Show Me How You See Lessons from Studying Computer Forensics Experts for Visualization

T.J. Jankun-Kelly, J. Frank, D. Wilson, J. Carver, D. Dampier, J. E. Swan II Mississippi State University









And now for something completely different.... nary a visualization will be in sight. However, visualization for security (specifically forensics) is the goal. However, this talk is more about our difficulties in doing the work surrounding the visualization; in this case, working on the domain analysis for the viz.



Today's talk will be a simple narrative about part of our multi-year computer forensics visualization work. In order to properly motivate our visualization design, we decided to perform a significant domain analysis of potential users—law enforcement officers in Mississippi. Fortunately for us, we have a training center for these cops at State. So, our goal was simple: Perform a study to observe their working patterns, identify areas of improvement, design the visualization, and validate it against our officers. Unfortunately, life is rarely so simple.

The Study



Our testbed was webmail based forensics. We explored several different types of studies until settling on a simple observational study. First, we created two datasets with fraudulent behavior via several false webmail accounts and emails back and forth. We mixed these in with more legitimate sources by signing up the main accounts to various mailing lists. In addition, the main account performed various web-browsing behavior, some related to the fraud, others not. Two disc images of these were then used as the base data for observation.

Q Cognition Assignment Tool



File View

Capture Playback Case2:hest1:vol1 - Madilla Firefox - -Edit Van History Bookharks Toolo Hele - 🧄 - 😴 🔘 🕋 🏠 impolieshess www.jw.spay.mod. seadanod. Heaves Casewheet Necture. Uninsurand value Image: Company of the second se 🗭 Catting Started 🔣 Latest Headings ela lla Opie Taul Papela (11 📋 🏦 Des Maxiliani) Confidential (12 FLEARADER REWORD SEARCH FLETTRE INASE DEVICE NETA DATE. DATA UNIT saving: Done IS hits and to results · PREVIDIN NEXT -Searching for Unicode: Done Search Done Eeroar Contents AppNote ASCH (DEGRAY - Cleaned display (No H INL tags)- (CCOT) * Hex (DEGRAY - (CCOT) * ASCH Shings (DEGRAY - (CCOT) File Type: ASCI Engistitiest, with CRUP incidentiators Cluster: 0015 Status: Allocated New Search nd Original File and Meta Data Address 18 occurrences of Xanazak were found earch Options A801 Case Sensitive Cluster 6038 (Hes - Asen) 1: 2541 (1000: Reconstant \$1287) i, the Meridanika∥XXI/Wednessing, Seriesing X Churler 20039 (Her Avril) 2: 2080 (Horn Hancocks#30;) Mailbox users+55/ 1s+17/ of 5 GS Cluster 68404 (<u>Hes</u> - <u>Aski</u>) 3. 1559 (Hannah) 1569 (Hermonik)
1566 (Lancock) Set an electronic set and Challer 81433 (the - Anni) 5: 1557 (Julio Romanti Ve Cluster 127860 (<u>Her</u> <u>Ascil</u>) 5: 1670 (https://lancock.was...) Suster 137823 (Hex - Asca) 2527 (January Manager (1382) 3038/9#4E IN M III 🕂 😰 🔞 24:54:93 Event List Event Parameters ^ Time Туре Cognition Name Value Message 24:45:01 mouse Left click @ x = 682 y = 45924:50:23 Left click @ x = 689 y = 254mouse 25:11:50 Left click @ x = 111 y = 490mouse 25:14:98 Left click @ x = 155 y = 494mouse 25:17:50 Left click @ x = 749 y = 248mouse 25:25:23 Left click @ x = 163 y = 538mouse 25:33:75 Left click @ x = 152 y = 595mouse Left click @ x = 159 y = 60525:34:68 mouse 25:37:79 Left click @ x = 700 y = 254mouse ¥ 26:24:32 Left click @ x = 164 v = 656mouse Playback started.

The experimental setup consisted of a laptop with an instrumented version of Autopsy that captured video of the subject, screen capture of their activity, and a time-stamped log for observer notation. Each of our potential subjects—Mississippi forensics practitioners—would be given basic details about the case and allowed to freely explore using the tool until they felt they had a good case or time expired. All subjects were encouraged to think-aloud and take notes.



The setup was simple enough, but the execution is everything. During the Winter of 2007 and Spring of 2008, we spent three months recruiting subjects: On average, 30 phone calls or emails were required in order to set up an appointment or to have them declined. Eventually, five experts were recruited. Unfortunately, that is not the end of the story. Only three completed. In the end, we learned some important things towards are visualization goal.... but we also learned some things about such studies themselves. It is the latter I wish to share today.

Lessons Learned

There are several lessons we learned in the design and execution of the study. However, for the sake of time, I will only go into a detail of a few of them. For the rest, I refer you to our paper.

Keep the Goal in Mind

Keep the goal in mind. We spent a lot of time over designing our study. Initially, we had a more full-blown cognitive analysis. However, we mainly wanted to determine **how** our experts work in the field. Thus, we simplified to our observational design.



Clear Communicate Expectations

Clearly communicate expectations: Expectations were unclear to subjects, causing protracted recruitment. Concern about job evaluation. Easier w/ latter. Though we lost two subjects due to bosses not liking the video/audio logs.

Be Prepared to develop own tools...

Be prepared to develop your own tools... No easily off-the shelf tools or similar framework that any of our colleagues used. So we rolled our own. Very lightweight, and can be used in various work.

01



... but use the tools the experts use. Autopsy good for own development, but not what our experts trained on. Too many questions about it. New versions now used FTK.

Where Do We Go From Here

- Follow-Up Studies
- Visualization System Development/Testing
- Continue to (Try to) Work With Users

Show Me How You See Lessons from Studying Computer Forensics Experts for Visualization

T.J. Jankun-Kelly, J. Frank, D. Wilson, J. Carver, D. Dampier, J. E. Swan II Mississippi State University





