# 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

Mississippi State
UNIVERSITY

JAMES WORTH
BAGLEY
COLLEGE OF ENGINEERING
MISSISSIPPI STATE UNIVERSITY

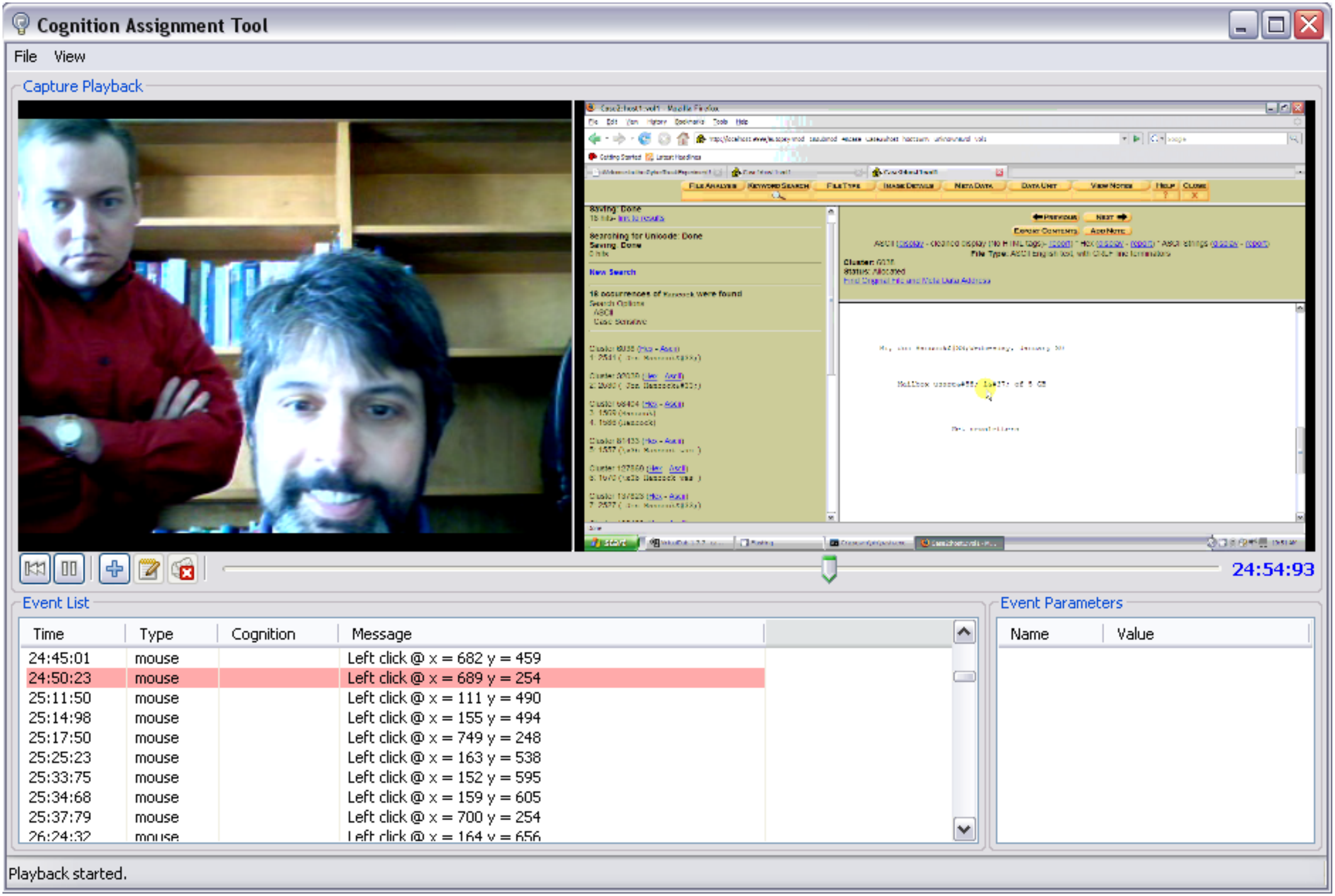
And now for something completely different.... nary a visualization will be in sight. However, visualization for security (specifically forensics) is the goal. However, this talk is more about our difficulties in doing the work surrounding the visualization; in this case, working on the domain analysis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

Forensics Training Center
Usurpo, Consigno, Inquiro
Mississippi State University

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.

