



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

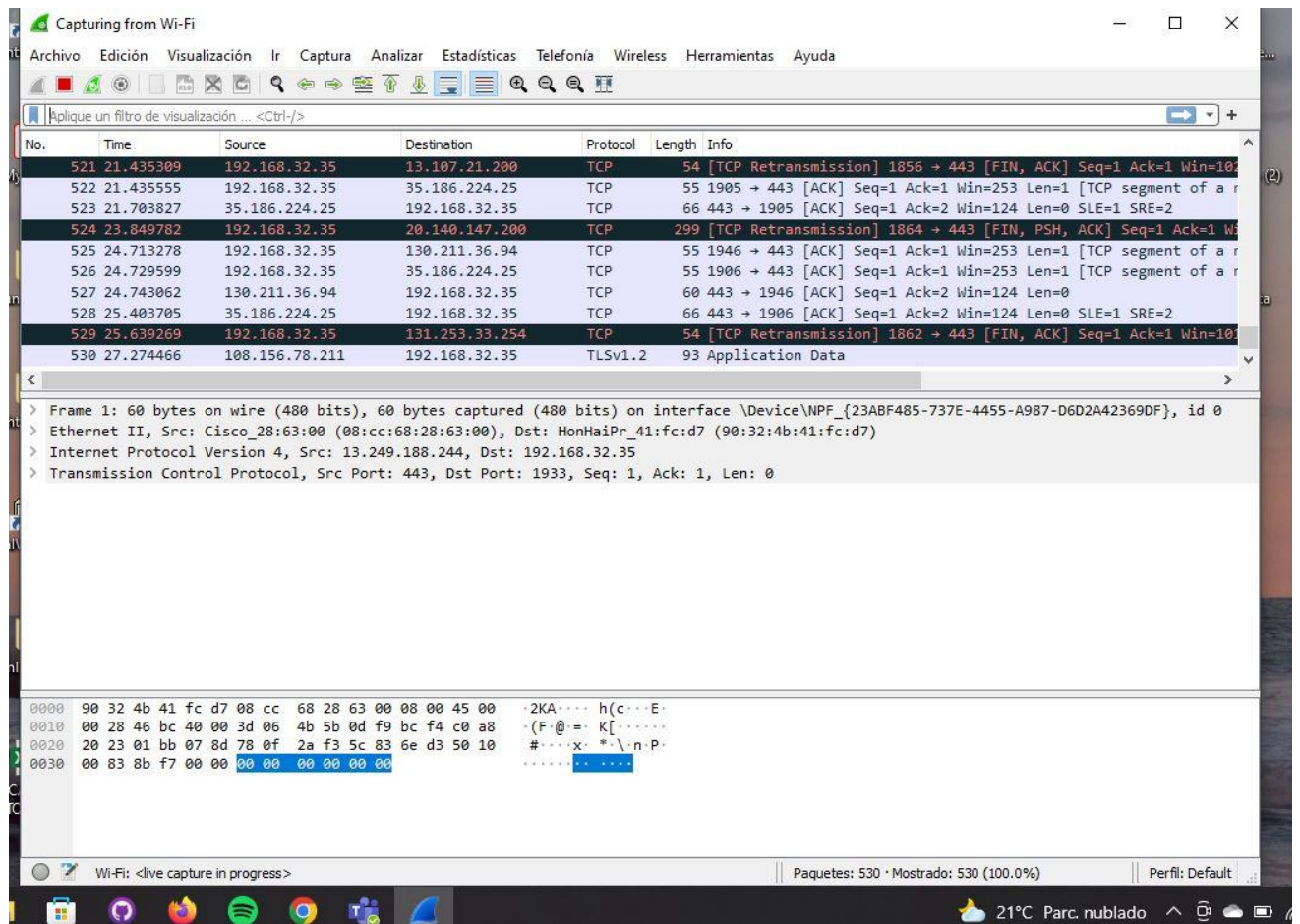
1693-12-7620 Rubenz Diego Alfredo Brito Ceto

