TU ABOGADO DIGITAL

MÓDULO 5

CUESTIONARIO TÉCNICO DE INTERROGATORIO EN INFORMÁTICA FORENSE

Manual estructurado para litigio técnico penal en evidencia digital.

ÍNDICE

CUESTIONARIO INTRODUCTORIO

ATAQUE A LA IDONEIDAD DEL PERITO

¿Cuál es su título profesional exacto?

¿Está su profesión reglamentada en Venezuela?

¿Posee certificaciones internacionales en informática forense?

¿Puede indicar número y fecha de certificación?

¿Ha sido recertificado?

¿Cuántos años de experiencia práctica tiene en informática forense?

¿Cuántos casos ha llevado específicamente como perito designado judicialmente?

¿Ha sido recusado en algún proceso?

¿En cuántos casos sus conclusiones han sido desestimadas?

¿Pertenece a alguna asociación técnica forense?

¿Ha publicado investigaciones técnicas verificables?

¿Ha recibido formación en análisis en vivo?

¿Está capacitado en análisis de memoria RAM?

¿Domina herramientas como FTK, EnCase, Autopsy o Cellebrite?

¿Tiene licencia legal de esas herramientas?

¿Puede explicar la diferencia entre imagen lógica y bit a bit?

¿Conoce el estándar ISO 27037?

¿Puede explicar el principio de volatilidad?

¿Tiene formación en cadena de custodia?

¿Ha dictado cursos en la materia?

¿Cuál fue su última actualización técnica?

¿Ha intervenido en infraestructura crítica?

¿Conoce protocolos para evidencia en la nube?

¿Ha realizado análisis de IoT?

¿Tiene experiencia en análisis de espectrogramas?

¿Ha sido perito de parte o solo del Estado?

¿Recibió instrucciones de alguna parte interesada?

¿Tiene relación laboral con el órgano investigador?

¿Puede explicar qué es contaminación digital?

¿Está consciente de que un error metodológico puede invalidar la prueba?

II. FASE DE PROTECCIÓN

¿Retiró usted personalmente al usuario del equipo?

¿Cómo garantizó que no alterara datos antes de retirarlo?

¿Documentó el momento exacto de intervención?

¿Por qué decidió mantener encendido el equipo?

¿Evaluó el riesgo de pérdida de RAM?

¿Deshabilitó WiFi?

¿Deshabilitó Bluetooth?

¿Desconectó cable Ethernet?

¿Utilizó bolsa o caja Faraday?

¿Cómo evitó accesos remotos?

¿Verificó si existían programas de borrado automático?

¿Revisó tareas programadas?

¿Documentó procesos activos?

¿Realizó captura de pantalla?

¿Anotó la hora del sistema?

¿Verificó sincronización de reloj?

¿Existía cifrado activo?

¿Había sesión abierta?

¿Se registraron usuarios conectados remotamente?

¿Evaluó si había acceso por VPN?

¿Identificó dispositivos IoT en red?

¿Analizó tráfico activo?

¿Usó herramientas de monitoreo?

¿Aplicó medidas del manual técnico correspondiente?

¿Quién autorizó la intervención?

¿Existía orden judicial?

¿Protegió sistemas críticos en funcionamiento?

¿Dejó registro escrito inmediato?

¿Hubo testigos técnicos?

¿Puede garantizar que no hubo alteración posterior?

III. OBSERVACIÓN

¿Qué observó al llegar?

¿El equipo estaba encendido?

¿Qué aplicaciones estaban abiertas?

¿Había sesión iniciada?

¿Había conexión a red?

¿Anotó dirección IP?

¿Identificó MAC address?

¿Había dispositivos externos conectados?

¿Registró número de serie?

¿Fotografió el entorno?

¿Registró periféricos?

¿Había cámaras CCTV activas?

¿Identificó servidores asociados?

¿Se verificó sincronización horaria?

¿Había discos externos?

¿Se observaron routers?

¿Se identificó topología básica?

¿Había señales inalámbricas activas?

¿Se detectaron drones o GPS?

¿Se verificó presencia de nube sincronizada?

¿Había cuentas abiertas?

¿Se observaron notificaciones activas?

¿Había procesos sospechosos?

¿Se capturó memoria?

¿Se registró consumo de batería?

¿Se revisaron logs visibles?

¿Había cifrado?

¿Existía software de protección activo?

¿Se documentó todo antes de intervenir?

¿Puede demostrar esa documentación?

IV. BÚSQUEDA

¿Aplicó método sistemático?

¿Revisó puertos USB?

¿Encontró tarjetas SD?

¿Revisó discos externos?

¿Revisó nube sincronizada?

¿Exploró IoT?

¿Revisó cámaras?

¿Analizó router?

¿Buscó logs?

¿Examinó historial de navegación?

¿Identificó cuentas activas?

¿Verificó accesos remotos?

¿Inspeccionó ranuras ocultas?

¿Analizó almacenamiento oculto?

¿Detectó particiones?

¿Revisó cifrado?

¿Buscó bases de datos?

¿Analizó correos electrónicos?

¿Buscó en redes sociales?

¿Documentó alcance?

¿Limitó búsqueda al objeto?

¿Hubo testigos?

¿Se registró cada hallazgo?

¿Se utilizó herramienta específica?

¿Se validó herramienta?

¿Se guardó copia?

¿Se generó hash?

¿Se mantuvo registro cronológico?

¿Se evitó acceso innecesario?

¿Puede probar que no excedió el alcance?

V. FIJACIÓN

¿Aplicó protocolo técnico?

¿Fotografió pantalla completa?

¿Grabó video?

¿Se visualizaba fecha?

¿Se visualizaba hora?

¿Se documentaron conexiones?

¿Identificó IMEI?

¿Registró SIM?

¿Identificó eSIM?

¿Ilustró topología?

¿Se preservó resolución original?

¿Hubo compresión?

¿Se guardó formato nativo?

¿Se generó hash de fijación?

¿Se registró cadena?

¿Se evitó manipulación?

¿Se documentaron usuarios conectados?

¿Se registraron IP?

¿Se guardaron metadatos?

¿Se almacenó en medio esterilizado?

¿Se etiquetó evidencia?

¿Se firmó acta?

¿Hubo testigo?

¿Se certificó integridad?

¿Se registró herramienta usada?

¿Se guardó copia espejo?

¿Se protegió evidencia visual?

¿Se controló acceso?

¿Se resguardó en contenedor adecuado?

¿Puede garantizar autenticidad?

VI. COLECCIÓN

¿El equipo estaba apagado?

¿Lo encendió?

¿Por qué?

¿Usó herramientas antiestáticas?

¿Desconectó correctamente?

¿Etiquetó puertos?

¿Inmovilizó interruptor?

¿Documentó contraseña?

¿Recabó cargadores?

¿Extrajo batería?

¿Aisló IoT?

¿Aplicó modo avión?

¿Usó contenedor Faraday?

¿Documentó accesorios?

¿Registró serial?

¿Identificó marca?

¿Registró modelo?

¿Verificó estado físico?

¿Selló evidencia?

¿Firmó cadena?

¿Hubo testigos?

¿Registró hora?

¿Verificó apagado real?

¿Consultó especialista?

¿Usó protocolo?

¿Hubo supervisión?

¿Registró manipulación?

¿Protegió contra imanes?

¿Protegió contra humedad?

¿Puede probar continuidad?

VII. ADQUISICIÓN

¿Qué técnica utilizó?

¿Imagen bit a bit?

¿Imagen lógica?

¿Captura en vivo?

¿Por qué eligió esa técnica?

¿Evaluó volatilidad?

¿Capturó RAM?

¿Capturó swap?

¿Capturó procesos?

¿Generó hash previo?

¿Generó hash posterior?

¿Coinciden?

¿Usó medio esterilizado?

¿Documentó herramienta?

¿Registró versión?

¿Trabajó sobre copia?

¿Se evitó trabajar en original?

¿Hubo interrupción eléctrica?

¿Evaluó batería?

¿Obtuvo credenciales?

¿Hubo autorización judicial?

¿Documentó autorización?

¿Aplicó adquisición selectiva?

¿Documentó alcance?

¿Capturó nube?

¿Usó API?