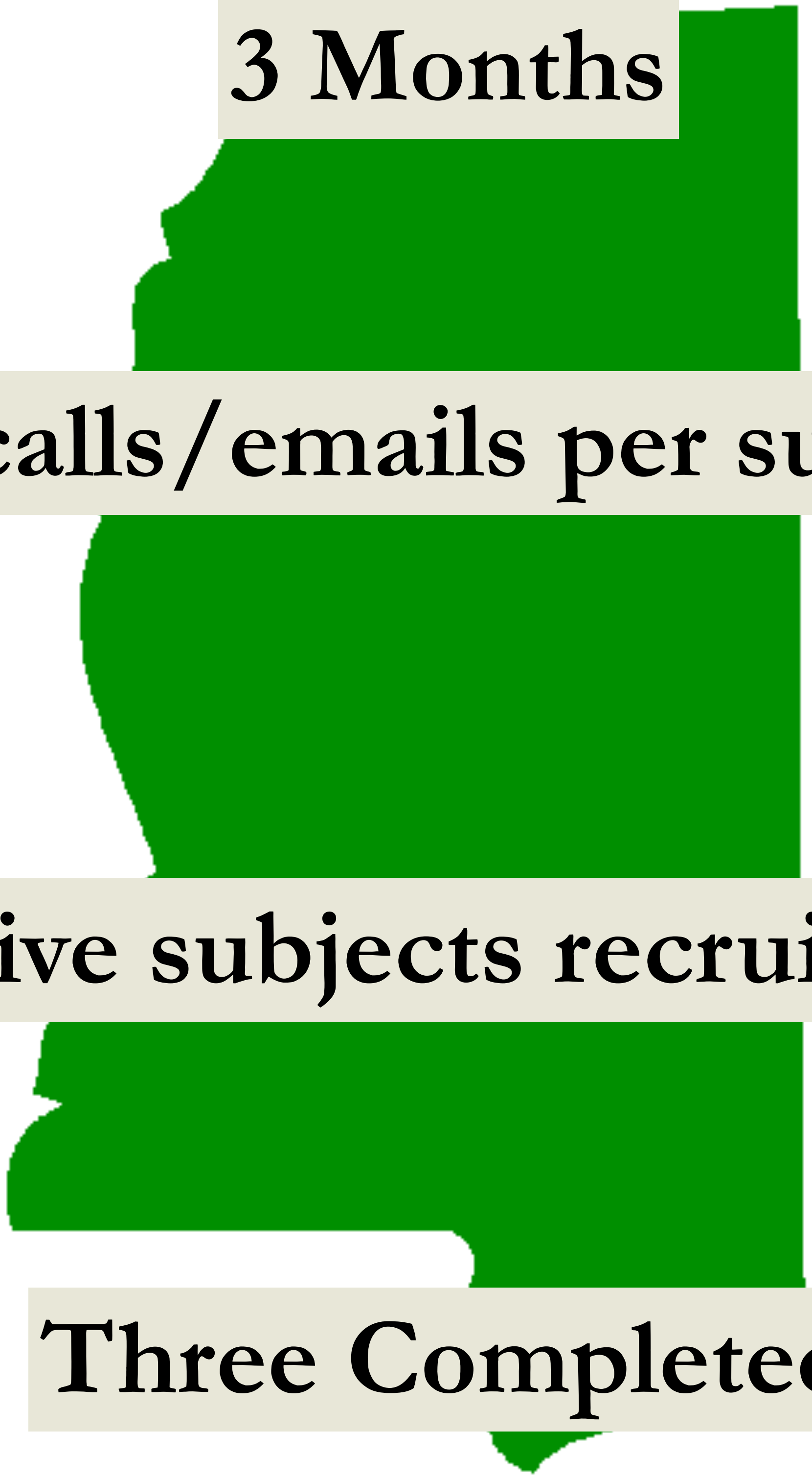


| Time | Type | Cognition | Message |
|---|---|---|---|
| 24:45:01 | mouse | | Left click @ x = 682 y = 459 |
| 24:50:23 | mouse | | Left click @ x = 689 y = 254 |
| 25:11:50 | mouse | | Left click @ x = 111 y = 490 |
| 25:14:98 | mouse | | Left click @ x = 155 y = 494 |
| 25:17:50 | mouse | | Left click @ x = 749 y = 248 |
| 25:25:23 | mouse | | Left click @ x = 163 y = 538 |
| 25:33:75 | mouse | | Left click @ x = 152 y = 595 |
| 25:34:68 | mouse | | Left click @ x = 159 y = 605 |
| 25:37:79 | mouse | | Left click @ x = 700 y = 254 |
| 26:24:32 | mouse | | Left click @ x = 164 y = 656 |

| Name | Value |
|---|---|

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.



