Análisis Forense de Drones

DRONESVIP | Centro de Instrucción de Aeronáutica Civil

Modulo II

ANALISIS FORENSE DE DRONES

Objetivos

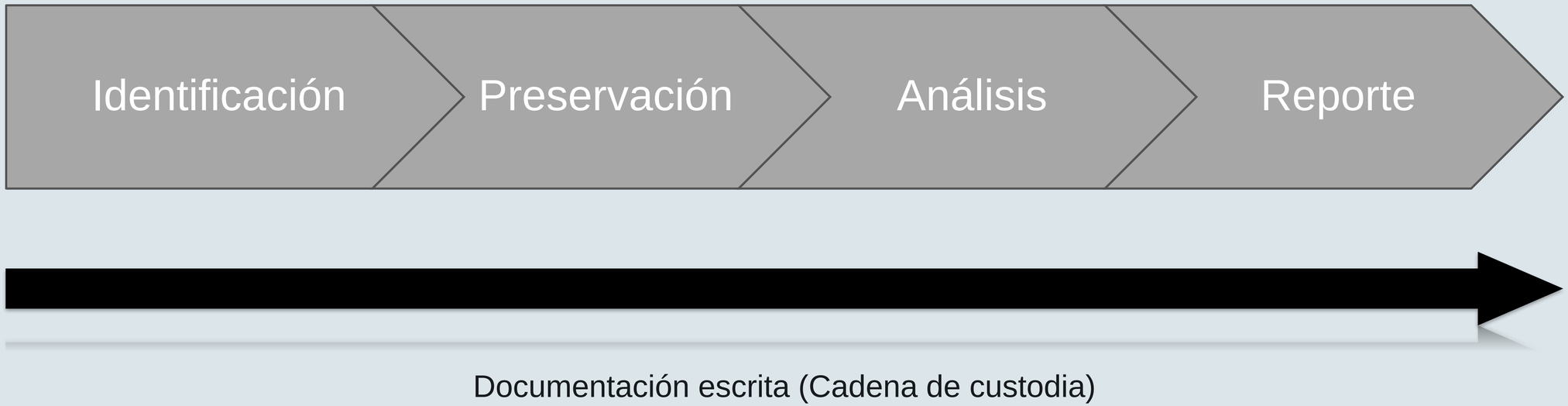
- Asimilar conceptos vinculados al análisis forense digital
- Reconocer principios que rigen esta ciencia
- Plantear interrogantes básicos
- Conocer reglas de buena práctica
- Identificar diferentes técnicas forenses
- Seguir una guía metodológica para el análisis forense

Definición de análisis forense digital

Conjunto de técnicas científicas y analíticas aplicadas sobre dispositivos electrónicos e infraestructuras tecnológicas para identificar, preservar, analizar y presentar datos que sean válidos en un procedimiento legal.

Análisis forense tradicional

ETAPAS DEL PROCEDIMIENTO FORENSE



Etapas del procedimiento forense

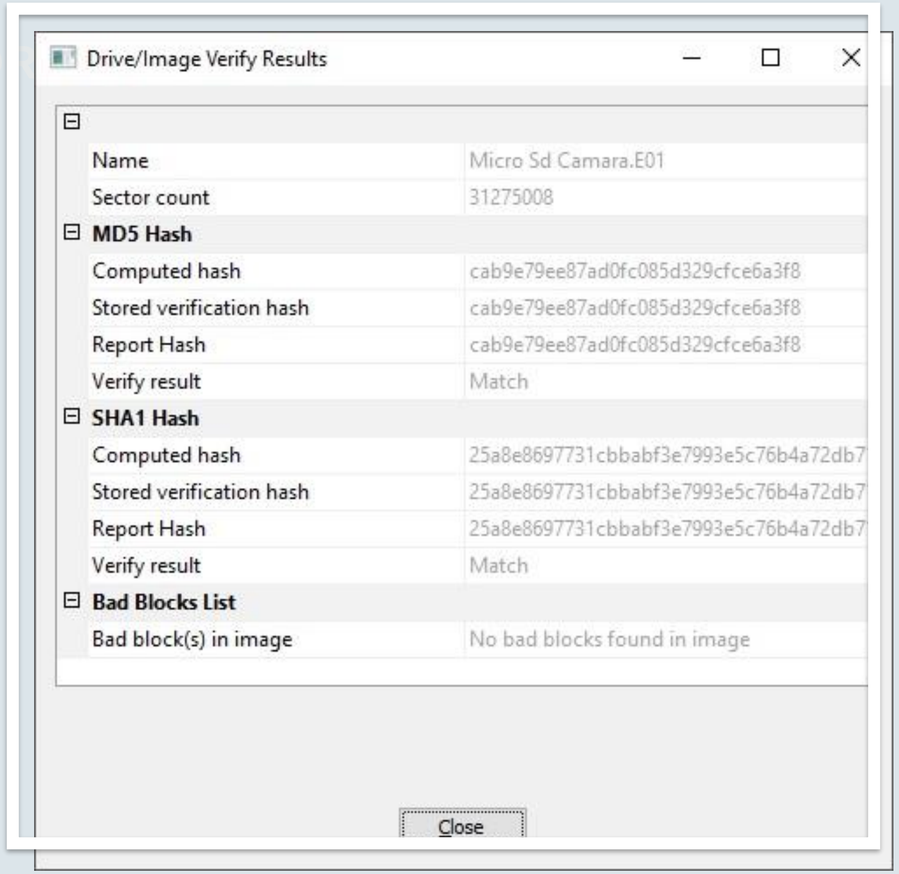
Identificación:

Primer acercamiento a los medios de prueba digitales, implica procesos tendientes a su individualización unívoca (marca, modelo, tipo de dispositivo, etc).

Etapas del procedimiento forense

Preservación:

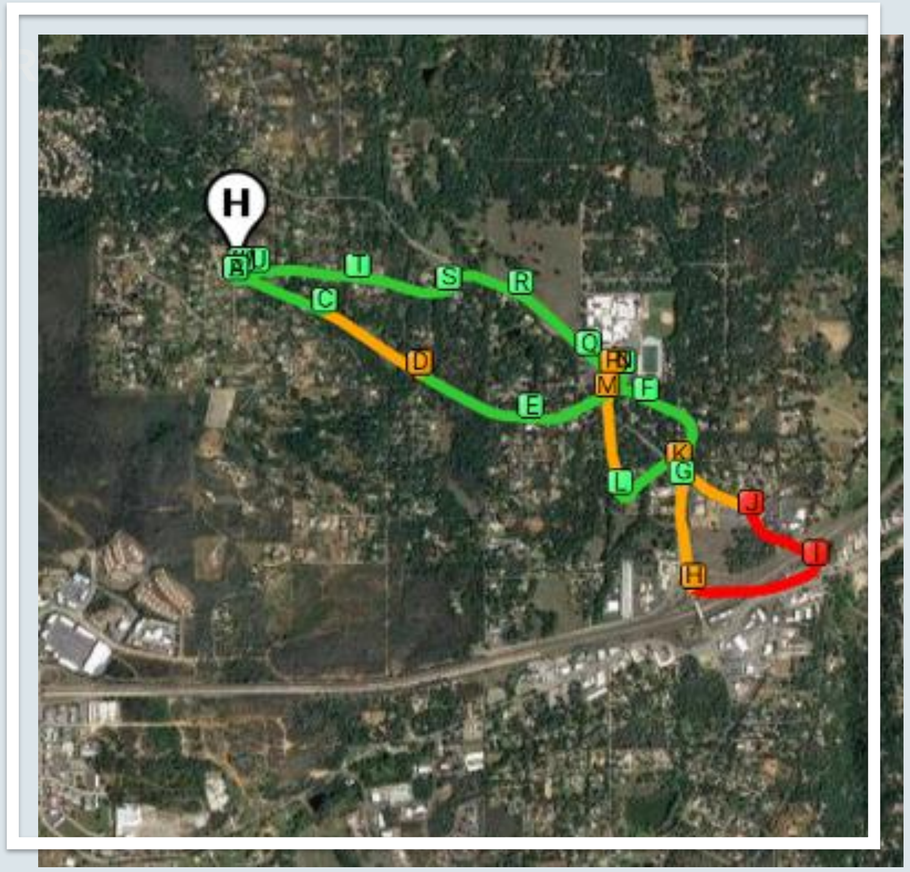
Tiene como finalidad salvaguardar la integridad y autenticidad de las evidencias digitales relevadas, garantizando la seguridad de la cadena de custodia.



Etapas del procedimiento forense

Análisis:

Conjunto de técnicas y procedimientos empleados a fin de inspeccionar y examinar los datos contenidos en los medios de prueba remitidos para estudio.



