El módulo **TFM Email Date Coherence** sirve para detectar **manipulaciones temporales** en correos electrónicos mediante el análisis forense de sus cabeceras y metadatos. Se centra en verificar la **integridad cronológica** del mensaje desde que se envía hasta que se almacena en el sistema.

Su función principal es analizar la coherencia entre tres puntos clave: la fecha declarada en la cabecera Date:, la fecha del último servidor de tránsito registrada en la cadena Received:, y los metadatos de tiempo del archivo .eml (creación/modificación).

El código extrae primero el *epoch* de la cabecera Date: y localiza el *epoch* del último *hop* válido en la cadena Received:. Luego, realiza comprobaciones clave:

1. **Date: Posterior a Received:** Alerta si la fecha declarada (Date:) es significativamente posterior al último servidor que procesó el correo. Esto sugiere que la cabecera Date: fue alterada para falsificar la hora de envío.
2. **Archivo EML Posterior a Received:** Advierte si la fecha de modificación del archivo es muy posterior al último Received:, indicando una posible manipulación posterior al tránsito.
3. **Date: Ausente/Inválida:** Penaliza la falta o el formato incorrecto de la cabecera Date:.

El módulo asigna una **puntuación de severidad** a los hallazgos y genera un informe detallado en Autopsy. Este análisis ayuda al forense a **identificar correos electrónicos sospechosos de alteración** o que pasaron por servidores mal configurados, siendo crucial en procesos de **adveración**.

**Detección de Inconsistencias**

El corazón del módulo reside en la función analyze\_date\_coherence, que compara estos tres valores en busca de desfases sospechosos:

1. **Date: posterior al Último Received (Alerta):** Detecta si la fecha declarada del correo es **posterior** a la fecha en que el último servidor de tránsito la registró. Una diferencia de más de 5 minutos (300 segundos) se marca como una anomalía grave.
2. **Metadato Archivo posterior al Último Received (Alerta):** Señala si la fecha de modificación/creación del archivo .eml en el disco es significativamente **posterior** a la fecha en que el servidor terminó de procesar el correo (más de 7 días), lo que sugiere una **manipulación del archivo EML** después de su entrega.
3. **Date: posterior al Metadato Archivo (Info):** Identifica cuando la fecha declarada es significativamente **posterior** a la fecha del archivo .eml (más de 7 días). Esto puede indicar que la cabecera Date: fue alterada y el archivo original fue copiado, o que el archivo EML ha estado guardado por un largo tiempo.

El módulo **Email Date Coherence** verifica la **consistencia temporal** de correos electrónicos comparando la cabecera **Date:** declarada por el cliente emisor con la **línea temporal real** inferida de la cadena **Received:** y, como referencia secundaria, con los **metadatos del archivo .eml** en el contenedor forense.  
Primero extrae Date y la convierte a **epoch UTC**; después parsea todas las cabeceras Received y determina el **instante más reciente** en el que un MTA procesó el mensaje (último hop efectivo).  
Si la Date aparece **posterior** al último Received por encima de un **umbral corto** (p. ej. 5 min), se marca **alerta**: es incoherente que el mensaje “se haya recibido” antes de “haber sido fechado”.  
El módulo también compara la Date con los **tiempos del archivo .eml** (creación/modificación). Diferencias **grandes** (p. ej. >7 días) se anotan como indicios de **reexportación**, **copia tardía** o posible **manipulación** del contenedor, con **penalización suave** porque son efectos habituales en la cadena de custodia.  
Todos los hallazgos se resumen en un **Analysis Result** con **desglose legible** (offsets, hops implicados) y una **puntuación** que cuantifica la severidad, facilitando priorización y reportabilidad.  
En el contexto del TFM, este módulo **apoya la adveración** al aportar una **prueba técnica trazable** de que la **cronología** interna del correo es **verosímil** o presenta **inconsistencias**; además, se integra con el resto de validaciones (cabeceras inconsistentes, hashes, etc.) para construir un **criterio pericial** robusto y reproducible.