**DKIM, SPF/ARC**

**Prueba de No Manipulación de Cabeceras Básicas**

Probar la "no manipulación" de cabeceras básicas (To, From, Subject, etc.) es un concepto más sutil y se centra en la **Integridad Criptográfica** del correo.

Es **imposible** que un módulo de ingesta de Autopsy (sin claves privadas) *pruebe* la no manipulación del cuerpo del correo o de las cabeceras básicas (que no están protegidas por Received:), ya que cualquier atacante puede cambiar la cabecera Subject: y recalcular el *hash* del archivo.

Sin embargo, tu módulo puede detectar la **ruptura de la integridad criptográfica** que prueba la manipulación del *contenido*, lo que automáticamente prueba que las cabeceras básicas NO pueden ser de confianza.

**El Enfoque Criptográfico (DKIM y ARC)**

El único mecanismo que prueba la integridad de las cabeceras básicas y el cuerpo del mensaje es **DKIM** (DomainKeys Identified Mail) y **ARC** (Authenticated Received Chain).

Tu módulo **no necesita validar las firmas (DKIM/ARC)** (eso requeriría resolver DNS para obtener claves públicas), solo necesita **detectar cuándo fallan**.

**Mecanismo para probar la no manipulación:**

**Detección de Fallo DKIM:**

**Original:** El extracto muestra dkim=pass en la cabecera Authentication-Results.

**Manipulación:** Cambia ligeramente el Subject: (e.g., de "Prueba para TFM" a "Prueba FINAL para TFM").

**Resultado Esperado:** Cuando el correo llega a un servidor validador (como Gmail), este recalcula la firma DKIM. Como el Subject: ha cambiado, la firma **fallará**. El servidor receptor (Gmail/Outlook) marcará en la cabecera **Authentication-Results** que dkim=fail.

**Detección de Fallo ARC:**

ARC es una cadena de sellos (ARC-Seal) que protege las cabeceras modificables (como Received:) a través de diferentes servidores. Si una cabecera Received: es alterada por un intermediario malicioso, ARC lo detectará.

La mejor prueba de manipulación es el **link\_break** que ya creamos en la sección 1.A, ya que una alteración tan flagrante debería hacer que el sello ARC se invalidara.

**Conclusión para tu Módulo**

Para tu TFM, el mejor modo de "probar la no manipulación" (o, más bien, **demostrar la integridad**) de las cabeceras es:

**Módulo de Headers/Coherencia:** Confirma que **no hay reverse\_order o link\_breaks** en los Received:.

**Módulo de Basic Headers:** Añade al reporte un *checkbox* que indique el **estado de DKIM** y **ARC** (pass, fail, o none) de la cabecera Authentication-Results más reciente.

Si el correo pasa estas dos pruebas (coherencia temporal y DKIM/ARC *pass*), se considera **auténtico** con alta probabilidad.

[ <https://www.proofpoint.com/es/threat-reference/spf> ]

Un SPF o sender policy framework es un protocolo de validación de correo electrónico y una estrategia de **[ciberseguridad](https://www.proofpoint.com/es/threat-reference/cybersecurity-network-security" \o "¿Qué es la seguridad de redes?)** que se usa para detener ataques de **[phishing](https://www.proofpoint.com/es/threat-reference/phishing" \o "Phishing)**. Le permite a su empresa especificar quién puede enviar correo electrónico en nombre de su dominio.

[ <https://www.cloudflare.com/es-es/learning/email-security/dmarc-dkim-spf/> ]

[<https://scholar.googleusercontent.com/scholar?q=cache:c3U3xhWwIR4J:scholar.google.com/+dkim+spf+arc+y+dmarc&hl=es&as_sdt=2007> ]

[ <https://www.mdirector.com/blog/comprobar-registro-dkim/> ]

[<https://github.com/kmille/dkim-verify> ]