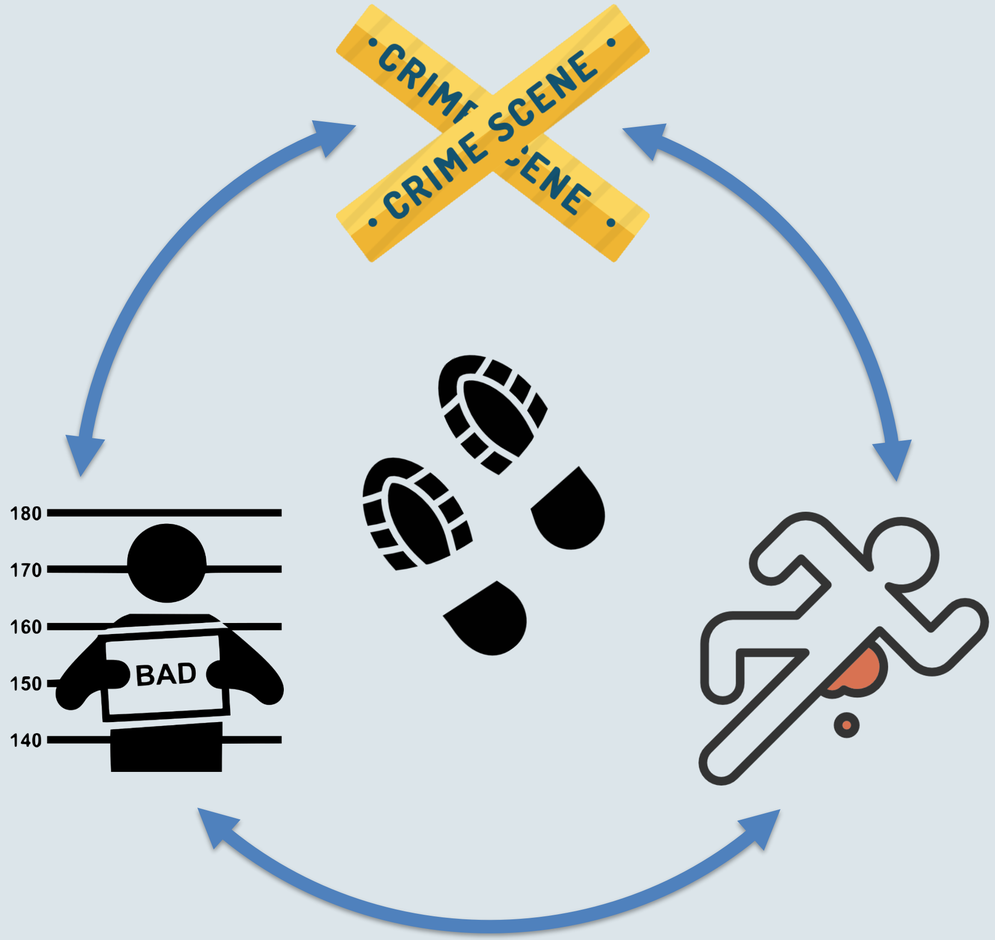
Etapas del procedimiento forense

Reporte:

Consiste en presentar la evidencia relevada y hallazgos identificados mediante un documento escrito en un formato legalmente aceptable y comprensible, incluso por quien no posea experiencia en el campo de la informática.

Principio de Intercambio

Siempre que dos objetos entran en contacto, estos transfieren parte del material que incorporan al otro objeto.



Principio del Árbol envenenado

Si la fuente de la prueba (el árbol) se corrompe, entonces cualquier elemento obtenido (fruto) también se considera corrupto y la prueba se torna no admisible.

Principio de incertidumbre

Principio de capas de ilusiones

Aspectos a tener en cuenta

EXISTE MUCHA INFORMACION

- Los sistemas son altamente complejos
- Los sistemas pueden ser altamente personalizados
- Existen diferentes componentes

IDENTIFICAR EL PROBLEMA QUE INTENTAMOS RESOLVER

- Incidente (~~Accidente~~)
- Irrupción de espacio aéreo controlado
- Invasión de privacidad
- Actividad ilegal

PREGUNTAS QUE DEBEMOS HACER

¿Qué elementos fueron recolectados?

¿Qué tipo de artefactos forenses pueden recuperarse?

¿Dónde se encuentran los datos?

PREGUNTAS QUE DEBEMOS HACER

¿Se aplican procedimientos forenses?

