UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA

Maestría en Seguridad Informática

Seguridad de Redes TCP/IP

Sniffing utilizando Wireshark

Integrantes Grupo #4

1693-10-7018 Mario Paul Figueroa Sandoval

1693-15-10442 Wilfredo Ricardo Chim Chim

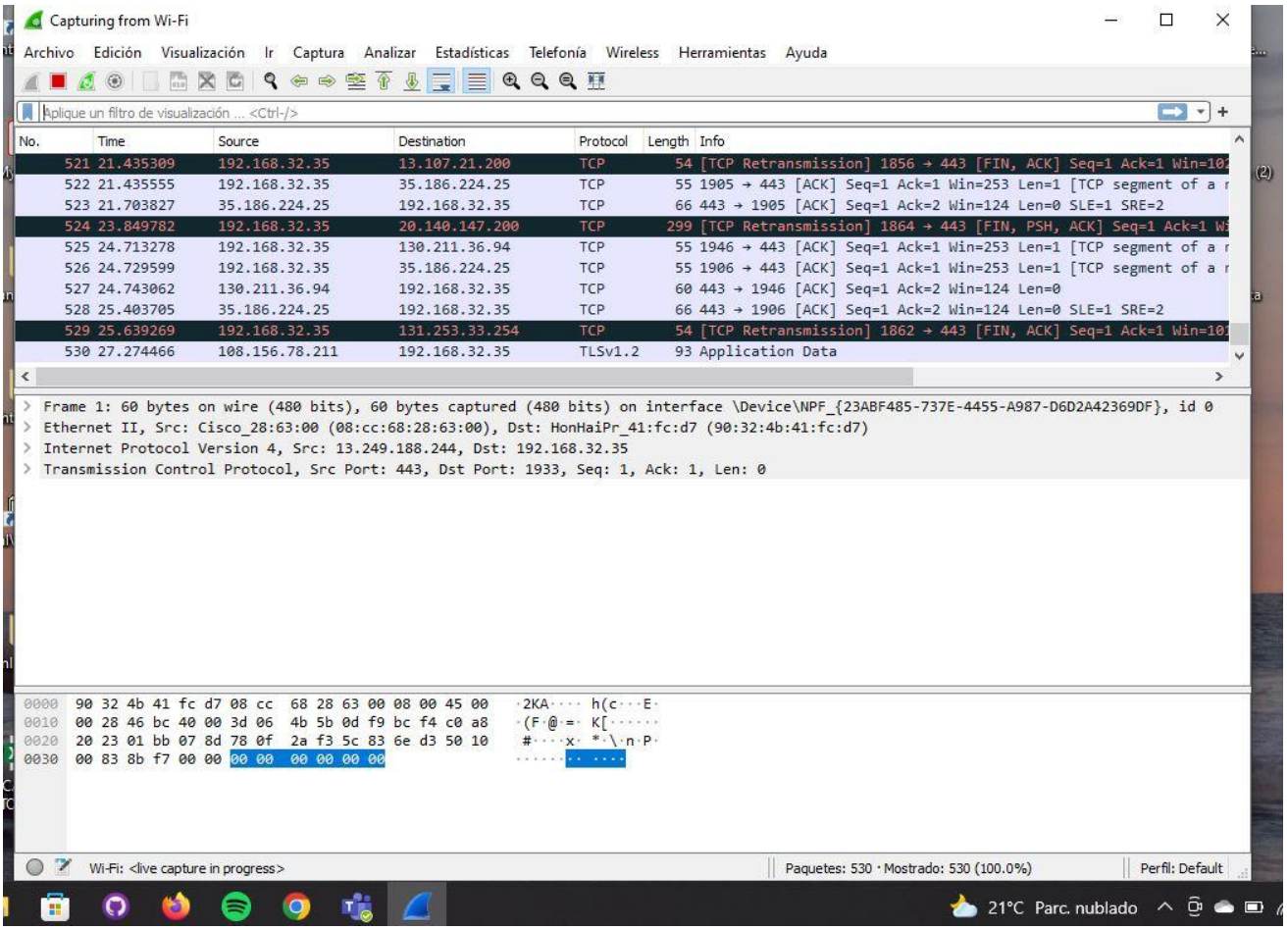
1693-12-7620 Rubenz Diego Alfredo Brito Ceto

1693-17-4319 Leonel Raymundo Jesús

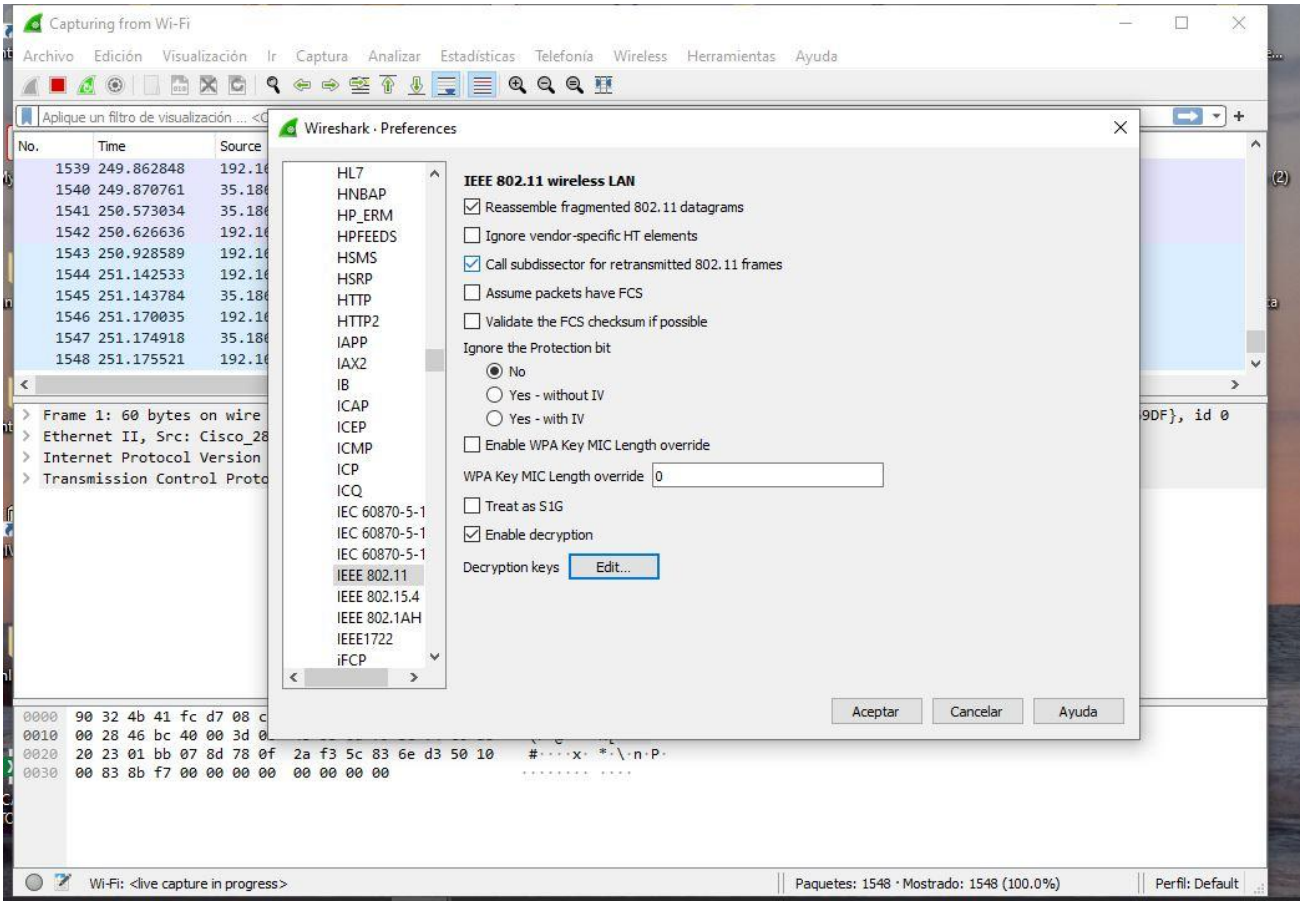
- **Sniffing WEP y Desencriptar**

Se utilizará una herramienta llamada Wireshark para registrar el tráfico de paquetes de la red.