¿Documentó sesión?

¿Grabó procedimiento?

¿Identificó snapshots?

¿Sincronizó nube?

¿Calculó hash en nube?

¿Registró logs?

¿Limitó alcance?

¿Puede reproducirse el procedimiento?

¿Puede otro perito validar resultado?

VIII. EMBALAJE Y ROTULADO

Cuestionario (mínimo 30 preguntas)

¿Qué tipo de contenedor utilizó para cada dispositivo (bolsa antiestática, caja rígida, evidencia húmeda, etc.)?

¿Qué criterio aplicó para decidir el tipo de embalaje según la naturaleza del dispositivo?

¿Usó protección antiestática (bolsa ESD, espuma, aislantes) para discos, RAM, tarjetas y placas?

¿Documentó el estado físico del embalaje antes de sellarlo (intacto, defectuoso, reutilizado)?

¿El embalaje era nuevo o reutilizado?

¿Qué medidas tomó para evitar descargas electrostáticas durante la manipulación?

¿Quién realizó físicamente el embalaje: usted o un tercero?

¿Se registró el nombre y cargo de quien embala?

¿Se colocaron sellos de seguridad con numeración única?

¿El sello permitía detectar apertura sin dejar evidencia?

¿Tomó fotografías del dispositivo ya embalado y sellado?

¿Rotuló el embalaje con identificación completa (marca, modelo, serial, descripción)?

¿Incluyó en el rótulo fecha y hora exacta del embalaje?

¿Incluyó el lugar de recolección y condiciones ambientales relevantes?

¿Rotuló y aisló accesorios por separado (cargadores, cables, adaptadores, dongles)?

¿Cómo evitó que un accesorio altere un dispositivo durante el traslado?

¿Qué hizo con SIM, microSD o eSIM si estaban presentes?

¿Cómo evitó la reconexión automática de redes en móviles durante traslado?

¿Aplicó aislamiento de señal (modo avión, Faraday, apagado controlado)?

Si usó bolsa Faraday, ¿cómo verificó su eficacia (por ejemplo, ausencia de señal)?

Si no usó Faraday, ¿por qué consideró que no era necesario?

¿Se registró el estado de batería (nivel de carga) y si estaba conectada?

¿Se transportó el dispositivo encendido? Si sí, ¿cómo garantizó estabilidad y registro?

¿Se evitó presión sobre teclas, botones o pantallas durante embalaje?

¿Usó material de relleno interno para evitar golpes?

¿Se consideró protección contra humedad, calor o campos magnéticos?

¿El embalaje fue etiquetado con advertencias (frágil, ESD, mantener aislado)?

¿Qué controles implementó para impedir sustitución de evidencia por empaques similares?

¿Se registró el número de bultos y su correspondencia con el inventario?

¿Se creó un inventario formal correlacionado al rotulado?

¿Qué procedimiento aplicó para medios digitales donde se almacenó evidencia adquirida (discos externos, DVD, USB)?

¿Rotuló también los contenedores lógicos (carpetas digitales) siguiendo criterios de identificación?

¿Cómo protegió la evidencia adquirida contra escritura o modificación accidental?

¿Se documentó el mecanismo de cierre del embalaje (cinta, sello, grapa, etc.)?

¿Puede demostrar con evidencia documental que el embalaje no fue abierto antes de laboratorio?

IX. REGISTRO DE CADENA DE CUSTODIA

¿Quién inició la cadena de custodia y a qué hora exacta?

¿Cuál fue el primer registro documental generado?

¿El formato de cadena incluye identificación del dispositivo (marca, modelo, serial)?

¿Incluye identificación de componentes anexos (cables, adaptadores, SIM, SD)?

¿Incluye la descripción técnica suficiente para evitar confusión con otro equipo similar?

¿Incluye el estado físico del dispositivo (daños, golpes, humedad, pantalla rota)?

¿Incluye el estado lógico observable (encendido, apagado, bloqueado, sesión abierta)?

¿Se registró si estaba conectado a red y de qué tipo?

¿Se registró el lugar exacto de hallazgo y el lugar de embalaje?

¿Se registró fecha y hora con precisión (no “aproximada”)?

