. Erbacher, D. Marks, M. Pollitt, and P. Sommer, "Computer Forensics Education," *Security & Privacy, IEEE*, vol. 1, no. 4, pp. 15–23, 2003.
[8] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of Digital Evidence*, vol. 1, no. 3, pp. 1–12, 2002.
[9] Encase examination of ntfs. Guidance Software. [Online]. Available: http://www.guidancesoftware.com/computer-forensics-training-ntfs.htm
[10] S. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, 2010.
[11] J. Farrell, "A Framework for Automated Digital Forensic Reporting," Master's thesis, Naval Postgraduate School, US, 2009.
[12] D. Manson, A. Carlin, S. Ramos, A. Gyger, M. Kaufman, and J. Treichelt, "Is the open way a better way? Digital forensics using open source tools," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. IEEE, 2007, p. 266b.
[13] B. Carrier, "Open source digital forensics tools: The legal argument," *stake Research Report*, 2002.
[14] N. Beebe and J. Clark, "Digital forensic text string searching: Improving information retrieval effectiveness by thematically clustering search results," *Digital Investigation*, vol. 4, pp. 49–54, 2007.