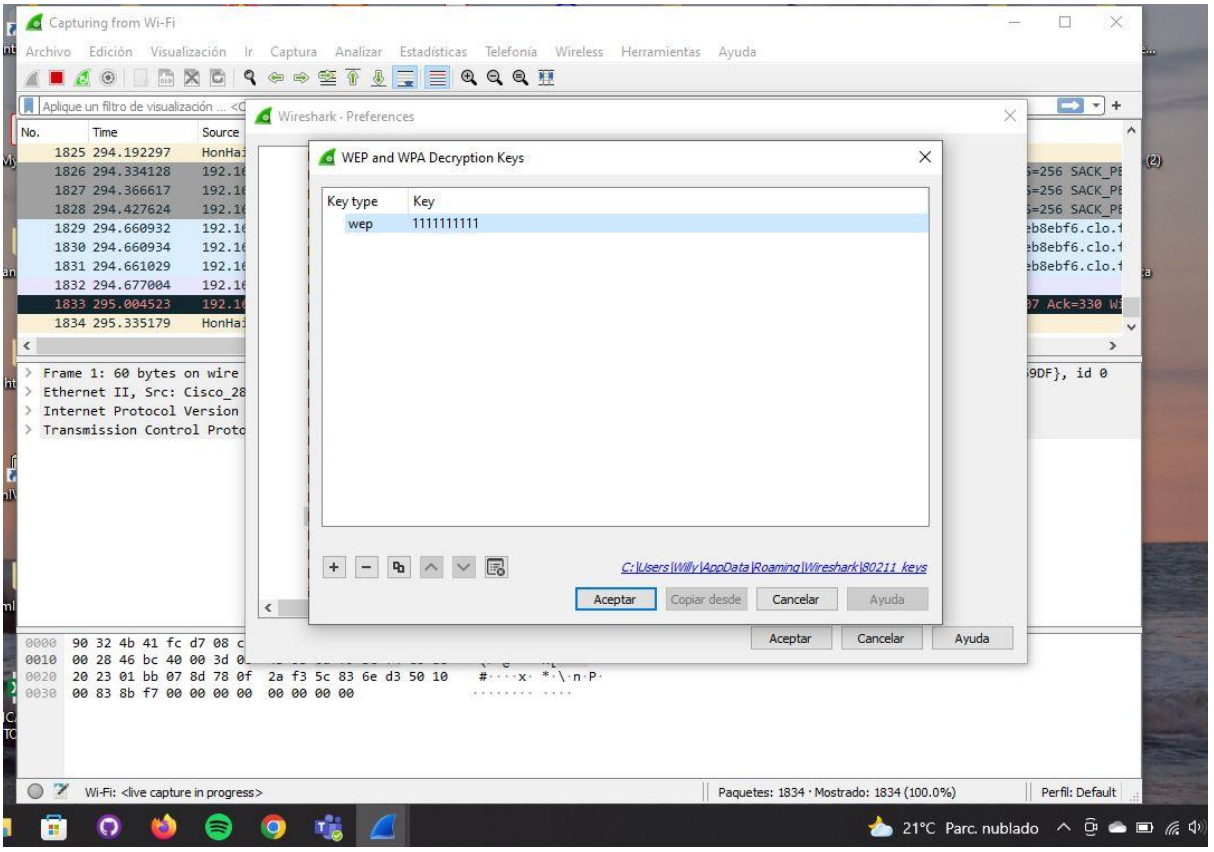
Al realizar este escaneo se podrá comprobar que el direccionamiento ip de los equipos de la red se encuentra oculto.



