ReSCIND Performer HSR Dataset
Cognitive Task Analysis Study Cover Sheet – ASCEND Project

ReSCIND

Dataset Details

Dataset Title:	ASCEND CTA Study		
Dataset Citation:	Gluck, K., Cranford, E. A., Pirolli, P., Blazek, S., Solway, A., Sanchez, H., Odem, T., Raj, A., Mather, B., & Denker, G. (2025). ASCEND Cognitive Task Analysis Study [Data set]. SRI, Menlo Park, California, USA. https://doi.org/10.17605/OSF.IO/56AXZ		
Data Format:	Word (.docx), Excel (.xlsx), Text (.txt), PDF (.pdf), MentalModeler files (.mmp, .png), and Test range raw Zip archives	Uncompressed Data Size:	5 GB
Dates & Duration:	November 13, 2024 – December 3, 2024 (N=5) Two in-person sessions per participant	Time Zone:	UTC for cyber test range data; CT for interview transcripts
How to access dataset:	https://ascend-data.sri.com		
Point of Contact for data questions:	ascend-info@sri.com		

Description of Scenario

Experiment Objectives

1. To jumpstart and accelerate MIMICK implementation, ASCEND's Phase 1 technical work included Cognitive Task Analysis (CTA) Human Subjects Research (HSR) to identify attackers' cognitive processes, decision-making factors, and actions, grounded in the Capture the Flag (CTF) task context that has been a focus of the ReSCIND Phase 1 investments. CTA is a systematic approach to achieving an understanding of knowledge, decision-making, and planning processes. Founded in the idiographic and ethnographic research traditions, it relies on domain analysis, subject matter expert (SME) input, and semi-structured interviews to produce actionable insights.

2. We down-selected from a broad range of CTA methods to tailor our design for maximum information value in the time and budget scope available. We selected the following methods for inclusion in this protocol: Task Diagrams, Goal-Directed Task Analysis, FCM Interviews, Recent Case Walkthroughs, and CTF tasks with concurrent think-aloud verbalizations.

3. Key outputs of these methods include the following:

- *Task Diagrams:* These flow diagrams decompose CTF tasks into 3-6 key steps and subtasks, offering a clear visualization of task workflow mental models.

- *Goal-Directed Task Analysis:* By hierarchically mapping task goal structures, decision requirements, and influencing factors, this analysis provides insights into the complexities of SME decision-making and the core concepts guiding their actions.
- *Fuzzy Cognitive Maps:* These maps, constructed from semi-structured interviews, reveal the causal relationships between concepts within CTF tasks, helping to model the factors driving SME strategies and outcomes.
- *Recent Case Walkthrough:* The walkthrough entails guided recall of decision-making during a specific recently completed CTF.
- *CTF Challenge w/Concurrent Verbal Protocols:* This non-elaborative talk-aloud while performing CTF to identify critical events and cues, judgments, and decisions provides a trace of attended information in working memory and the environment.

4. Together, these results provide a rich understanding of the cognitive processes behind CTF task performance, offering critical insights for refining the design and development of C3M systems. We analyze these data to develop a model of their goal structures, mental models, cognitive processes, and decision-making, and map these down to the traces of their actions with the platform. These models and this mapping from cognition to behavior will be a foundation for inferring the hacker mental states and processes from online activity.

Experiment Description

5. Five SMEs each participated in two hybrid remote and in-person sessions over two nonconsecutive days (4.5 hours total for each participant), with screen and voice recordings collected via Zoom (not made publicly available due to privacy concerns). This setup ensured the capture of rich, detailed, high-quality data concerning expert cognition essential for informing MIMICK design and functionality.

6. On the first day, lasting 2.5 hours, activities include check-in, signing consent forms, completing demographic and professional expertise questionnaires, and engaging in Task Diagram development, Goal-Directed Task Analysis, and FCM interviews, with breaks provided as needed. The second day, lasting 2 hours, involves a review of a recent case, participating in two CTF challenge tasks with concurrent verbalization, and a debriefing session, including time for breaks. The protocol collects comprehensive participant data while adhering to Institutional Review Board (IRB) approval guidelines.