¿Se registró el método de obtención (colección, adquisición in situ, adquisición selectiva)?

¿Se registraron los nombres completos y cargos de cada custodio?

¿Cada transferencia incluye motivo y condiciones?

¿Cada transferencia incluye firma (o constancia) de entrega y recepción?

¿Cada transferencia incluye fecha/hora exacta?

¿Hubo lapsos sin custodio identificado?

¿Hubo almacenamientos temporales? ¿Dónde, cuánto tiempo, bajo qué control?

¿Quién tuvo acceso físico al área de resguardo?

¿Existió registro de control de acceso (bitácora, cámaras, libro de ingreso)?

¿Cómo se asegura que el mismo elemento entregado es el recibido (identificadores + sellos)?

¿Se registró el número de sello al inicio y se verificó en cada transferencia?

¿Se documentó cualquier anomalía del sello (levantado, rasgado, reemplazado)?

¿Se registraron condiciones de transporte (temperatura, golpes, vibración, humedad)?

¿Se registró la ubicación del dispositivo dentro del transporte (maletín, caja, bulto)?

¿Se registró si el dispositivo cambió de estado (encendido/apagado) durante custodia?

¿Se registró si se aplicaron inhibidores o modo avión?

¿Se documentó si hubo intervención antes de laboratorio?

¿Se adjuntó inventario de evidencia digital adquirida (archivos, hashes, tamaños)?

¿Se documentó el hash cuando correspondía (imagen forense, volcado, contenedor)?

¿Se preservaron registros originales y copias certificadas?

¿Se documentó quién realizó el cálculo hash y con qué herramienta?

¿Se documentó la versión de la herramienta y el método?

¿Puede mostrar continuidad completa sin “huecos” entre recolección y análisis?

¿Puede demostrar que nadie no autorizado tuvo oportunidad real de acceder o sustituir?

¿Se correlaciona su dictamen con la cadena (mismos identificadores, mismos sellos)?

X. PERITAJE INFORMÁTICO (LABORATORIO)

A) Preservación y metodología

¿Usted trabajó sobre el original o sobre una copia forense?

Si trabajó sobre copia, ¿cómo garantizó que esa copia es íntegra?

¿Se verificó hash antes de iniciar cualquier análisis?

¿Se verificó hash al finalizar el análisis?

¿Qué algoritmo hash usó y por qué?

¿Qué herramienta utilizó para hash y cuál era su versión exacta?

¿El ambiente de laboratorio estaba controlado (acceso, bitácora, cámaras)?

¿El equipo de análisis estaba aislado de internet?

¿Cómo evitó contaminación cruzada entre casos (medios esterilizados, políticas de borrado)?

¿Qué procedimiento aplicó para documentar cada acción (bitácora técnica)?

B) Tiempo, reloj y consistencia

¿Determinó la hora del sistema del dispositivo y la comparó con hora real?

¿Identificó zona horaria, DST y desfases?

¿Cómo trató inconsistencias entre hora de sistema, hora de red y metadatos?

¿Construyó línea de tiempo? ¿Con qué fuentes (MAC times, logs, eventos)?

¿Incluyó en su dictamen cómo corrigió desfases temporales?

C) Búsqueda, alcance y reproducibilidad

¿Qué criterios exactos de búsqueda utilizó (palabras, rutas, extensiones, hashsets)?

¿Estaban esos criterios alineados al objeto solicitado o investigado?

¿Cómo evita usted “pesca exploratoria” fuera del alcance?

¿Qué filtros aplicó para evitar falsos positivos?

¿Qué método empleó para asegurar que otro perito pueda reproducir su búsqueda?

D) Evidencia encontrada y clasificación

¿Identificó la ruta exacta de ubicación de cada archivo relevante?

¿Clasificó evidencia por tipo: texto, imagen, audio, video?

¿Cuantificó volúmenes por tipo y por relevancia?

¿Creó carpeta contenedora con estructura verificable?

¿Aplicó compresión? Si sí, ¿cómo preservó integridad y trazabilidad?

¿Codificó/Encriptó la carpeta? ¿Con qué método y cómo quedó documentado?

¿Generó tabla índice con: nombre nativo, fechas, tamaño, hash, ruta?