1693-17-4319 Leonel Raymundo Jesús

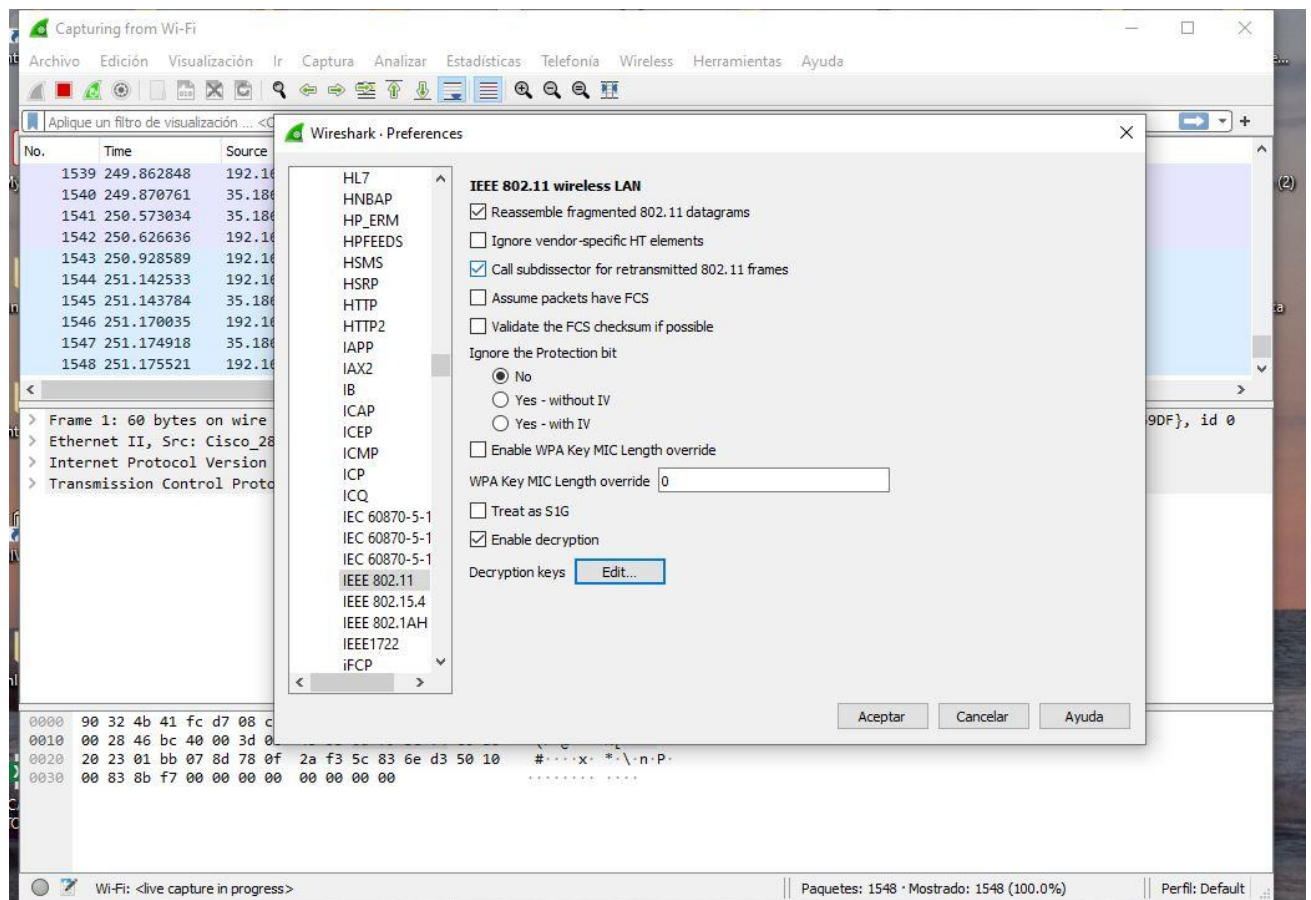
- **Sniffing WEP y Desencryptar**

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

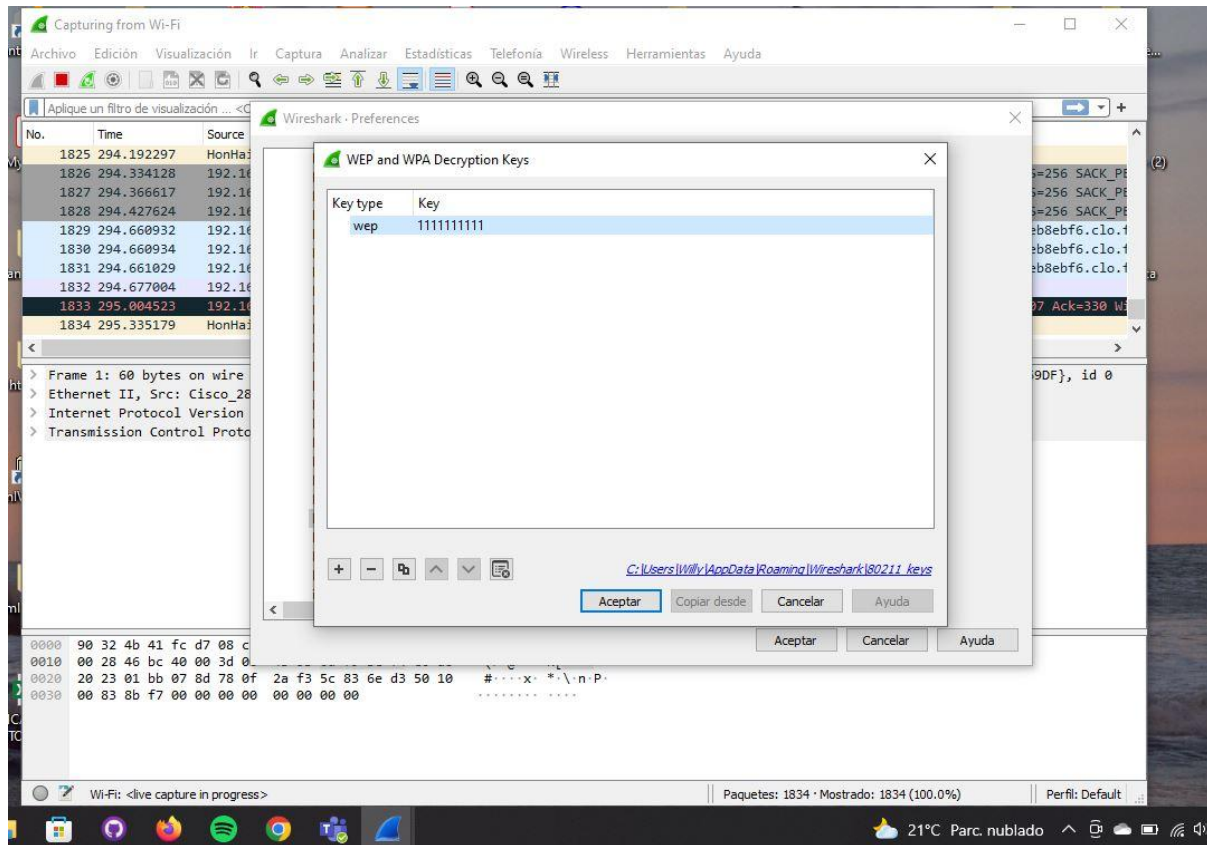
Al realizar este escaneo se podrá comprobar que el direccionamiento ip de los equipos de la red se encuentra oculto.



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.

Wireshark interface showing a packet capture of IGMPv3 messages. The packet list shows several 'Membership Report' packets from 192.168.32.35 to 224.0.0.22. The packet details pane shows the structure of an IGMPv3 Membership Report, including the group address and source address. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1839	296.925817	192.168.32.35	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
1855	296.955432	192.168.32.35	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
1895	297.004508	192.168.32.35	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
1902	297.069219	192.168.32.35	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
1904	297.070182	192.168.32.35	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
1906	297.070695	192.168.32.35	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
1921	297.183858	192.168.32.35	224.0.0.22	IGMPv3	70	Membership Report / Join group 239.255.255.250 for any sources / Join group 224.0.0.251 for any sources / Join gr-
1932	297.683979	192.168.32.35	224.0.0.22	IGMPv3	62	Membership Report / Join group 239.255.255.250 for any sources / Join group 224.0.0.251 for any sources