7. The CTA comprises multiple methods, including:

- *Task Diagrams.* Task Diagramming aims to elicit a broad overview of how an SME thinks about the overall structure and flow of a task, in this case, a CTF. The interviewer asks the SME to decompose the task into an ordered sequence of three to six subtasks.
- *Goal-Directed Task Analysis.* The purpose of the Goal-Directed Task Analysis is to unpack the high-level structure provided by the Task Diagram into a more detailed representation that includes:
  - Any further decomposition of the subgoals identified in the Task Diagram into sub-subgoals.
  - Decisions that must be made to achieve each subgoal and sub-subgoal.
  - The information requirements associated with making each of those decisions at three levels of analysis:
    (a) Basic perceptual information/data available in the environment.
    (b) Integration of that information/data to draw implications or conclusions about the current state of things.
    (c) How that information/data would be expected to change over time, if at all.
- *FCM Interviews.* An FCM is a graph-based representation of subjective causal beliefs: how people believe a change (i.e., an increase/decrease or a change between on and off states) in one concept impacts another. The nodes are the concepts, and the edges are the causal relationships between them. Interviews first seek to

define core concepts and then identify associated concepts with relationship types. This iterates outward from the associated concepts, asking "what drives" each new concept. MentalModeler is a common software tool for constructing graphs during interviews and is used here.

- *Recent Case Walkthrough.* The purpose of the Recent Case Walkthrough is to elicit from the SME a brief yet detailed accounting of how they handled a recent specific CTF. It will reveal what is most salient from their episodic memories of that event.
- *CTF with Verbal Protocol.* The purpose of the CTF with concurrent verbal protocol is to understand what people think about when performing the CTF task. Participants speak only about the things they naturally think about. The verbal protocol data will provide a way to compare decision processes that participants actually engage in when performing a task versus how they represent and think about the task as elicited through the structured interviews.

8. Each participant completed the treatment version of two CTF challenges while concurrently thinking aloud. Participants were pseudo-randomly assigned to challenges across the five bias types (described in the subsequent section) so that each participant experienced two different biases, and so all bias types and versions were sampled across participants. ***Table 1*** depicts the CTF challenge-to-participant assignment, and the time allotted for each. Each participant was allotted a total of 30 minutes to complete the two challenges.

The CTA study used challenges and surveys from the ECSC and EkoParty experiments. Thus, for challenge descriptions and blank surveys, please see:

https://ascend-data.sri.com/experiment-conf-ecsc-2024/
  - For Loss-1a and b, Rep-8a and b
- https://ascend-data.sri.com/experiment-conf-ekoparty-2024/
  - For Anch 1A and B, Cult-1, Cult-5 and Conf 5A and B

Table 1. CTA CTF Challenge Distribution

Scenario ID	Scenario Name	P1	P2	P3	P4	P5	Allotted Time (min)
Loss-1a	Fun and Games with User Accounts	2nd					20
Loss-1b	Lands of Fruits		2nd				20
Rep-8a	Website Party Favors				2nd		15
Rep-8b	Illegal Backward Pass	1st					10
Anch 1A	It's All a Gamble					1st	10
Anch 1B	Ante Up		1st				10
Cult-1	Intranet if you can					2nd	20
Cult-5	Forward Me the Flag			1st			10
Conf 5A	War and Peas			2nd			20
Conf 5B	Peakaboo				1st		15

9.

10. The following cognitive vulnerabilities (CogVulns) were examined in the CTA CTF design described above in ***Table 1***.

- *(Loss) Loss Aversion:* The tendency for people to strongly prefer avoiding losses over acquiring gains (value functions that relate subjective to objective losses are steeper than value functions that relate subjective to objective gains).
- *(Rep) Representativeness:* The tendency for people to judge the probability or frequency of a hypothesis by considering how much the hypothesis resembles available data.

- *(Anch) Anchoring:* The tendency to rely too heavily on, or overly restrict one's attention to, one trait or piece of information when making judgments. The information in question can be relevant or irrelevant to the target decision, as well as numerical or non-numerical. Includes focalism or the focusing illusion.
- *(Cult) Socio-Cultural:* The tendency to interpret and judge phenomena in terms of the distinctive values, beliefs, and other characteristics of the society or community to which one belongs. This sometimes leads people to form opinions and make decisions about others in advance of any actual experience with them.
- *(Conf) Confirmation:* The tendency to search for or interpret information in a way that confirms one's preconceptions.