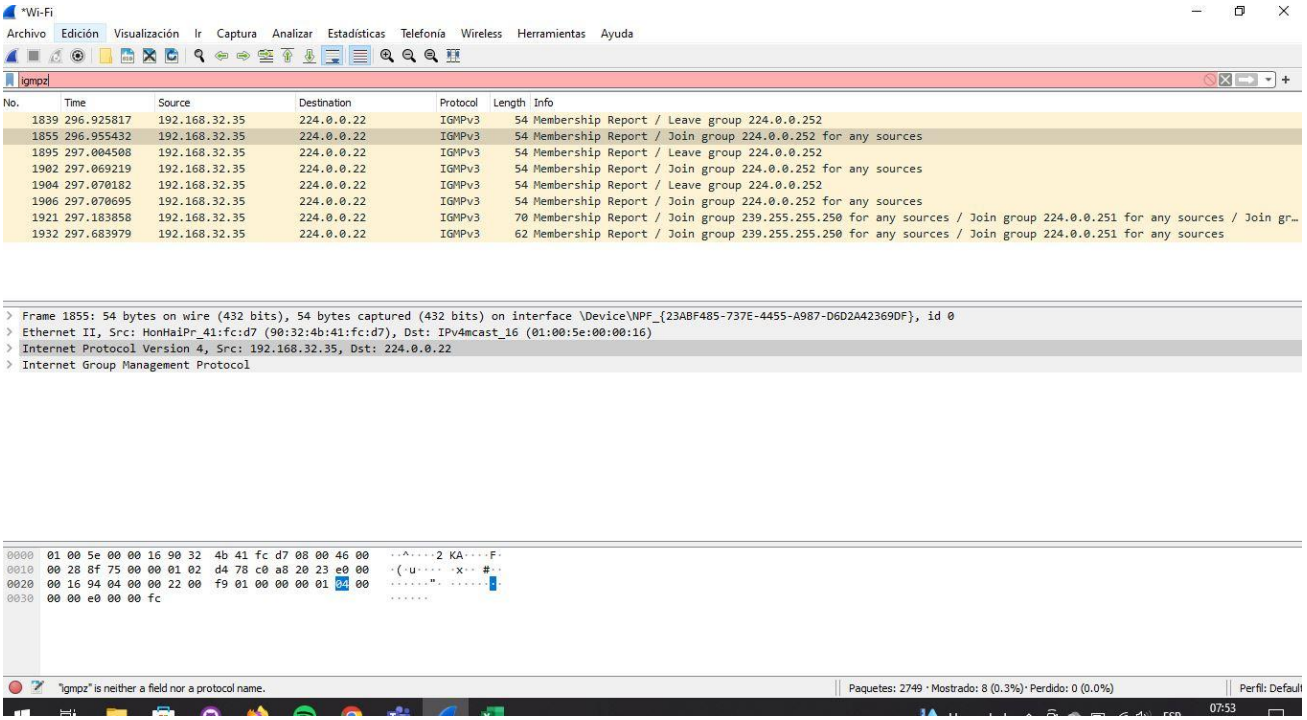
Configuramos lo siguiente: en Edición->Configuración->Protocolos->IEEE 802.11, pudimos decodificar las direcciones de los dispositivos de la red.



Se configura la clave de descifrado WEP en el protocolo IEEE 802.11, La clave debe proporcionarse como una cadena de números hexadecimales, con o sin dos puntos, y se analizará como una clave WEP