¿Incluyó sector o ubicación lógica cuando correspondía?

E) Eliminados y recuperación

¿Realizó búsqueda de archivos eliminados?

¿Qué técnica utilizó: carving, MFT/USN, journal, snapshots?

¿Cómo distinguió entre “archivo recuperado completo” y “parcial”?

¿Cómo documentó fragmentación o corrupción de archivos recuperados?

¿Cómo evitó afirmar contenido sin certeza técnica?

F) Comparativos y autenticidad

¿Determinó correspondencia entre archivos y la evidencia adquirida mediante comparación?

¿Comparó hash, metadatos y contenido?

¿Cómo evaluó la posibilidad de manipulación de metadatos?

¿Qué controles aplicó contra anti-forensics (timestamp spoofing, wiping, stego)?

¿Identificó indicios de esteganografía o contenedores ocultos?

¿Qué hallazgos excluyó y por qué (criterio de pertinencia y confiabilidad)?

¿Puede afirmar que sus conclusiones son reproducibles por un tercero independiente?

XI. PERITAJE FÍSICO COMPARATIVO (IMÁGENES/AUDIOS/VIDEOS/VOZ)

A) Parámetros objetivos

¿Recibió parámetros objetivos de tiempo (rango exacto) para el material?

¿Qué ocurre si no existe rango temporal objetivo? ¿Cómo limita su análisis?

¿El material fue entregado en formato nativo?

Si no era nativo, ¿cómo determinó que no hubo transcodificación previa?

B) Determinación de edición (video e imagen)

¿Aplicó análisis cuadro a cuadro?

¿Revisó continuidad de frames, GOP, saltos y duplicaciones?

¿Analizó inconsistencias de iluminación, sombras y equilibrio de blancos?

¿Analizó compresión y artefactos por recodificación?

¿Detectó cortes abruptos o pérdida de continuidad temporal?

¿Verificó coherencia de audio con video (sincronía labial/ambiental)?

¿Revisó metadatos del contenedor (MP4/MOV/AVI) y su consistencia?

¿Buscó indicios de edición por software (tags, encoder signatures)?

C) Análisis de contenido

¿Su análisis de contenido describe hechos observables o conclusiones interpretativas?

¿Cómo separa “descripción” de “inferencia”?

¿Identificó elementos verificables: ubicación, objetos, secuencia, interacción?

¿Documentó la metodología usada para interpretar el contenido sin sesgo?

¿El material tiene cortes que impidan inferir continuidad del evento?

D) Voz: identificación e individualización

¿Se realizó análisis acústico antes de comparar?

¿Se verificó que existan fonemas aptos para comparación?

¿Cuál fue la tasa de muestreo del audio?

¿Hay ruido de fondo que afecte espectrograma?

¿Qué software usó para espectrogramas y su versión?

¿Qué parámetros usó: ventana, solapamiento, FFT?

¿Cuántas muestras comparó y bajo qué criterio?

¿Tuvo muestra control obtenida de forma adecuada?

¿La persona repitió palabras/frases de la muestra problema al menos tres veces?

¿Cómo evitó sesgo por entrenamiento o sugestión?

¿Su conclusión es categórica o probabilística?

¿Cuál es el margen de error y el soporte empírico?

E) Autenticidad y procedencia

¿Puede demostrar procedencia del archivo (origen, dispositivo, ruta)?

¿El archivo fue extraído con método forense o fue enviado por mensajería?

Si fue enviado por mensajería, ¿cómo controló pérdida de metadatos?

¿Se verificó hash del archivo recibido?

¿Se mantuvo trazabilidad del archivo desde su obtención hasta análisis?

F) Consistencia y límites

¿Qué limitaciones técnicas reconoce en su dictamen?

¿Qué hipótesis alternativas consideró (edición, recorte, deepfake, recodificación)?

¿Revisó indicios de inteligencia artificial (rostro, voz sintética, patrones de parpadeo)?

¿Qué criterios objetivos utilizó para excluir deepfake?

¿Puede un tercero replicar su análisis con el mismo resultado?

¿Qué datos serían necesarios para aumentar certeza si el material es incompleto?