3 Months

30 calls/emails per subject

Five subjects recruited

Three Completed

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.

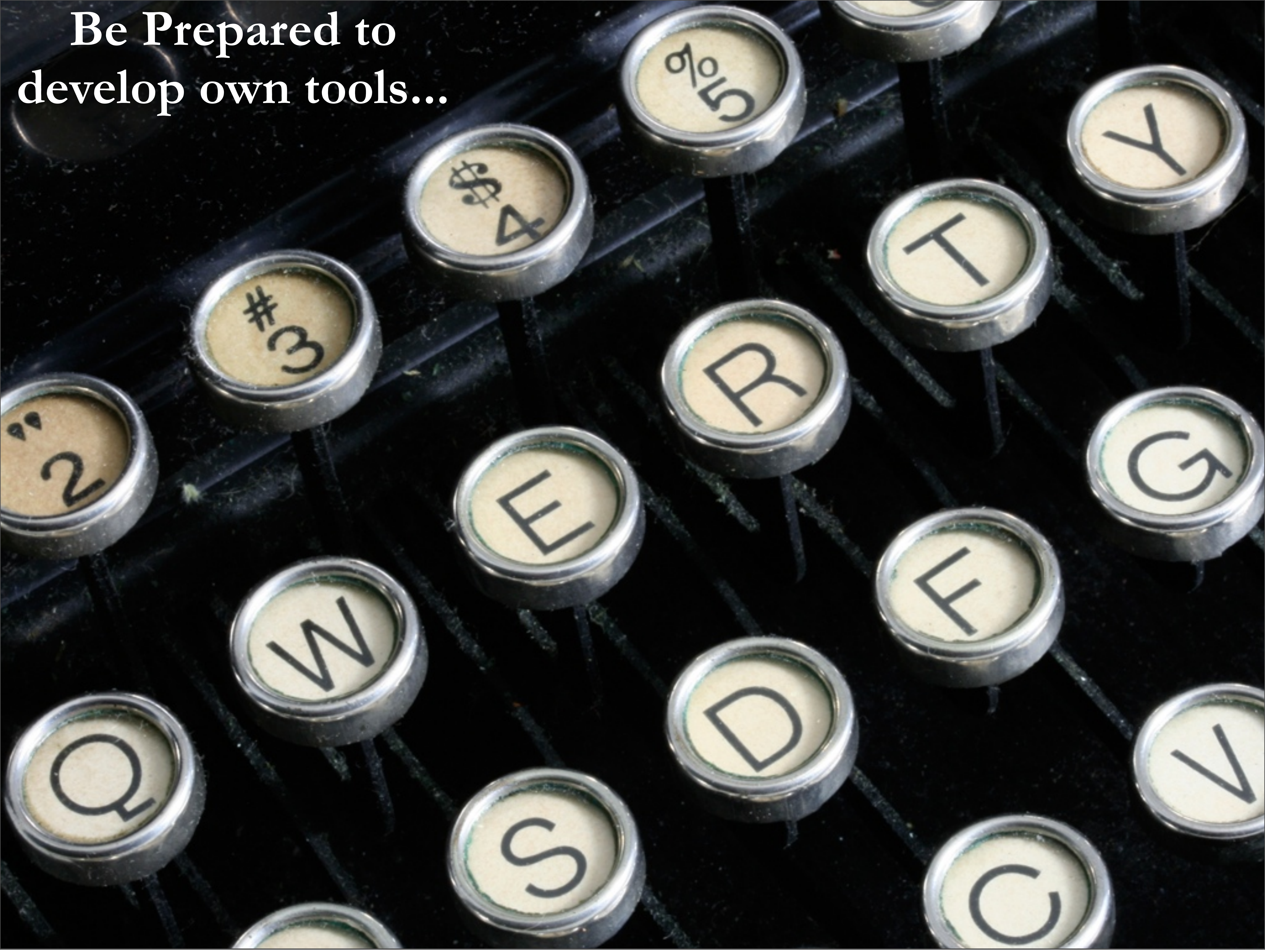
# Keep the Goal in Mind

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.

... 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

Mississippi State UNIVERSITY

JAMES WORTH BAGLEY COLLEGE OF ENGINEERING MISSISSIPPI STATE UNIVERSITY