¿Cuáles son los niveles de extracción?

¿Qué tipo de técnicas forenses deben emplearse?

¿Existe una guía metodológica?

Elementos recolectados

MULTIPLES FUENTES DE DATOS

El SANT es el ecosistema compuesto por una gran cantidad de hardware, software y firmware diferente, antes de cualquier análisis debemos identificar cada elemento.

DIFERENTES FORMAS DE ESTABLECER CONEXION

- USB
- WiFi
- Bluetooth
- RF
- Imagen Física
- ISP/JTAG (eMMC)

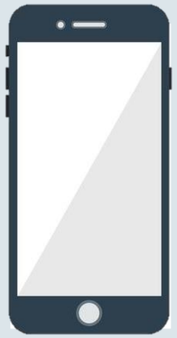
Artefactos forenses

- Información del propietario
- Número de serie que se puede usar para rastrear al propietario
- Rutas de vuelo, lugar de lanzamiento y destino de aterrizaje
- Fotos y videos que permiten a los investigadores identificar sospechosos.
- Números de versión del firmware
- Información sobre cambio de estado: lanzamiento / aterrizaje, operación manual / waypoint y GPS disponible / no disponible
- Información de ubicación geográfica para ubicaciones de lanzamiento

¿Dónde se encuentran los datos?

Dispositivo móvil (App)

- Información de identificación personal (Nube?).
- Logs de vuelo (GPS, velocidad, batería)
- Registros multimedia
- Nro de Serie del VANT



USB/WiFI

RF

Control remoto

- Puntos de lanzamiento.
- Datos de vuelo (Temporal)
- Nro de Serie del VANT

Drone

- Firmware
- Nro de Serie
- Datos del control remoto
- Logs de vuelo (GPS, velocidad, batería)
- Registros multimedia

Procedimientos forenses

RFC 3227/2002 – Internet Society

"Guía Para Recolectar y Archivar Evidencia"

- Principios de recolección de evidencia digital en función del orden de volatilidad, recaudos técnicos y legales.

- El proceso de recolección: técnicas de control y procesos.

- El proceso de archivo: la cadena de custodia y almacenamiento de los datos.

