**IDS SNORT**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Ejercicio 1**](#_6erur3e87c8s) **2**

[**3. Ejercicio 2**](#_nqazzb649q3b) **2**

[**4. Ejercicio 3**](#_4yt9f8eds1xz) **4**

[**5. Ejercicio 4**](#_pdkryclpuh6p) **5**

[**6. Ejercicio 5**](#_v8com11juyyj) **7**

[**7. Ejercicio 6**](#_sj40utjtbeah) **8**

[**8. Ejercicio 7**](#_22vdsc1n3pkm) **9**

[**9. Ejercicio 8**](#_kyyh5djl4s6t) **10**

[**10. Ejercicio 9**](#_37v5ru22q5j1) **11**

[**11. Ejercicio 10**](#_n2uabjibu8j1) **12**

[**12. Ejercicio 11**](#_g27kw39d8hjy) **13**

[**13. Ejercicio 12**](#_anx7ku6yk6zp) **14**

[**14. Ejercicio 13**](#_qfp3zkmvzql7) **15**

[**Apartado B:**](#_w6qgt23zdcr2) **15**

[**Apartado C:**](#_k7vr3hixgg37) **16**

[**15. Ejercicio 14**](#_ywae9wro15ow) **17**

[**Apartado A:**](#_6i31uzmpbjzu) **17**

[**Apartado B:**](#_p0tch0e24mwp) **17**

[**Apartado C:**](#_l1syyyxjjca8) **18**

[**16. Ejercicio 15**](#_47y69zmit43e) **20**

[**Apartado B:**](#_dzdbjcwmg3ei) **20**

[**Apartado C:**](#_456s4iqbnrnv) **21**

[**Apartado D:**](#_ls5qosxi5f5n) **22**

[**17. Ejercicio 16**](#_7z0umygqk3jr) **22**

[**Apartado A:**](#_n6py3j8donq4) **22**

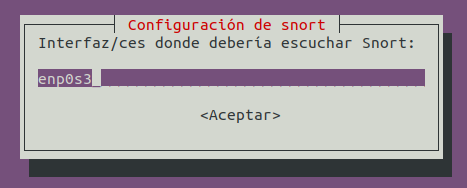
[**18. Ejercicio 17**](#_4krfi11iqdt4) **22**

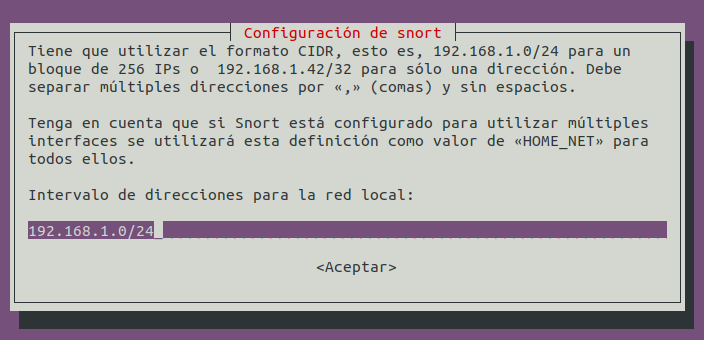
[**Apartado A:**](#_misehw6lgsam) **23**