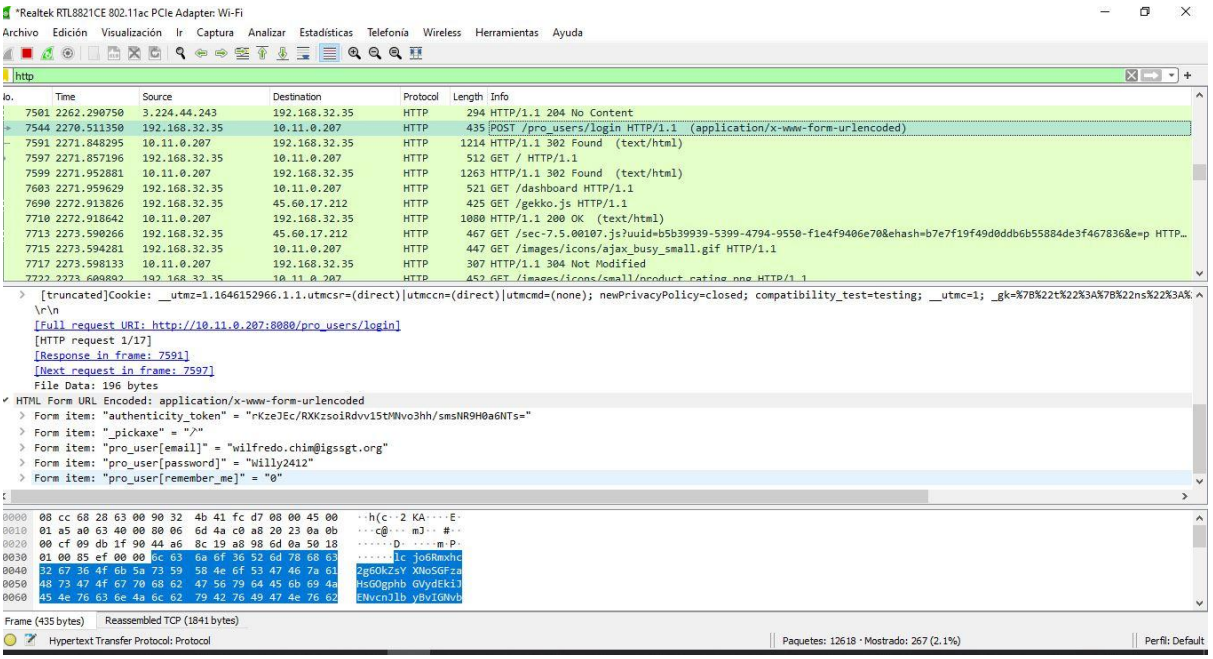


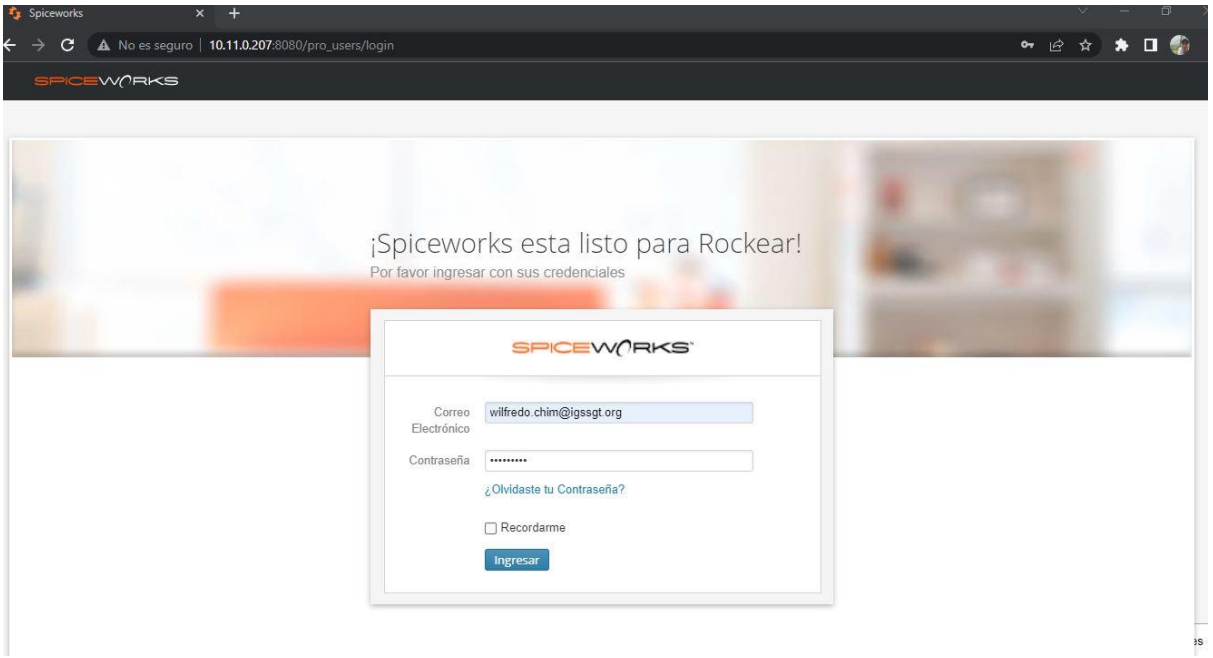
El filtrado por IP con Wireshark permite observar el enrutamiento descifrado de cada ordenador de la red y analizar sus paquetes.

