eJERCICIOS DE ANÁLISIS DE TRÁFICO I

Apellidos, Nombre

Dirección de correo electrónico



**INDICE**

[Escenario planteado: 2](#__RefHeading___Toc3644_207282615)

[Preguntas: 2](#__RefHeading___Toc3646_207282615)

[1. ¿Cuál es el nombre del amigo de Ann? 2](#__RefHeading___Toc3648_207282615)

[2. ¿Cuál es el primer comentario de la conversación? 2](#__RefHeading___Toc3650_207282615)

[3. ¿Cuál es el nombre del archivo transferido? 2](#__RefHeading___Toc3652_207282615)

[4. ¿Cuáles son los “magic number” del fichero que se quiere extraer (4 primeros bytes)? 2](#__RefHeading___Toc3654_207282615)

[5. ¿Cuál es el MD5 del fichero? 2](#__RefHeading___Toc3656_207282615)

[6. ¿Cuál es la receta secreta? 2](#__RefHeading___Toc3658_207282615)

[Herramientas: 2](#__RefHeading___Toc3660_207282615)

[Análisis: 3](#__RefHeading___Toc3662_207282615)

# **Escenario planteado**:

La empresa Anarchy sospecha que la empleada Ann está extrayendo información para sus competidores.

La empleada ha accedido a la **receta secreta** de la compañía, por ello los analistas de seguridad están preocupados de que se produzca una fuga de información.

Los analistas han estado monitorizando la actividad de Ann durante un tiempo pero aún no tenían evidencias…hasta ahora! Hoy ha aparecido un pc inesperado durante un pequeño periodo de tiempo en la red wifi de la compañía.

Se sospecha de alguien en el parking, ya que no se ha visto a ningún extraño en el edificio.

El equipo de Ann (192.168.1.158) ha estado enviando paquetes de mensajería instantánea a través de la red wifi a dicho pc.

# **Preguntas**:

### ¿Cuál es el nombre del amigo de Ann?

### ¿Cuál es el primer comentario de la conversación?

### ¿Cuál es el nombre del archivo transferido?

### ¿Cuáles son los “magic number” del fichero que se quiere extraer (4 primeros bytes)?

### ¿Cuál es el MD5 del fichero?

### ¿Cuál es la receta secreta?

# **Herramientas**:

Listado de herramientas utilizadas:

* *Herramienta1*
  + *Sitio oficial de la herramienta*

# **Análisis**: