

Fuente fotográfica: FBI Law Enforcement Bulletin.



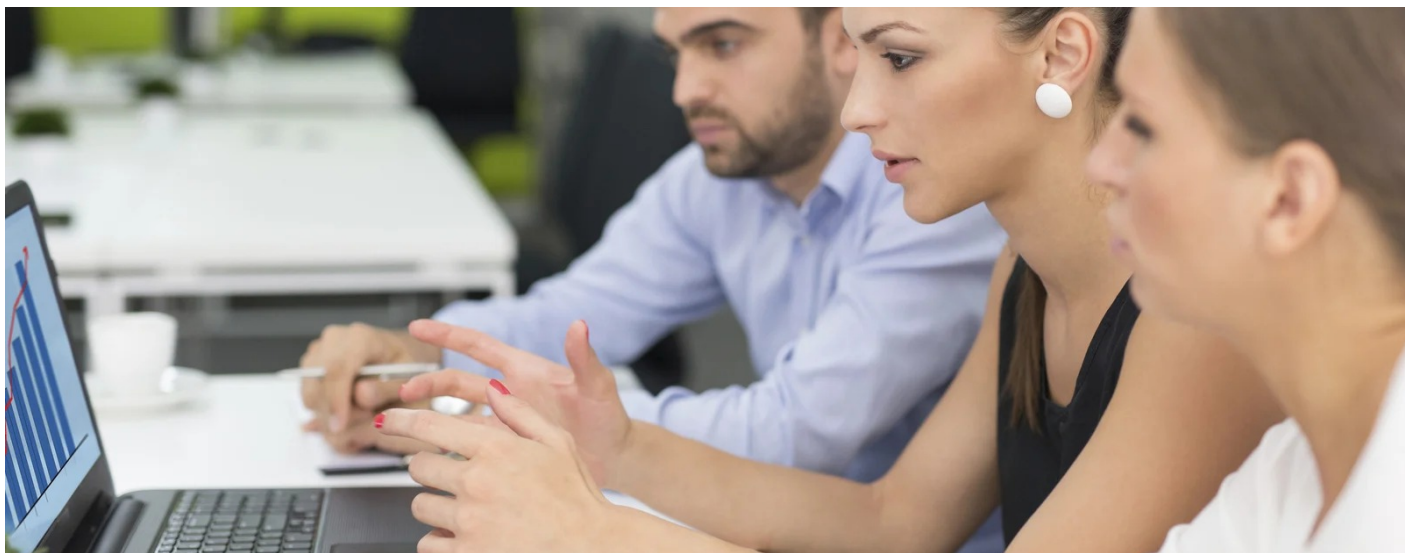
Fuente fotográfica: FBI Law Enforcement Bulletin.



3. El teléfono móvil como fuente de evidencia

Los celulares pueden conservar conversaciones, registros de llamadas, ubicaciones, fotografías, archivos y datos de aplicaciones relevantes para una investigación.

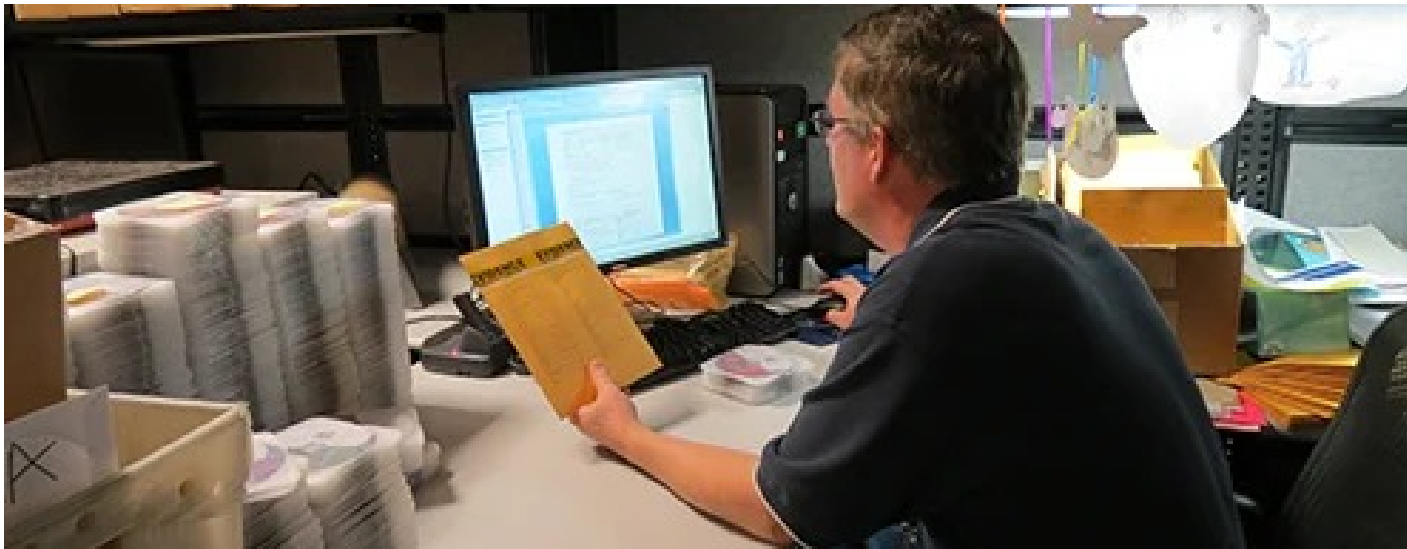
Fuente fotográfica: FBI Law Enforcement Bulletin.



4. Análisis colaborativo de información

Los equipos de investigación comparan datos, relacionan eventos y elaboran hipótesis para interpretar grandes volúmenes de información digital.

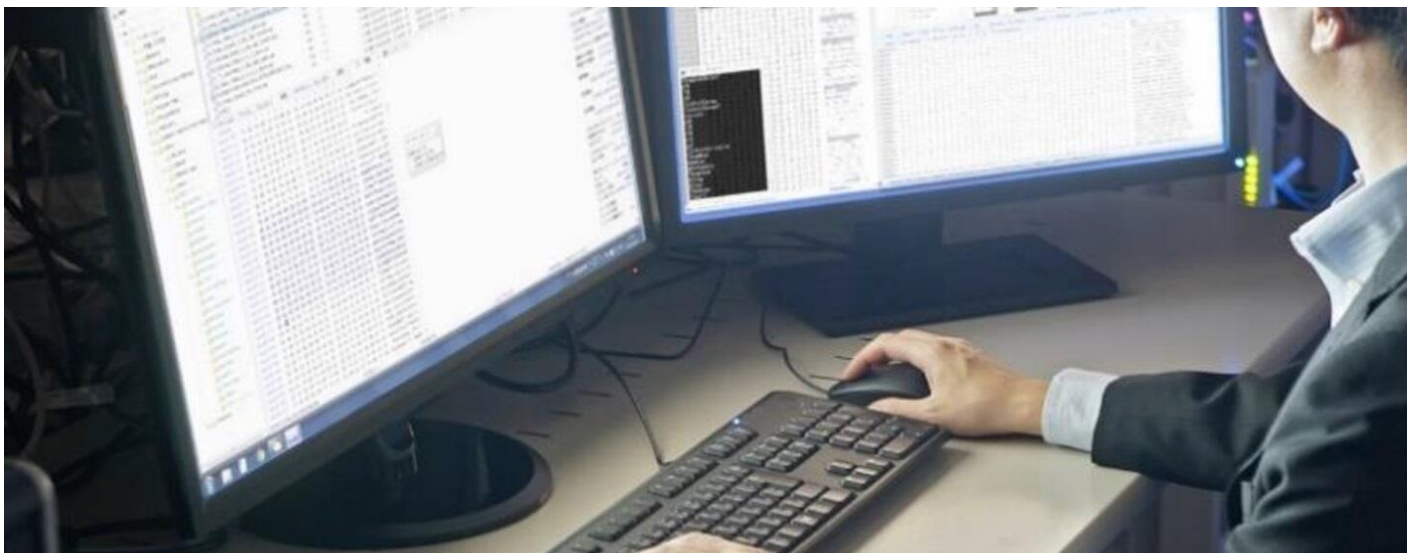
Fuente fotográfica: Federal Bureau of Investigation (FBI).



5. Revisión y clasificación de soportes

La evidencia puede encontrarse en discos, computadoras, memorias, cámaras, servidores y otros medios. Cada elemento debe identificarse y documentarse correctamente.

Fuente fotográfica: Federal Bureau of Investigation (FBI).



6. Estación profesional de análisis forense

El especialista emplea programas y equipos específicos para duplicar soportes, recuperar archivos, revisar metadatos y examinar registros del sistema.

Fuente fotográfica: NTT Advanced Technology.



7. Investigación de incidentes informáticos

El análisis de pantallas, archivos y conexiones ayuda a detectar accesos no autorizados, sabotajes, fraude, amenazas y otras conductas delictivas.

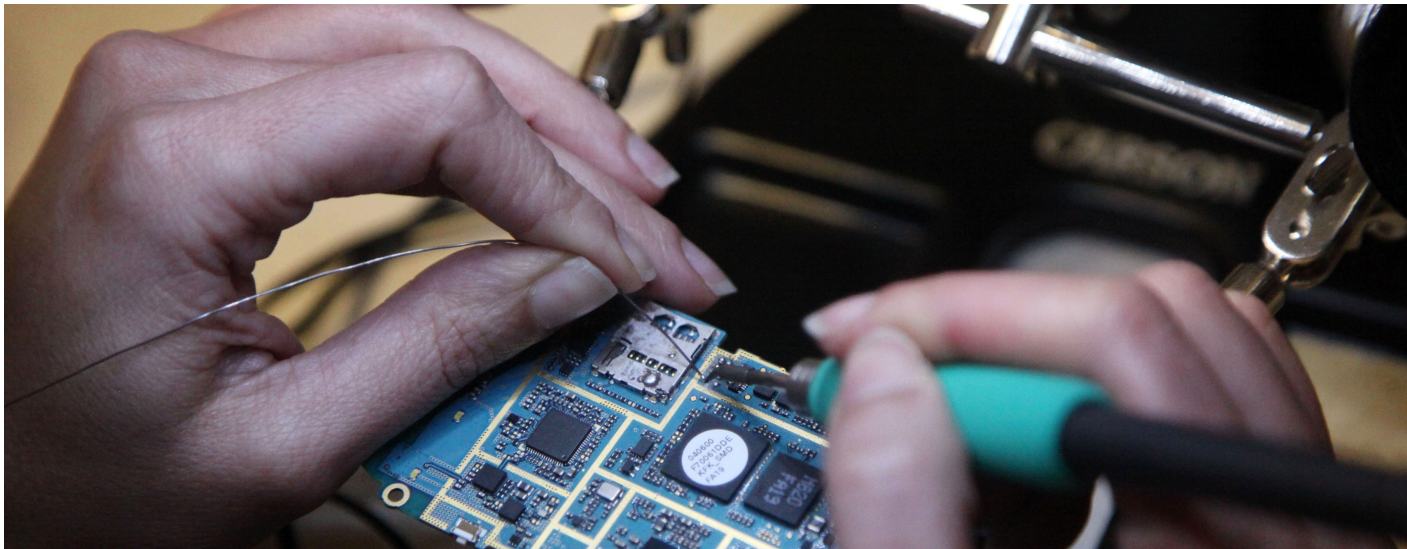
Fuente fotográfica: SalvationDATA.



8. Monitoreo de redes y correlación de datos

La observación de conexiones y eventos permite reconocer patrones, vincular actividades y reconstruir la secuencia temporal de un incidente digital.

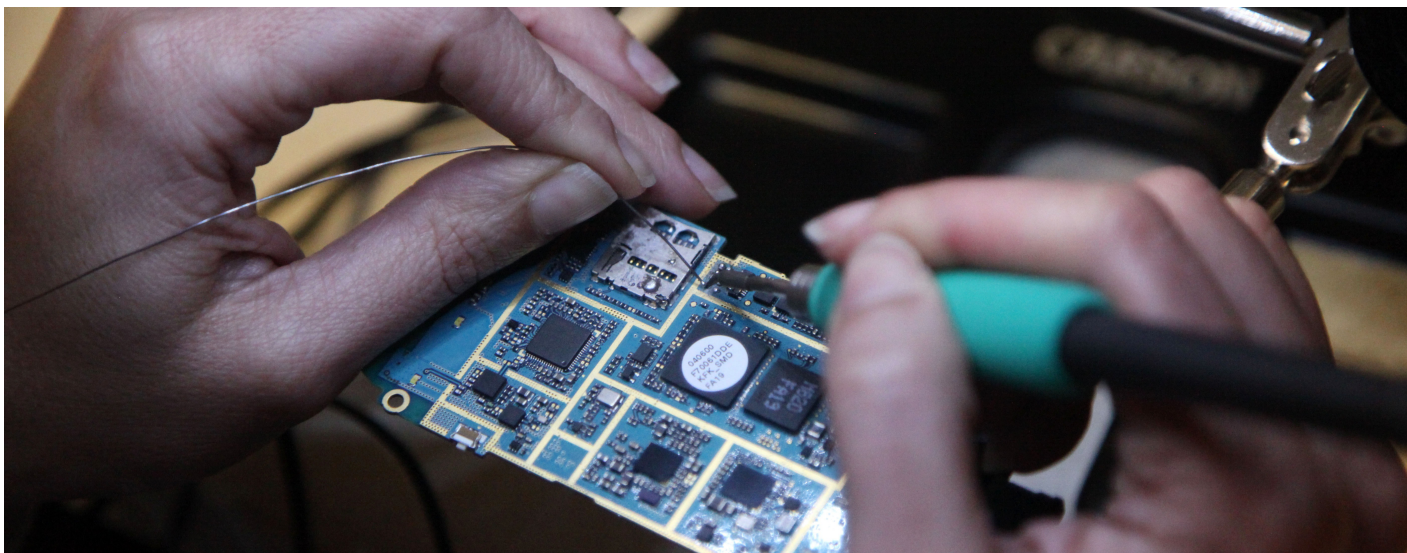
Fuente fotográfica: SalvationDATA.



9. Extracción técnica desde dispositivos dañados

En determinados casos se trabaja directamente sobre circuitos y componentes electrónicos para recuperar información de equipos que no funcionan normalmente.

Fuente fotográfica: R. Press / NIST.



10. Preservación y recuperación avanzada

Las técnicas de laboratorio permiten acceder a datos almacenados en placas y memorias, manteniendo procedimientos controlados para proteger su integridad probatoria.

Fuente fotográfica: R. Press / NIST.