



FAQ – California Cyber Crime Center (C⁴)

1. What is the California Cyber Crime Center (C⁴)?

C⁴ brings together the California Department of Justice's (DOJ's) resources to investigate and prosecute cyber crime, enhance digital evidence capabilities, and promote innovation. C⁴ supports DOJ internally as well as local and state law enforcement agency partners throughout the cyber crime lifecycle by providing services, technical assistance, and training related to cyber crime, digital evidence, and digital forensics. C⁴ also advances DOJ's internal capabilities to utilize digital evidence for investigations and litigation.

2. What types of services do you currently offer?

The mission of C⁴ is to combat and prevent crime by harnessing the Department's expertise in cyber crime, cyber security, and digital evidence by offering technical assistance, training, and case-specific services, including:

- Digital forensics analysis support (e.g. cell phones, social media, etc.)
- Investigation and prosecution of cyber crimes
- Technical assistance for cyber crime investigation and prosecution
- Technical assistance for network security
- High quality cybercrime and security training on digital evidence, legal services, and investigations
- Research and development of advanced forensic tools, techniques, best practices, and policy recommendations regarding cyber crime

3. How do I access those services?

To access services you may contact C⁴ at C4@doj.ca.gov or (916) 210-5001. Please describe the specific service you are requesting, pertinent case details (e.g. timeline requested), as well as contact information to allow us to follow up. If you are not requesting C⁴ services, but are a member of law enforcement or the public who need assistance reporting an Internet crime occurring in California, contact your local Law Enforcement Agency, local High Crimes Task Force, or the Attorney General's [eCrime Unit](#).

4. Can I suggest a new service?

Yes, you may contact C⁴ at C4@doj.ca.gov or (916) 210-5001. Please describe the service you are requesting as it relates to the scope and mission of C⁴. Also, please provide any specific details regarding the service that you would like to see from C⁴ in the future. C⁴ may follow up to request further information, however is unable to provide ongoing updates on the request.

5. Where can I find the DOJ mobile device kiosks?

The DOJ Bureau of Forensic Services (BFS) is a comprehensive, state-of-the-art system accredited by the American Society of Crime Laboratory Directors, Laboratory Accreditation Board (ASCLD/LAB-International). Available to law enforcement at each laboratory location are mobile device kiosks for extracting cellular phones. Laboratories locations:

- Richmond DNA Laboratory
1001 West Cutting Blvd, Ste. 110
Richmond, CA 94804
(510) 620-3300
- Sacramento Laboratory – Digital Evidence Program
4949 Broadway, F-147
Sacramento, CA 95820
(916) 227-3623

- Fresno Laboratory
California State University, Fresno
5311 North Woodrow Ave
Fresno, CA 93740
(559) 294-4000
- Riverside Laboratory
7425 Mission Blvd
Riverside, CA 92509
(951) 361-5000
- San Diego Division of Law Enforcement
(Contact Riverside Laboratory for more information)

6. What is required to use the mobile device kiosk?

You need to be a representative of a law enforcement agency or district attorney office. You must also successfully complete a short training program on the use of the kiosk and technologies available. The laboratory that supports the kiosk you'd like to use will schedule and provide the training.

7. How long does it take for a particular service?

Completion timelines depend on the complexity of the service requested. Some services take longer depending on whether the service requested is a cell phone extraction versus investigation and prosecution of cyber crime, as an example. When you request service from C⁴ please ensure to include your desired timeline of completion in order to be processed accurately. C⁴ will follow up with you regarding completion of the service.

8. For services not offered, where do you suggest I go to meet my needs and get other resources?

For more information regarding resources for victims of cyber exploitation and tools for law enforcement, please visit the DOJ's cyber exploitation page [here](#). To report an Internet crime that has occurred in California, contact your local Law Enforcement Agency, your local High Crimes Task Force, or the Attorney General's [eCrime Unit](#). We encourage all victims of Internet Crimes to contact [The Internet Crime Complaint Center \(IC3\)](#) as well. For more information on these agencies, see the C⁴ website.

9. How do I get assistance with investigations in which the crime(s) is multi-jurisdictional or involves intellectual property, piracy, or counterfeiting?

You may file a police report with local law enforcement. Also, as stated above, to report an Internet crime that has occurred in California, contact your local Law Enforcement Agency, your local High Crimes Task Force, or the Attorney General's [eCrime Unit](#). We encourage all victims of Internet Crimes to contact [The Internet Crime Complaint Center \(IC3\)](#) as well. For more information on these agencies, again see the C⁴ website.

10. How does a law enforcement agent upload search warrant notification information as required by California Penal Code 1546.2?

Please use our on-line form located in California Law Enforcement Website (CLEW) to submit search warrant notification documents. To create a CLEW account:

- Go to the CLEW Sign Up Page <http://clew.doj.ca.gov/user> and click on the "I want to create an account" tab in the upper right side.
- You will need to know the ORI for your agency and then complete the required information.
- Complete and submit the request
- You will receive notification when approved.
- The site also provides further directions on the uploading process.

11. Where can I find the DOJ published search warrant notification information provided by law enforcement?

You can find this information on [OpenJustice](#) in the [Open Data section](#) of the DOJ website, under Electronic Search Warrant Notifications.

12. Do you provide resources regarding cyber safety for children and adults, cyber security, preventing identity theft, and/or privacy topics?

As part of the Attorney General's initiative to combat cyber exploitation, you can find various resources for victims and tools for law enforcement on the [Cyber Exploitation](#) page. The DOJ webpage on [Cyber Safety](#) also has an abundance of resources including:

- **Children Online:** Everyone has a role to play in ensuring that our children are smart, safe, and legal online. See the DOJ's [Protecting Children Online](#) webpage for informational guides and educational resources for parents, educators and all of us.
- **Privacy:** The Privacy and Enforcement & Protection Unit within DOJ:
 - Enforces state and federal privacy laws.
 - Empowers Californians with information on their rights and strategies for protecting their privacy.
 - Encourages businesses to follow privacy-respectful best practices.
 - Advises the Attorney General on privacy matters.
 - Visit the [Privacy Enforcement and Protection](#) page for resources and tips for consumers, businesses and others on a wide range of privacy issues.
- **Identity Theft:** In California, all forms of identity theft are crimes (Penal Code section 530.5 et.seq.). For more information on Identity Theft for Consumers and Identity Theft Alerts visit the [Identity Theft](#) webpage.
- **eCrime Unit:** The eCrime Unit identifies and prosecutes large-scale identity theft crimes, cyber crimes, and other crimes involving the use of technology. Such as: identity theft, child exploitation, fraud committed using the Internet, theft of computer components or services, and intellectual property crimes. For more information, see [eCrime Unit](#).
- **Data Security Breach Reporting:** Data breaches and other privacy violations place the privacy, security, and economic wellbeing of businesses and consumers at risk. California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Visit the [Data Security Breach Reporting](#) page for more information.