[**Apartado B:**](#_jdol91gfizsh) **23**

[**Apartado C:**](#_yb1fjvcdhml) **23**

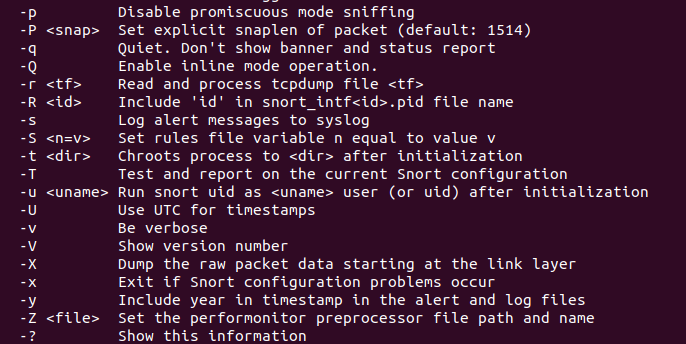
# **2. Ejercicio 1**

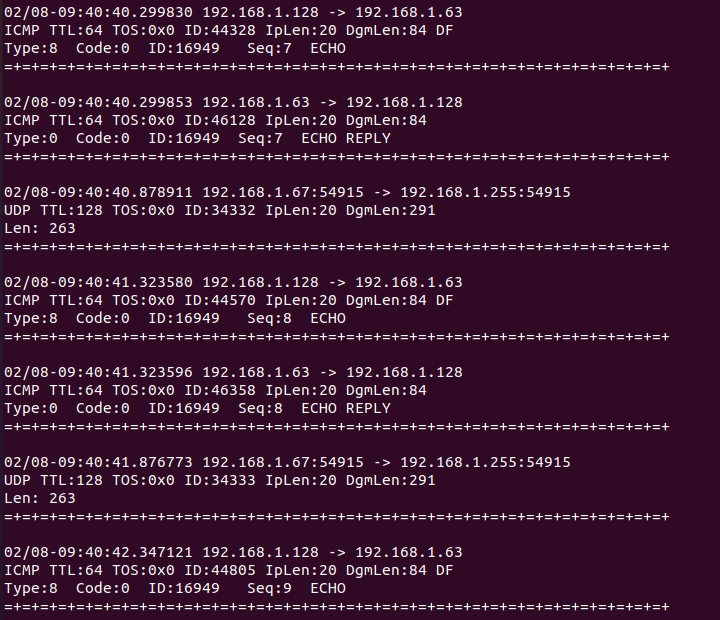




# **3. Ejercicio 2**

### 



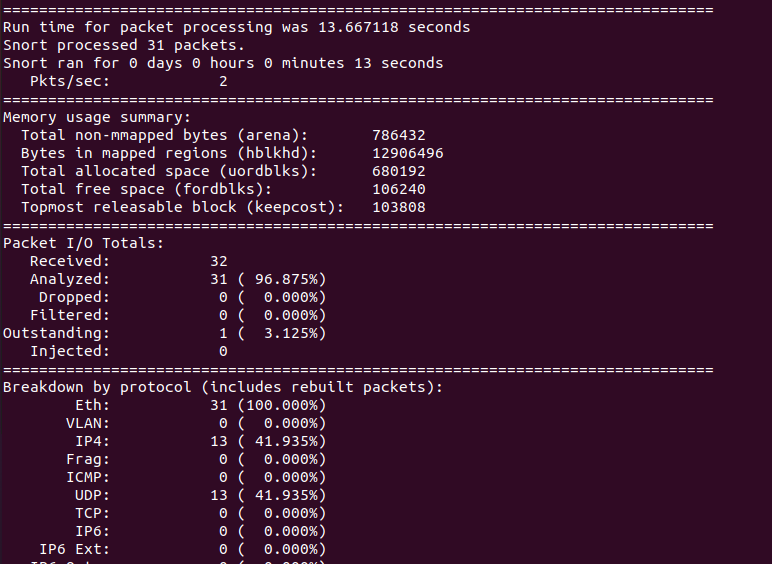


# **4. Ejercicio 3**

### 

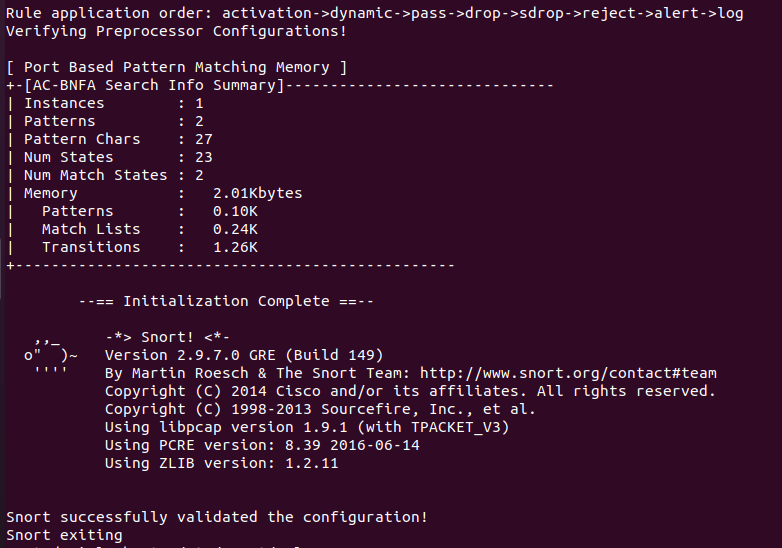
# **5. Ejercicio 4**

### 



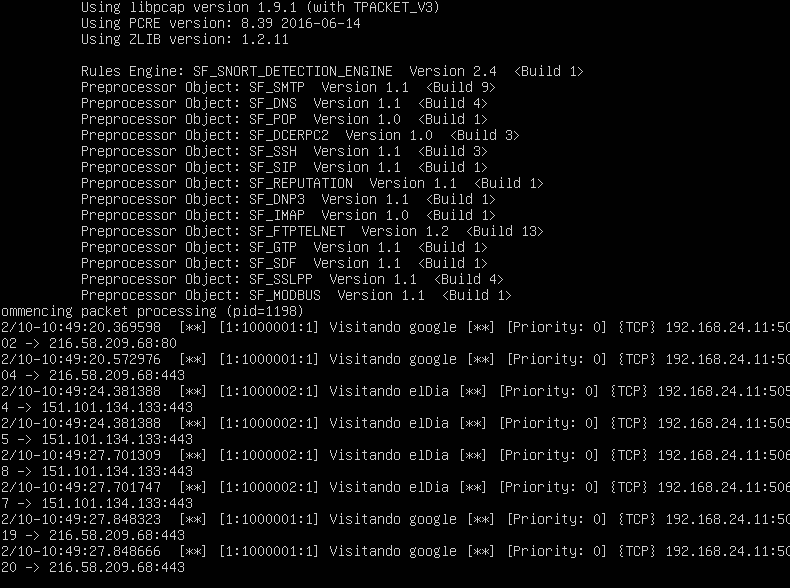
