As a law enforcement first responder (LEFR), it is your job to arrive at a scene, gather as much information as possible, and analyze the information for leads, all while preserving evidence in the process. Many LEFRs are simply not prepared when presented with cyber crimes. The aim of CLEW is to turn any first responder into a competent cyber investigator.

This tool is being developed by the National Center for Supercomputing Applications (NCSA) at the University of Illinois in collaboration with the FBI, Springfield, IL Division. It is a continuation of NCSA’s Live Computer System Capture and Triage Tool (CCTT) project, which has been received with enthusiasm by the local police departments.

### Goals

**User-Friendly:** LEFR are not trained cyber investigators; the tool should contain an interface that is easy to use and understand

**Effective:** Should provide the LEFR with useful information that can quickly start an investigation

**Portable:** Cannot be physically restraining and should be compatible with many systems

**Robust and reliable:** First responders will depend on this tool; it should be robust, or at least easily adaptable, while ensuring that the LEFR uses up-to-date software

**Minimal footprint:** Information gathering is important; however, if the case is criminal, it cannot damage any potential evidence contained on the computer (registry, timestamps, etc.)

### Fundamental Questions

**Design/Direction-Based Questions:** For which situations will this tool be useful? What kind of data is important to an investigator? How can this be incorporated into an LEFR’s toolset? Where does communication occur on the internet? How much (or little) information could the LEFR have?

**Technical/Implementation Questions:** Which language(s) should be used for implementation? How can we ensure that the LEFR’s tool is up to date? How can we reduce our footprint for future forensics? What can we do if we don’t have user credentials? How to provide efficiency while maintaining robustness?

### Results

**Support**

- Operating Systems: Windows XP and Windows 7
- E-Mail Clients: G-Mail, Windows Live, Yahoo!, AOL, Outlook
- Instant Messengers: Windows Live, Yahoo!, AOL
- Social Networking Sites: Facebook

### Data capture

- Live system state (COFFE backend)
- E-mail messages and headers
- Instant messenger conversations and logs
- Facebook friends, activity, and media
- Graph API with XML parsing of Facebook mobile

### Analysis

- Visually displays various statistics to LEFR on scene
- Provides LEFR with photos of suspects and victim
- Searches data for inputted key words or phrases
- Saves data to USB for archiving and investigation

### Other Features

- Bypass site’s login with user’s session cookies
- Access saved credentials in Firefox, IE, and Chrome
- Reduces footprint by running Lobo browser on a USB

### Future Work

**Maintenance:** provide automatic updates for reliable service when interfaces change

**Expansion:** create new modules to support more operating systems (Mac OS, Linux) and social networking sites (MySpace, Twitter)

**Testing:** gain feedback and implement ideas from officers’ on-the-job experiences