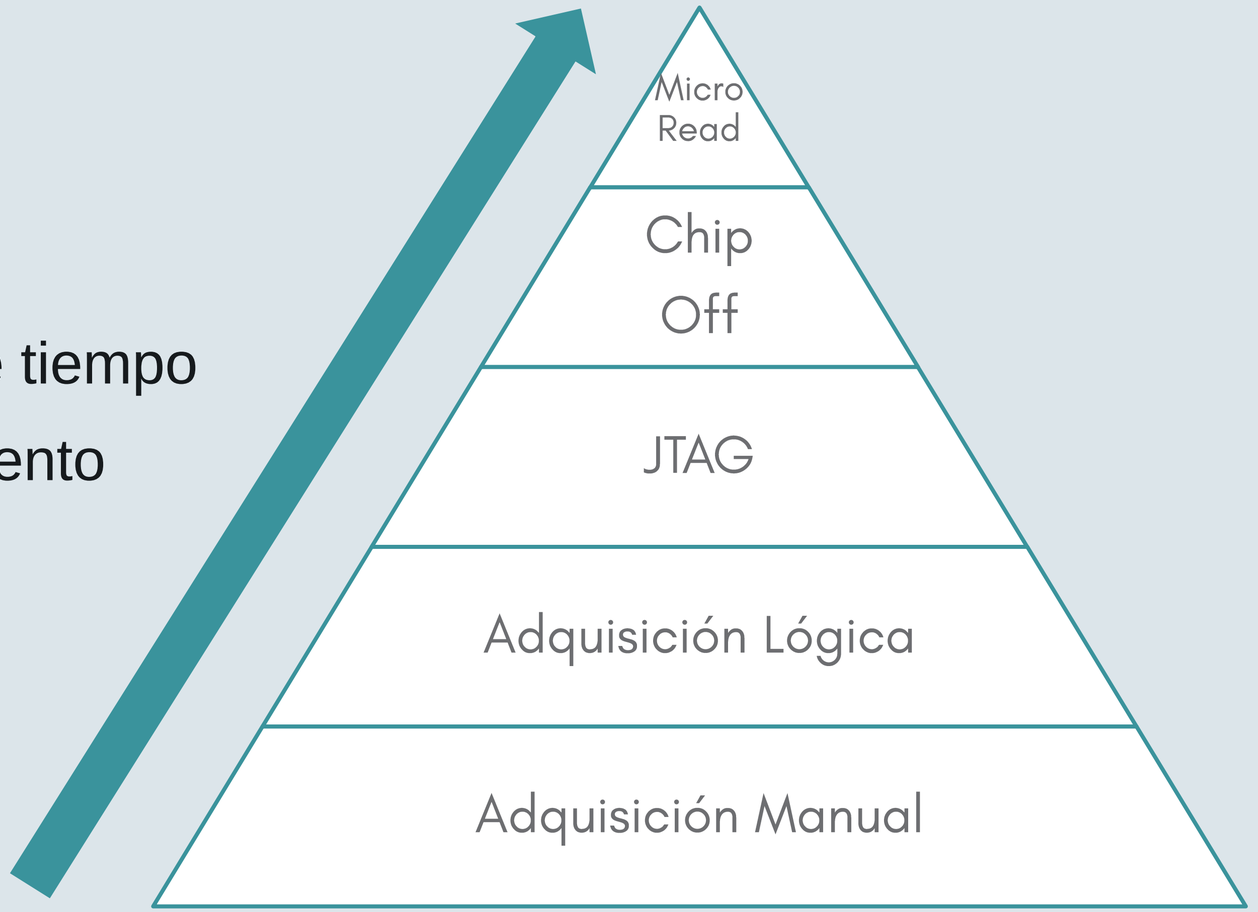
Técnicas forenses

Componente	Técnica Forense aplicada
Dispositivo móvil (App)	Análisis forense de Móviles
Control remoto	Análisis forense de Redes
Drone	Análisis forense de SO (Linux)
Tarjeta Mircro-SD	Análisis forense tradicional
Almacenamiento en la nube	Análisis forense en la nube

El análisis forense permitirá describir actividades ejecutadas, vincular al Drone con aplicaciones de control e incluso con usuarios mediante artefactos de identificación personal.

Diferentes niveles de extracción

- Mayor técnica
- Mas demanda de tiempo
- Mayor entrenamiento
- Mas invasiva



Diferentes niveles de extracción

Adquisición manual:

Implica ver el contenido de datos almacenado en un dispositivo manipulando manualmente el artefacto.

Diferentes niveles de extracción

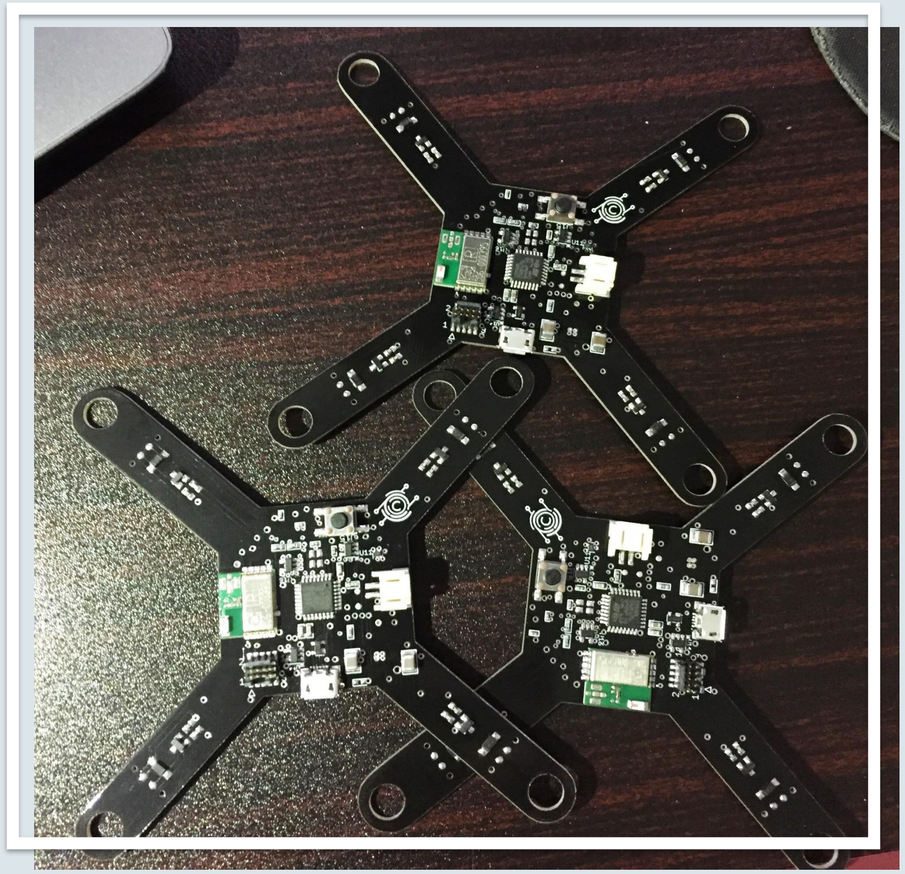
Adquisición lógica:

Consiste en establecer conectividad entre el dispositivo y la estación de trabajo forense, ya sea mediante una conexión por cable (por ejemplo, USB) o inalámbrica (como WiFi).

Diferentes niveles de extracción

JTAG:

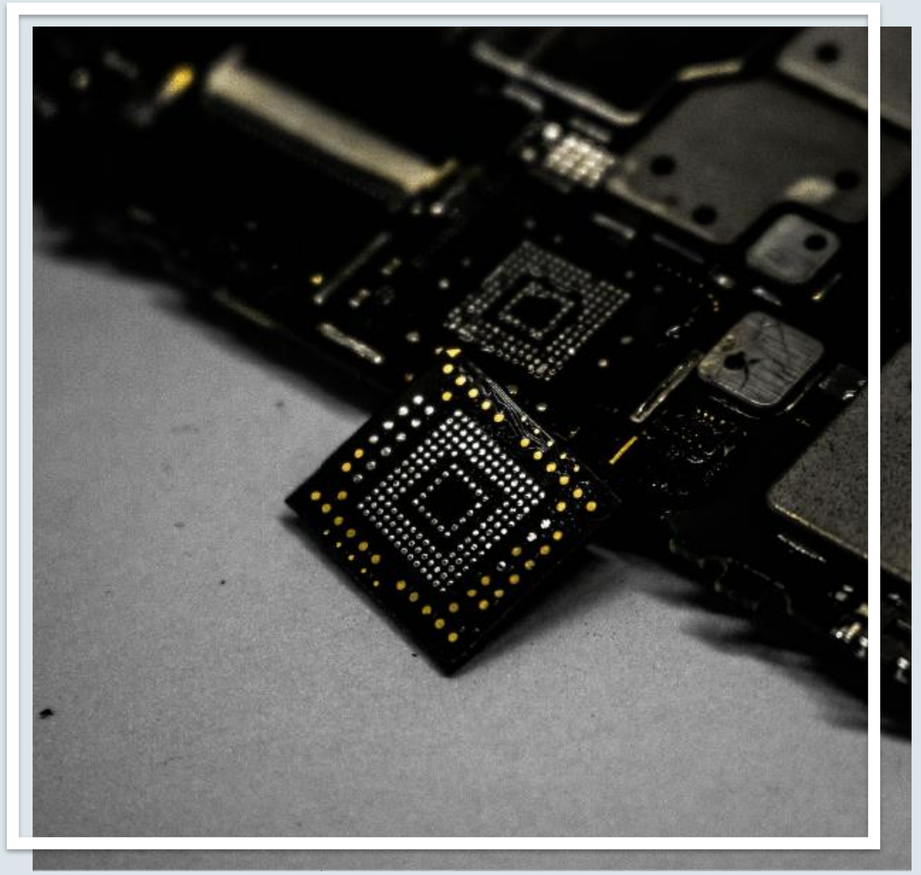
Es el acrónimo de Join Test Action Group, un estándar tecnológico desarrollado en los años 80 para verificar circuitos impresos y componentes electrónicos.



Diferentes niveles de extracción

Chip-Off:

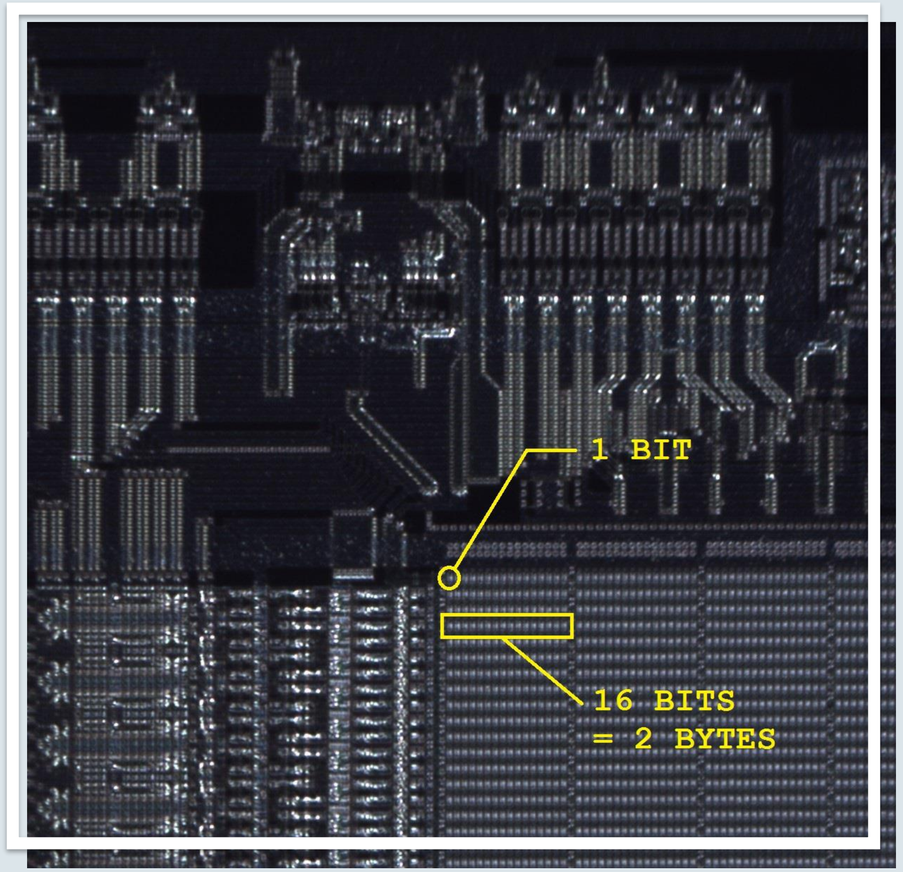
Esta técnica consiste en extraer físicamente el circuito de memoria para analizarlo mediante equipos y software especializado.



Diferentes niveles de extracción

Micro-read:

Este tipo de lectura implica registrar la observación física de las compuertas NAND o NOR de un chip con el uso de microscopios electrónicos.



Guía metodológica

PRIMERA ETAPA: IDENTIFICACIÓN

1. Verificar la recolección y resguardo del dispositivo
2. Documentación fotográfica
3. Obtener de otro tipo de evidencias
4. Consultar sobre el rol del VANT en el incidente.
5. Determinar marca, modelo y número de serie.
6. Investigar características del dispositivo.
7. Describir sus capacidades.
8. Señalar posibles modificaciones/daños.

Guía metodológica

SEGUNDA ETAPA: PRESERVACIÓN

9 → Establecer puertos de conexión.

10 → Identificar unidades de almacenamiento.

11 → Extraer medios de almacenamiento removibles.

12 → Resguardar los medios de almacenamiento.

13 → Análisis en vivo del drone (*)

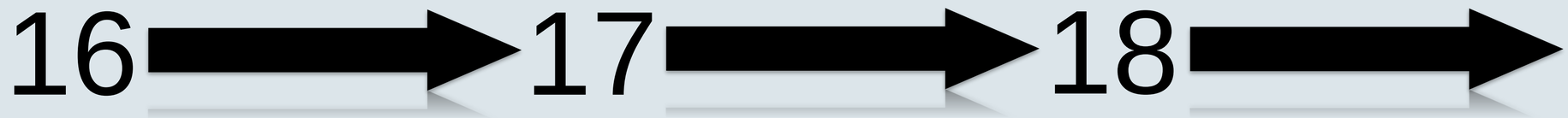
14 → Extraer medios de almacenamiento fijos (*)

15 → Resguardar registros almacenados en periféricos.

(*) Técnicas invasivas por su naturaleza

Guía metodológica

TERCERA ETAPA: ANÁLISIS



16 — Identificación y recolección de evidencias

17 — Interpretación de las evidencias recolectadas.

18 — Revisión de artefactos extraídos.

Guía metodológica

CUARTA ETAPA: PRESENTACIÓN DE RESULTADOS

19 → Interpretación y traducción de datos.

20 → Elaborar un Informe / Reporte.

Muchas gracias!

Seguinos en redes sociales

DRONESVIP | Centro de Instrucción de Aeronáutica Civil