# **6. Ejercicio 5**

### 



# **7. Ejercicio 6**

### 



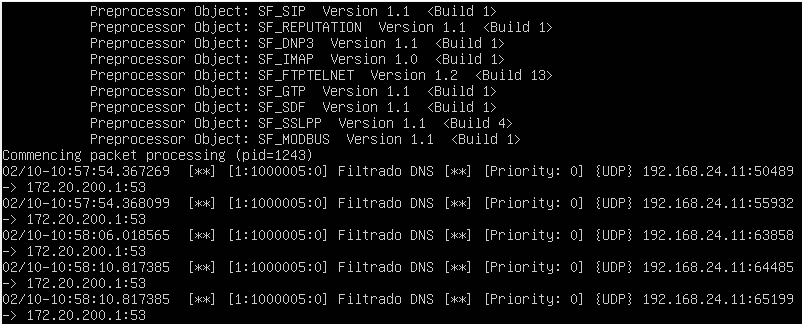
# **8. Ejercicio 7**

### 

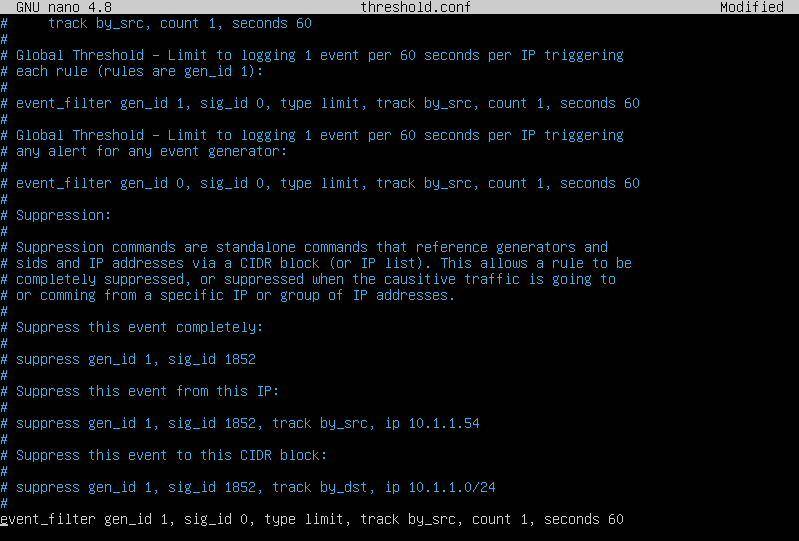


# **9. Ejercicio 8**

### 



# **10. Ejercicio 9**



# **11. Ejercicio 10**

### 

### 

# **12. Ejercicio 11**

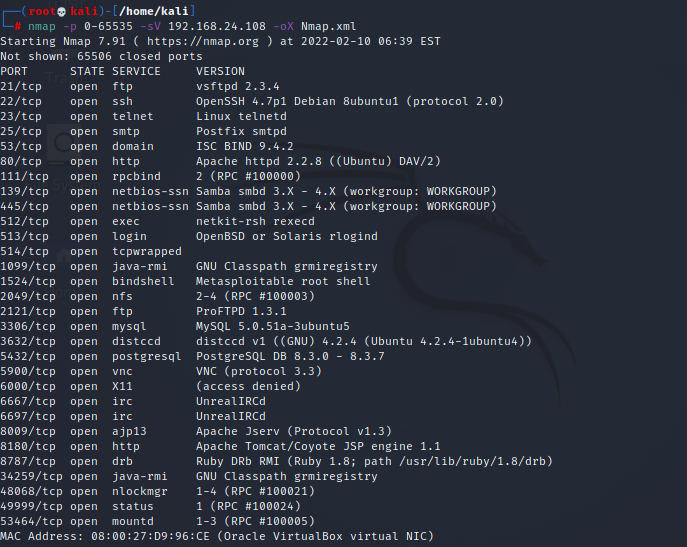
### 

# **13. Ejercicio 12**

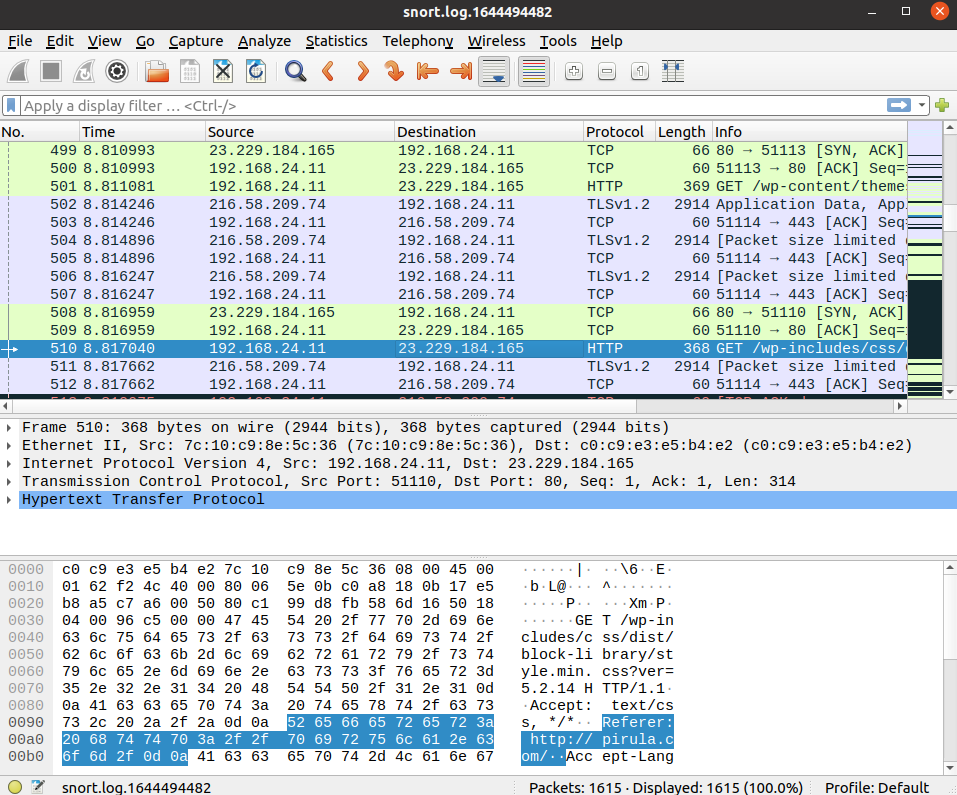