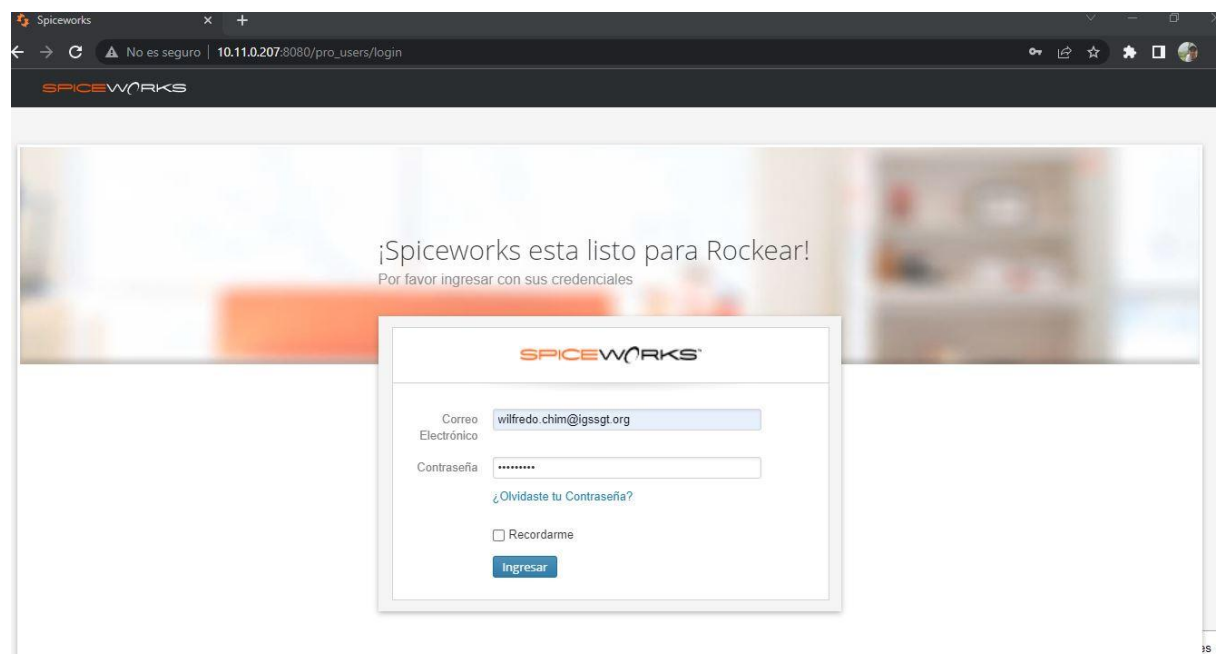
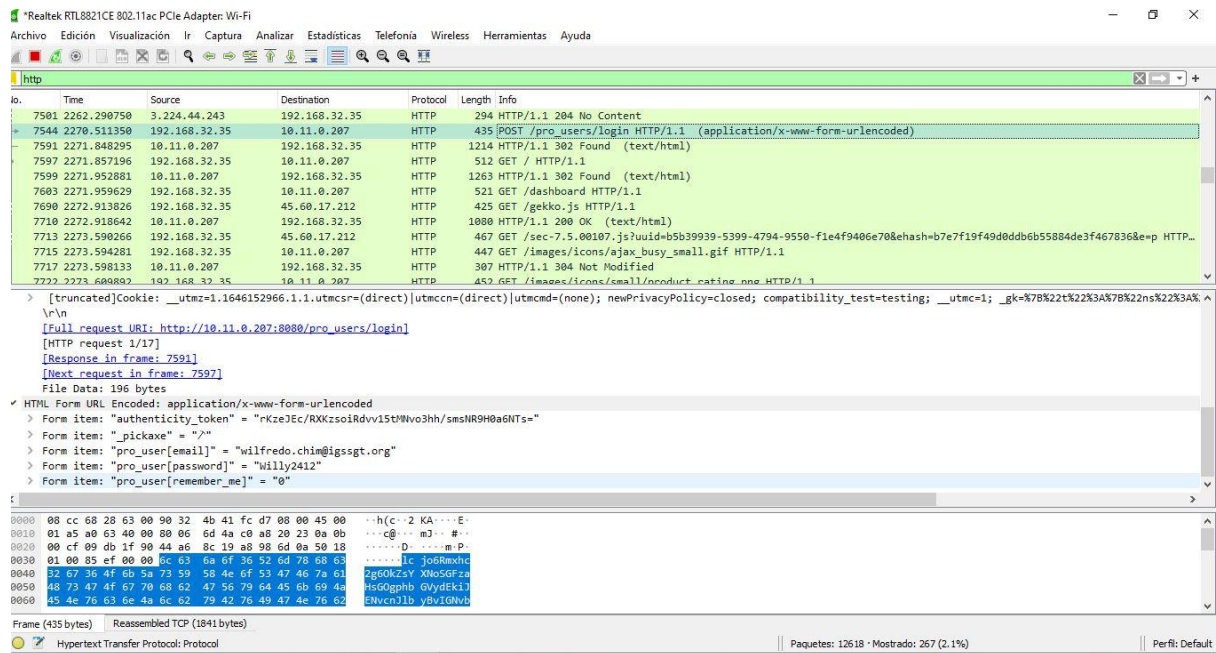
> Frame 1855: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{23ABF485-737E-4455-A987-D6D2A42369DF}, id 0
> Ethernet II, Src: HonHaiPr_41:fc:d7 (90:32:4b:41:fc:d7), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 192.168.32.35, Dst: 224.0.0.22
> Internet Group Management Protocol

0000 01 00 5e 00 00 16 90 32 4b 41 fc d7 08 00 46 00 ... 2 KA ... F-
0010 00 28 8f 75 00 00 01 02 d4 78 c0 a8 20 23 e0 00 ... (u ... x ... # ...
0020 00 16 94 04 00 00 22 00 f9 01 00 00 00 01 04 00
0030 00 00 e0 00 00 fc

"igmp2" is neither a field nor a protocol name. | Paquetes: 2749 - Mostrado: 8 (0.3%) - Perdido: 0 (0.0%) | Perfil: Default

- 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.utmcsrc=(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/RXKzsoiRdvV15tPwVo3hh/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"
```

Frame (435 bytes)	Reassembled TCP (1841 bytes)
-------------------	------------------------------