California Cyber Crime Center (C^4)
Cyber Response Vehicle

C^4 provides investigative and prosecutorial support on a wide range of cyber crime incidents encountered by law enforcement. As a part of its support model, C^4 offers the Cyber Response Vehicle (CRV) to serve as a mobile cyber laboratory. The CRV is a purpose-built digital forensics center that allows multiple staff to work as if they were in the computer lab to collect, acquire and process loose media, mobile devices, personal computers, servers and other sources of electronically stored information (ESI) during the course of an investigation. It provides a designated workspace for examiners, legal and investigative personnel working together. With the latest technology and digital evidence gathering tools onboard, the CRV is a turn key solution that can respond to a wide variety of digital forensics needs whether a simple mobile device, PC, or a more advanced server network to capture, preserve and analyze data onsite. The CRV may be deployed in situations where rapid collection of digital evidence is essential for successful investigations of crime. It is stationed in Sacramento and can be anywhere within Northern California within a few hours.

The CRV is equipped with the following:

- Two Digital Evidence Workstations loaded with the latest digital forensics tools for imaging and examination of PC/Server/Loose Media and other Dead/Live Box applications
- Digital Evidence Processing Server dedicated to the high speed processing of evidence for presentation to Litigation Support or other agencies
- Two PC workstations to provide remote connectivity to DOJ applications, databases and systems
- Super Imager that performs high speed forensic data extractions from computers/laptops, hard drives and portable/removable media
- Mobile phone/tablet Kiosk including Cellebrite, XRY and Susteen SecureView mobile forensic investigative devices
- 24 Terabyte data storage device for the electronic storage of evidence gathered
- Secured wireless dual band network to provide connection to internet as well as provide additional coverage for agency phones and mobile devices in near proximity
- Evidence documentation center for photos, documentation and proper tagging of evidence
- 7KW gasoline powered generator to provide an independent power source if required

Example Use Cases

There are a variety of situations that may require the immediate gathering of ESI located on various digital devices that cannot be gathered through traditional methods in a timely manner.

(1) Lab-quality response onsite to analyze large amount of evidence or avoid business disruption
Seizing information technology equipment to take back to a lab to preserve and analyze is not always practical due to the volume of evidence (e.g., cases involving numerous computers). In these cases, there is inevitably a lot of evidence to analyze and substantial processing power is needed on site. Other times, evidence sits on production servers and business computers but business operations must be kept uninterrupted during the course of an investigation. Past practices consisted of setting up a temporary lab by bringing equipment in multiple vehicles and spending hours in setup and takedown; this also required coordination as well as identifying available space and power for equipment. The CRV eliminates the need for a temporary on-site lab set-up and provides a high-efficiency mobile alternative as it can arrive on scene already setup and ready to triage, acquire, and process digital evidence immediately.

(2) Mobile capabilities to acquire evidence from citizen footage captured on phones
As the proliferation of mobile devices with high quality cameras continues, witnesses are recording and/or photographing critical incidents, such as an officer involved shooting or hostage situation. This potentially valuable evidence may prove important for the investigation and prosecution of those responsible. Current methods would require that the cell phones be brought to a forensic-capture capable location to be processed. When citizens are advised that their cell phones may be kept by law enforcement for multiple days to conduct analysis, they will understandably be hesitant to consent. The CRV allows C^4 to arrive on scene and begin capturing evidence from these sources that we otherwise may not have been able to access.

(3) Immediate onsite analysis to support search warrant execution
The CRV can provide key operational support in tactical situations to law enforcement teams serving warrants. In cases where there are multiple locations to be served, timely analysis and delivery of information at one site can be critical to the service of subsequent warrants and the overall safety and success of the investigation. It may be crucial to understand if suspects have made contact with associates at other locations that are the focus of the next warrant(s). In other cases, if an interview is being conducted with a suspect on-site, real-time feedback provided through digital forensics could help investigators ask the right questions and or corroborate the information related to his/her computers being shared.