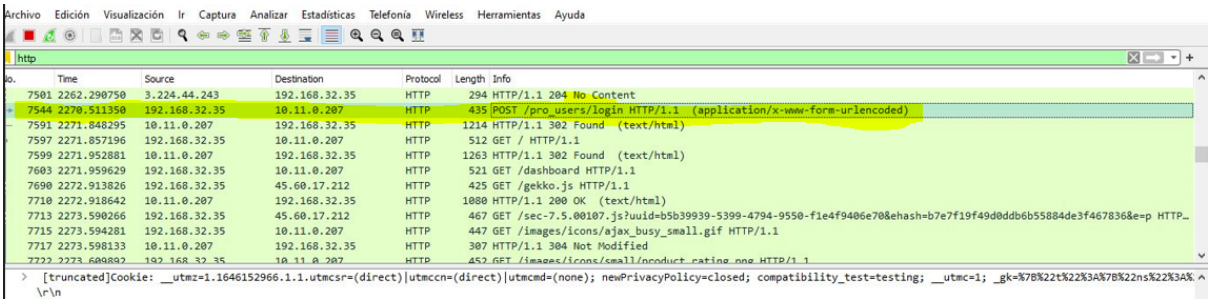


- Password Sniffing

Es una técnica de hacking que permite a los hackers robar nombres de usuario y contraseñas mediante el uso de aplicaciones de software especiales para observar y grabar pasivamente el tráfico de la red. Esto suele ocurrir en las redes WiFi públicas, donde es relativamente fácil espiar el tráfico vulnerable o no cifrado.







[truncated]Cookie: __utmz=1.1646152966.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); newPrivacyPolicy=closed; compatibility_test=testing; __u
\r\n
[Full request URI: http://10.11.0.207:8080/pro_users/login]
[HTTP request 1/17]
[Response in frame: 7591]
[Next request in frame: 7597]
File Data: 196 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "authenticity_token" = "rKzeJEc/RXKzsoiRdvv15tMNvo3hh/smsNR9H0a6NTs="
Form item: "_pickaxe" = "/"
Form item: "pro_user[email]" = "wilfredo.chim@igssgt.org"
Form item: "pro_user[password]" = "Willy2412"
Form item: "pro_user[remember_me]" = "0"

```
000  08 cc 68 28 63 00 90 32  4b 41 fc d7 08 00 45 00   ··h(c··2 KA····E·
010  01 a5 a0 63 40 00 80 06  6d 4a c0 a8 20 23 0a 0b   ···c@··· mJ·· #··
020  00 cf 09 db 1f 90 44 a6  8c 19 a8 98 6d 0a 50 18   ·····D· ····m·P·
030  01 00 85 ef 00 00 6c 63  6a 6f 36 52 6d 78 68 63   ·····lc jo6Rmxhc
040  32 67 36 4f 6b 5a 73 59  58 4e 6f 53 47 46 7a 61   2g6OkZsY XNoSGFza
050  48 73 47 4f 67 70 68 62  47 56 79 64 45 6b 69 4a   HsGOgphb GVydEkiJ
060  45 4e 76 63 6e 4a 6c 62  79 42 76 49 47 4e 76 62   ENvcnJlb yBvIGNvb
```

Frame (435 bytes) Reassembled TCP (1841 bytes)