Email Forensic

Що таке Email Forensic?

Email forensic (криміналістичний аналіз електронної пошти) — це процес збору, збереження, аналізу та презентації доказів, отриманих з електронних листів, з метою розслідування злочинів, внутрішніх корпоративних порушень або інших інцидентів інформаційної безпеки.

Основні завдання email forensic:

- Встановлення автентичності листа
- Визначення справжнього відправника
- Виявлення підроблених або змінених листів
- Відстеження маршруту доставки листа
- Збір доказів для судових справ
- Виявлення фішингу та соціальної інженерії

Структура електронного листа

Електронний лист складається з двох основних частин:

1. Заголовок (Header)

Містить технічну інформацію про лист, яка зазвичай прихована від користувача:

- **From:** адреса відправника (може бути підроблена)
- **To:** адреса отримувача
- **Subject:** тема листа
- **Date:** дата і час створення листа
- **Message-ID:** унікальний ідентифікатор листа
- **Received:** ланцюжок серверів, через які пройшов лист
- **Return-Path:** адреса для повернення листа у разі помилки
- **Authentication-Results:** результати перевірки SPF, DKIM, DMARC

- **X-Originating-IP:** IP-адреса відправника

2. Тіло листа (Body)

Містить основний вміст повідомлення у текстовому або HTML форматі.

Ключові заголовки для аналізу

Received Headers

Найважливіші заголовки для трасування маршруту листа. Кожен поштовий сервер додає свій запис **Received**. Читати їх потрібно **знизу вгору** (від найстарішого до найновішого).

Приклад:

```
Received: from mail.example.com (192.168.1.1)
    by mx.google.com with ESMTP id abc123
    for <user@gmail.com>; Mon, 25 Nov 2025 10:30:00 +0000
```

Authentication Headers

- **SPF (Sender Policy Framework):** перевіряє, чи дозволено серверу відправляти пошту від імені домену
- **DKIM (DomainKeys Identified Mail):** криптографічний підпис, що підтверджує автентичність
- **DMARC (Domain-based Message Authentication):** політика обробки листів, що не пройшли SPF або DKIM

X-Headers

Додаткові заголовки, що можуть містити корисну інформацію:

- X-Mailer: поштовий клієнт відправника
- X-Originating-IP: IP-адреса джерела
- X-Spam-Score: оцінка ймовірності спаму

Типові сценарії використання

1. Виявлення фішингу

Аналіз заголовків допомагає виявити:

- Невідповідність між відображуваною адресою та справжнім відправником
- Підозрілі IP-адреси або географічні локації
- Відсутність або провал SPF/DKIM перевірок

2. Розслідування інцидентів

- Встановлення точного часу відправки та доставки
- Визначення ланцюжка пересилання
- Збір доказів для судових справ

3. Аудит безпеки

- Перевірка налаштувань поштових серверів
- Виявлення вразливостей у конфігурації
- Моніторинг спроб злому

Завдання: Аналіз заголовків електронних листів у Thunderbird

Мета роботи

Навчитися встановлювати поштовий клієнт Thunderbird, переглядати та аналізувати повні заголовки електронних листів для криміналістичного дослідження.

Необхідне програмне забезпечення

- **Mozilla Thunderbird** (безкоштовний поштовий клієнт)
- Доступ до електронної пошти (Gmail, Outlook, або інший провайдер)

Частина 1: Встановлення Thunderbird

Крок 1: Завантаження

1. Перейдіть на офіційний сайт: https://www.thunderbird.net
2. Натисніть кнопку **"Download Thunderbird"**

3. Виберіть версію для вашої операційної системи (Windows, macOS, Linux)
4. Збережіть інсталяційний файл

Крок 2: Інсталяція

Для Windows:

1. Запустіть завантажений файл `.exe`
2. Виберіть тип інсталяції (рекомендується стандартна)
3. Слідуйте інструкціям майстра встановлення
4. Дочекайтеся завершення інсталяції

Для macOS:

1. Відкрийте завантажений файл `.dmg`
2. Перетягніть іконку Thunderbird у папку Applications
3. Запустіть програму з папки Applications

Для Linux:

```
sudo apt update
sudo apt install thunderbird
```

Крок 3: Налаштування облікового запису

1. Запустіть Thunderbird
2. У вікні привітання натисніть **"Set up an existing email account"**
3. Введіть ваші дані:
   - Ім'я (як воно відображатиметься отримувачам)
   - Email адреса
   - Пароль
4. Натисніть **"Continue"** та дочекайтеся автоматичного налаштування
5. Підтвердіть налаштування сервера (IMAP/POP3, SMTP)
6. Натисніть **"Done"**

Частина 2: Відправка тестового листа

Завдання: Створіть тестовий лист

1. У Thunderbird натисніть кнопку **"Write"** (Написати) або використайте Ctrl+N
2. У полі **"To:"** введіть **вашу власну email адресу**
3. У полі **"Subject:"** напишіть: **HELLO, WORLD**
4. У тілі листа напишіть будь-який текст, наприклад:

   > Це тестовий лист для аналізу заголовків.
   > Практична робота з Email Forensic.

5. Натисніть **"Send"** (Відправити)
6. Зачекайте кілька секунд, поки лист не з'явиться у вашій скриньці
7. Оновіть список листів (F5 або кнопка оновлення)

> **Примітка:** Цей лист ви будете використовувати для аналізу заголовків разом з іншими листами зі своєї скриньки.

Частина 3: Перегляд заголовків листа у Thunderbird

Метод 1: Через меню

1. Відкрийте будь-який лист у Thunderbird (наприклад, ваш тестовий "HELLO, WORLD")
2. Натисніть на кнопку **"More"** (три крапки) у правому верхньому куті
3. Виберіть **"View Source"** (Ctrl+U)
4. Відкриється нове вікно з повним текстом листа, включаючи всі заголовки

Метод 2: Через контекстне меню

1. Клацніть правою кнопкою миші на листі у списку
2. Виберіть **"View Source"** або **"Message Source"**

Метод 3: Через головне меню

1. Виберіть лист
2. У головному меню: **View → Message Source** (або Ctrl+U)

Копіювання заголовків для аналізу

1. Після відкриття вихідного коду листа (View Source)
2. Виділіть весь текст (Ctrl+A)
3. Скопіюйте його (Ctrl+C)
4. Збережіть у текстовий файл або використайте для онлайн-аналізу

Частина 4: Аналіз заголовків у Google Admin Toolbox

Що це таке?

Google Admin Toolbox Messageheader — це безкоштовний онлайн-інструмент від Google для візуального аналізу заголовків електронних листів. Він автоматично розбирає заголовки та показує маршрут листа, результати автентифікації та інші важливі параметри.

Як використовувати:

1. Перейдіть на сайт: Google Admin Toolbox - Messageheader
2. **Отримайте заголовки листа в Thunderbird:**
   - Відкрийте ваш тестовий лист "HELLO, WORLD" або будь-який інший лист
   - Натисніть Ctrl+U (View Source)
   - Скопіюйте весь текст (Ctrl+A, потім Ctrl+C)
3. **Вставте заголовки на сайт:**
   - У велике текстове поле вставте скопійовані заголовки (Ctrl+V)
   - Натисніть кнопку **"Analyze"** (Аналізувати)
4. **Вивчіть результати:**

   Інструмент покаже:

- **Message delivery path** (Шлях доставки повідомлення) — візуальну схему з IP-адресами та серверами
- **Delay information** (Інформація про затримки) — час проходження між серверами
- **Authentication results** (Результати автентифікації) — статус SPF, DKIM, DMARC
- **Original message** (Оригінальний лист) — форматований вигляд заголовків

Переваги Google Admin Toolbox:

- Автоматичне розпізнавання та розбір заголовків
- Візуальне представлення маршруту листа
- Виділення проблемних місць червоним кольором
- Розрахунок часу доставки
- Визначення геолокації серверів
- Виявлення проблем з автентифікацією

Порівняння методів аналізу

Метод	Переваги	Недоліки
Thunderbird (View Source)	Повний контроль, офлайн робота, бачите необроблені дані	Потрібно вручну інтерпретувати
Google Admin Toolbox	Візуальний аналіз, автоматична інтерпретація, зручність	Потрібен інтернет, дані надсилаються на сервер Google

> **Рекомендація:** Використовуйте обидва методи — Thunderbird для детального вивчення сирих заголовків та Google Toolbox для швидкого візуального аналізу

Частина 5: Детальний аналіз заголовків

Завдання 1: Базовий аналіз

Проаналізуйте ваш тестовий лист "HELLO, WORLD" та ще один будь-який лист зі скриньки.

Для кожного листа знайдіть та запишіть:

1. **Відправник:**
   - Поле `From:`
   - Поле `Return-Path:`
   - Чи збігаються ці значення?
2. **Отримувач:**
   - Поле `To:`
   - Поле `Delivered-To:`
3. **Тема та дата:**
   - Поле `Subject:`
   - Поле `Date:`
4. **Унікальний ідентифікатор:**
   - Поле `Message-ID:`

Завдання 2: Трасування маршруту

Виконайте для обох листів (вашого тестового та будь-якого іншого):

1. Знайдіть усі заголовки `Received:` (їх може бути декілька)
2. Запишіть їх у зворотному порядку (знизу вгору)
3. Для кожного запису визначте:
   - Назву сервера
   - IP-адресу сервера
   - Час проходження
4. Створіть схему маршруту листа від відправника до отримувача
5. **Порівняйте:** Скопіюйте заголовки обох листів у Google Admin Toolbox та порівняйте візуальні схеми маршрутів

Приклад аналізу:

```
Received: from mail.sender.com (192.168.1.10)
   [Перший сервер - початок шляху]
   ↓
Received: from relay.isp.com (203.0.113.25)
   [Проміжний сервер провайдера]
   ↓
Received: from mx.gmail.com (172.217.1.1)
   [Кінцевий сервер - доставка]
```

Завдання 3: Перевірка автентифікації

Знайдіть та проаналізуйте для обох листів:

1. **SPF запис:**
   - Поле `Received-SPF:`
   - Чи пройдено перевірку? (Pass/Fail/Neutral)
2. **DKIM підпис:**
   - Поле `DKIM-Signature:`
   - Поле `Authentication-Results:` (шукайте dkim=pass або dkim=fail)
3. **DMARC політика:**
   - Поле `Authentication-Results:` (шукайте dmarc=pass або dmarc=fail)
4. **Порівняння:** Перевірте результати автентифікації в Google Admin Toolbox — чи збігаються вони з тим, що ви знайшли вручну?