Raven Eye: A Mobile Computing Solution for Site Exploitation

Juan Miguel Archuleta, Sergio R. Jimenez, Ben Kline, Diana A. Tsang, and Steven J. Henderson

Department of Systems Engineering
United States Military Academy
West Point, New York

Corresponding author's Email: Sergio.Jimenez@usma.edu

The views expressed herein are those of the author and do not reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.

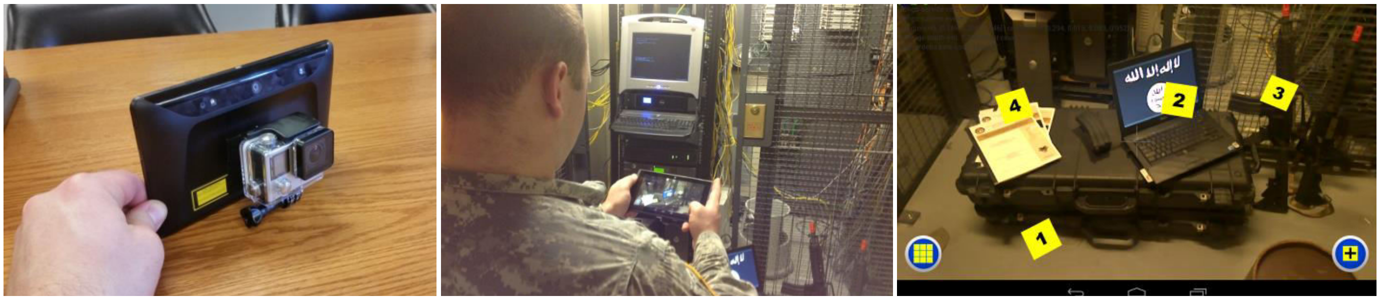

Figure 1. The Raven Eye system (left) is used by a soldier (center) to exploit a sensitive site. A screen capture from the system (right) shows tracked, virtual tags (yellow numbers) which annotate and geo-locate items of interest as the soldier navigates the scene.

Abstract: Site exploitation (SE) remains a critical mission for operators on the battlefield. Since SE is a fairly new operation in the military, soldiers face specific challenges that hinder them from conducting a successful SE operation. This paper details the design of a system, *Raven Eye*, which endeavors to improve the efficiency and effectiveness of SE. Raven Eye is an Android based system that collects, stores, and sends SE data. Raven Eye allows operators to collect exploited site data by capturing photos, videos, and biometrics. Operators can annotate and tag recorded items. Lastly, the operators transform data stored and collected via Raven Eye to a standardized report that accelerates follow-on analysis by intelligence personnel.

Keywords: Site Exploitation, Android, Military Intelligence, Scrum Methodology, Forensic Science, Graphical User interface