### 

# **14. Ejercicio 13**

### **Apartado B:**



### **Apartado C:**



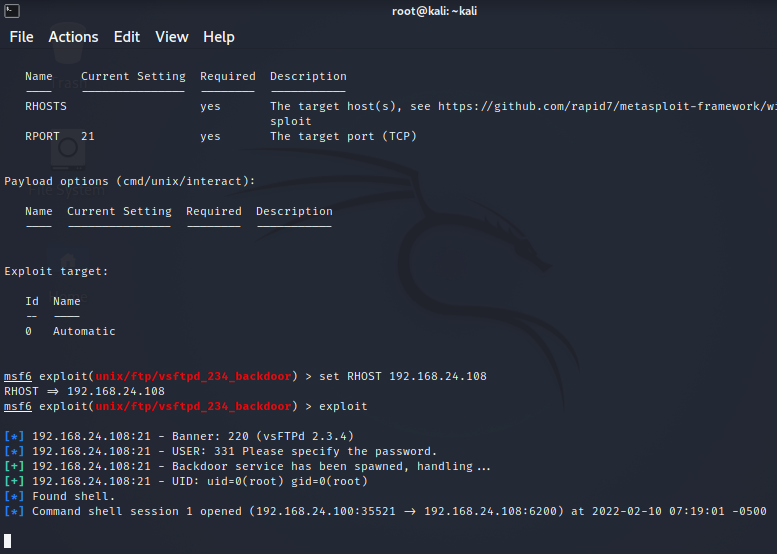
# **15. Ejercicio 14**

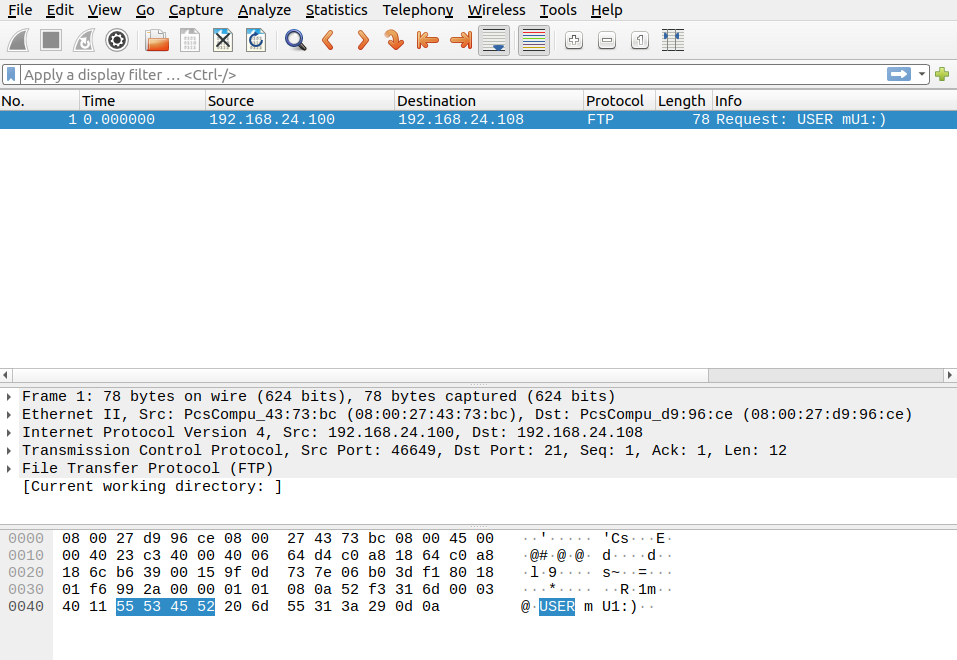
### **Apartado A:**



### **Apartado B:**

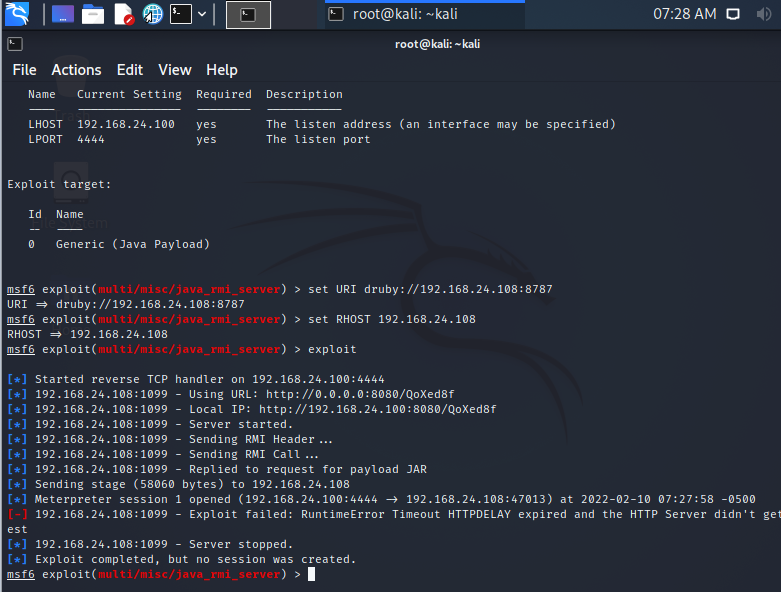


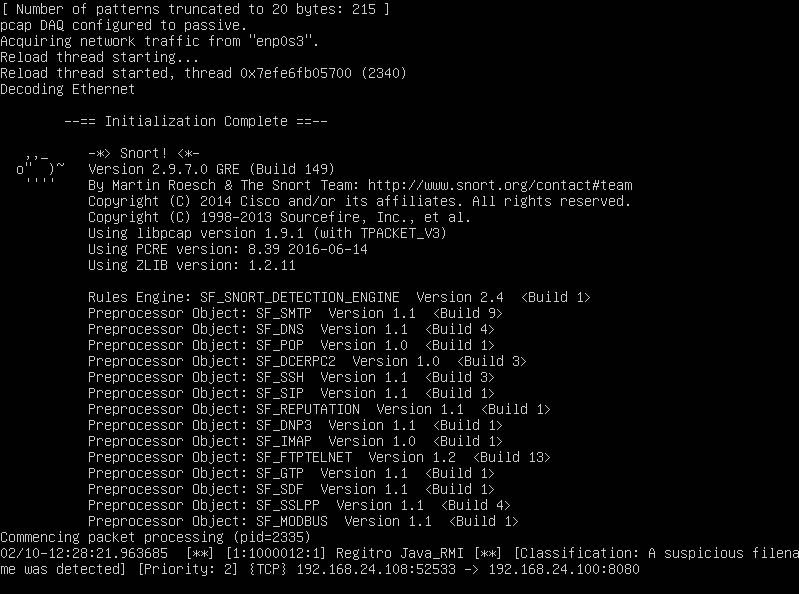




### **Apartado C:**





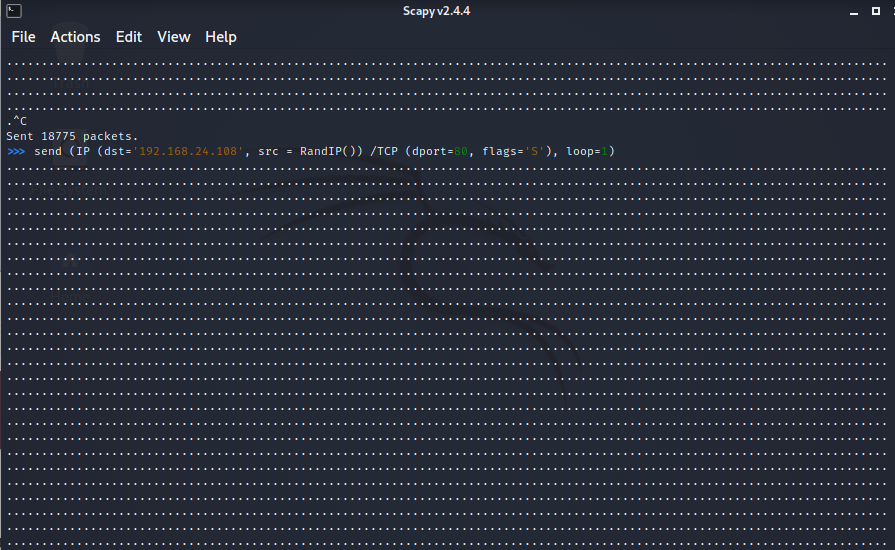


# **16. Ejercicio 15**

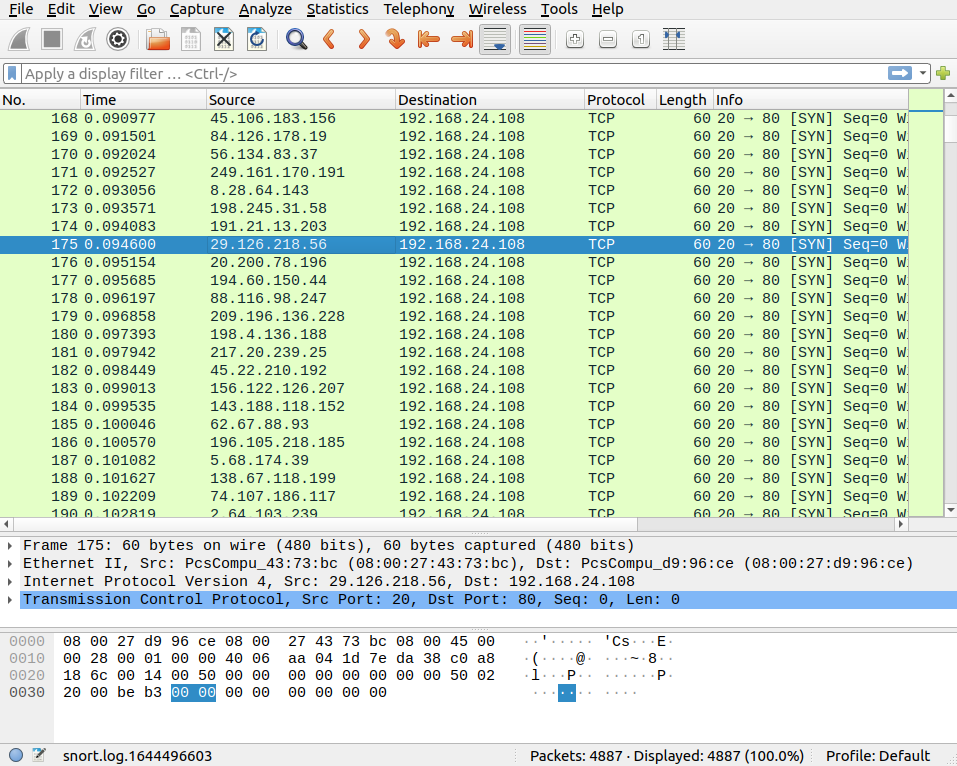
### **Apartado B:**



### **Apartado C:**



### **Apartado D:**



# **17. Ejercicio 16**

### **Apartado A:**



Creamos una alerta para indicarnos cuando intentan acceder mediante ssh con cualquier usuario.

# **18. Ejercicio 17**

### **Apartado A:**

**¿Qué son los preprocesadores de SNORT?**

Los preprocesadores, son unos módulos o plugins que usa Snort para arreglar, reparar y modificar tramas que vienen del decodificador de paquetes antes de que pasen por el motor de detección y las reglas.

### **Apartado B:**

**¿Qué son las listas blancas y listas negras?**

Un paquete se puede configurar de diferentes modos, los cuales determinan qué es más importante. Si se establece en la lista negra, el paquete generará una alerta. Si esto está configurado en la lista blanca, entonces se permitirá que el proceso pase.

### **Apartado C:**

**¿Podríamos almacenar los logs en una base de datos de SQL?**

Crearemos la base de datos y toda la configuración necesaria para la comunicación entre SNORT y MYSQL.

Una vez hecho esto, crearemos las tablas de la base de datos y modificaremos la configuración del fichero snort.conf para que las alertas sean dirigidas a la base de datos MYSQL.