11. From each of the five SME participants, we have approximately 4.5 hours of recorded Zoom video (not made publicly available due to privacy concerns) and associated transcripts, semi-structured interview content from the Task Diagramming, Goal-Directed Task Analysis, Fuzzy Cognitive Mapping, and Recent Case Walkthrough activities, and the log files generated by SimSpace from the two CTFs they each completed.

Experimental Results

12. Analysis of the CTA data includes manual summarization and documentation of the knowledge, strategies, and decision-making processes reported by participants during the interviews. We also use the data to compare and contrast participant mental model descriptions of how they think about CTFs (TD, GDTA, and FCM tasks) to how they actually solve CTFs (RCW and CTF tasks), as well as comparison across participants to assess individual differences.

13. Separate analytical development (e.g., CTA analysis, FCM Interviews, workflow analysis) showed the potential of these methods to complement one another in representing attacker knowledge, modeling behavioral evolution, and inferring intent. FCMs proved effective for capturing and aggregating attacker knowledge and beliefs from heterogeneous data sources. Dynamic Behavior Embeddings (DBEs), scoped for future implementation, were defined to capture temporal patterns of attacker behavior and enable intent trajectory analysis. Information Foraging Theory (IFT) provided an interpretable framework for modeling attacker decision-making patterns, adapted from prior work in information-seeking behaviors. Collectively, these analytical explorations underscored the value of integrating knowledge, behavior, and decision-making to expose cognitive and tactical vulnerabilities.

Data

Primary Data Sources

Data includes the following:

1. Demographics
2. Experimenter notes
3. Participant notes, drawings, and diagrams
4. Zoom Closed Caption transcripts for each task
5. CTA Task Worksheets
6. Fuzzy Cognitive Map results
7. CTF data

Category	Data Sources	Examples of Select Data Features
Demographics	Questionnaire	Age, gender, education, and cyber expertise
Experimenter Notes	Word document	General notes about experimentation, including what went wrong or went well during interviews for each task

Category	Data Sources	Examples of Select Data Features
Participant Notes Drawings Diagrams	PDF files	Diagrams from Task Diagraming and Goal-Directed Task Analysis Notes taken and diagrams made during Recent Case Walkthrough Notes taken during CTF challenges
Zoom Closed Caption Transcripts	Text files	Cleaned and deidentified closed caption transcripts generated by Zoom during recorded interviews, separated by task.
CTA Task Worksheets	Excel spreadsheets	Interview worksheets for taking notes and recording responses for the Task Diagraming and Goal-Directed Task Analysis tasks, and the Recent Case Walkthrough task
Fuzzy Cognitive Map results	MentalModeler files (*.mmp) for use with MentalModel software (www.mentalmodeler.com)	Source files for fuzzy-logic cognitive maps created during the Fuzzy Cognitive Map interviews, which can be loaded and viewed using the MentalModeler software.
	PNG files	Image files of the fuzzy-logic cognitive maps created during the Fuzzy Cognitive Map interviews.
CTF Data	*Kali Linux (participant workstation) Instrumentation*	
	• Screen capture	Full session video capture of participant desktop
	• Terminal logger (using *script* command)	All terminal commands entered and responses provided by the system. Captures stdin and stdout plus timing data. This data includes all activity conducted in remote ssh sessions.
	• Keylogger	Delta time key press events in all applications (extract rates, commands)
	• Click logger	Mouse clicks
	• Cursor logger	Movements and actions of mouse cursor
	• Clipboard logger	Copies of clipboard contents
	• Menu logger	Command invocations from menu bar
	• Web logger	Browser mouse clicks mapped to tabs, plus keys pressed
	• *Snoopy*	System processes started
	Target System Syslog	
	• Journal	All system events, including logins
	• auth.log	Successful and failed login attempts via console, terminal, and ssh
	• nginx/access.log • php.log	Web server logs, including pages accessed, data served (including flags)
	• Roundcube.log	Successful and failed email login attempts by account
	Kali Linux VM, *tcpdump*: PCAP full packet capture data	Timestamped network communication packets, including payloads. Where possible, unencrypted communications were used to enable extraction of remote logins and information accesses.

Derived Data Sources

Datasets created from aggregating, analyzing, curating, and labeling the source data

Category	Data Sources	Examples of Select Data Features
LLM Summaries	Word document	ChatGPT 4o summaries of Recent Case Walkthrough interviews and strategy comparisons to strategies identified in the Task Diagram and Goal-Directed Task Analysis interviews.
Task Explorer Data	.csv files	14. Task Explorer Pipeline (TEP) is a framework for extracting key strategies and subtasks in each CTF challenge. It describes the distinct families of interrelated tool-based strategies and subtasks participants follow or perform while attempting to capture a flag. Strategies are reflected in the tools participants use over time—represented as sequences of tool use—called command traces. As command traces are analyzed, strategic decisions surface through the tools that participants use and the composition in which they use them

Research

Hypotheses

15. There are no hypotheses for this research. It was not conducted in the hypothetico-deductive tradition, but in the idiographic/ethnographic tradition. The ASCEND CTA study is an exploratory study to identify attackers' cognitive processes, decision-making factors, and actions, grounded in the CTF task context. The analysis of this rich source of data can be used for many purposes, including developing cognitive models of attacker behavior.

Publications

See http://ascend-data.sri.com/docs/publications.

References

Anderson, J.R. (1990). *The adaptive character of thought*. Lawrence Erlbaum Associates.

Chi, E.H., Rosien, A., Heer, J. (2003). LumberJack: Intelligent discovery and analysis of web user traffic composition. In *Proceedings of the 4th International Workshop on Mining Web Data for Discovering Usage, 2703,* (pp. 1-16). Springer: Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-39663-5_1

Dalton, A., Dorr, B., Liang, L., & Hollingshead, K. (2017). Improving cyber-attack predictions through information foraging. *IEEE International Conference on Big Data (Big Data)*, (pp. 4642-4647). Boston, MA.

Ericsson, K. A., & Simon, H. A. (1984). *Protocol analysis: Verbal reports as data.* The MIT Press.

Fu, W., & Pirolli, P. (2007). SNIF-ACT: A model of user navigation on the World Wide Web. *Human Computaer Interaction*, *22*(4), 355-412.

Giabbanelli, P.J., & Napoles, G. (Eds.). (2024). *Fuzzy Cognitive Maps: Best practices and modern methods*. Springer Cham. https://doi.org/10.1007/978-3-031-48963-1

Hoffman, R.R., Crandall, B., Klein, G., Jone, D., & Endsley, M. (2008). *Protocols for Cognitive Task Analysis*. Florida Institute for Human and Machine Cognition, Pensacola, FL. https://www.ihmc.us/wp-content/uploads/2025/06/Protocols-for-Cognitive-Task-Analysis.pdf

Lawrance, J., Burnett, M., Bellamy, R., Bogart, C., & Swart, C. (2010). Reactive information foraging for evolving goals. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Atlanta, Georgia, USA. https://doi.org/10.1145/1753326.1753332

Lawrance, J., Bogart, C., Burnett, M., Bellamy, R., Rector, K., & Fleming, S.D. (2013). How programmers debug, revisited: An Information Foraging Theory perspective. *IEEE Transactions on Software Engineering*. *39*(2):197-215. doi:10.1109/TSE.2010.111.

Lebiere, C., Pirolli, P., Thomson, R., Paik, J., Rutledge-Taylor, M., Staszewski, J., & Anderson, J.R. (2013). A functional model of sensemaking in a neurocognitive architecture. *Computational Intelligence and Neuroscience*, *921695, 1-29*. https://doi.org/10.1155/2013/921695

McFadden, D. (1974). Conditional logit analysis of qualitative choice behavior. In P. Zarembka (Ed), *Frontiers of econometrics*. Academic Press.

Militello, L. G., & Hutton, R. J. (1998). Applied cognitive task analysis (ACTA): a practitioner's toolkit for understanding cognitive task demands. *Ergonomics*, *41*(11), 1618–1641. https://doi.org/10.1080/001401398186108

Oaksford, M., & Chater, N. (Eds.). (1998). *Rational models of cognition*. Oxford University Press.

Olston, C., & Chi, E.H. (2003). ScentTrails: Integrating browsing and searching on the web. *ACM Transactions on Computer-Human Interaction*, *10*(3), 177-197.

Pirolli, P. & Card, S.K. (1999). Information foraging. *Psychological Review*, *106*, 643-675.

Schraagen, J.M., Chipman, S.F., & Shalin, V.L. (Eds.). (2000). *Cognitive Task Analysis (1st ed.)*. Psychology Press. https://doi.org/10.4324/9781410605795

Stephens, D.W., & Krebs, J.R. (1986). *Foraging theory*. Princeton University Press.