Auditoria informatica a Twitter

Jorge González

Profesor: Maximiliano Vega

29/ 11 /2017

Creadores e historia

-fundador
Jack Dorsey 21 de marzo del 2006.
-Twitter surgió como proyecto
de investigación dentro de Obvious.
-una pequeña
compañía situada en San Francisco.
-Consejo
de Administración está formado por
Dorsey, Evan Williams y Biz Stone.

Datos técnicos

Escrita en Ruby on Rails
Se caracterizapor su interfaz sencilla.
Todos los mensajes de Twitter van a parar al servidor servidor de un software programado en Scala la API está totalmente abierta a desarrolladores

Datos Especificos

- Localización San Francisco, California
- País de origenEstados Unidos
- Área de servicio Mundial
- Fundador(es):
  - Jack Dorsey
  - Noah Glass
  - Biz Stone
  - Evan Williams
- Presidente Omid Kordestani

Hackeo ético

- Hats, hackers
de sombrero blanco, o hacker éticos
-Black Hat o ciberdeluente

Exploit

Que es un Exploit?:
aprovecha de un agujero de seguridad

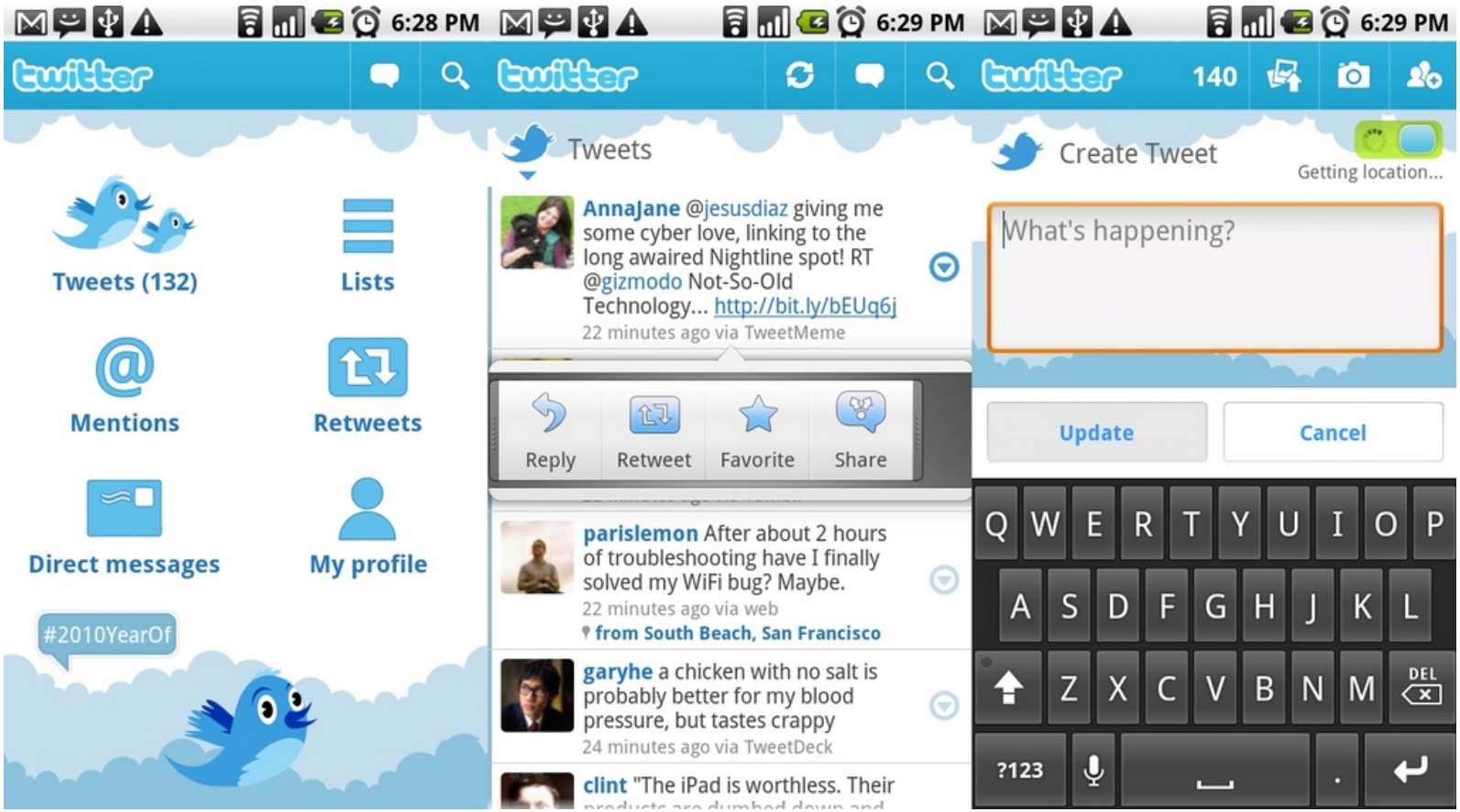
Medidas de protección

- Mantener todas nuestras aplicaciones y sistemas actualizados.
- Mitigar los efectos de posibles exploits usados en nuestra contra.
- Contar con una solución de seguridad avanzada como.

algunos ejemplos

- Análisis dinámico.
- Comunicación con el servidor
- Estudio de la estructura de protección del almacenamiento de datos.
- Decompilación de la aplicación.
- Revisión del código fuente.

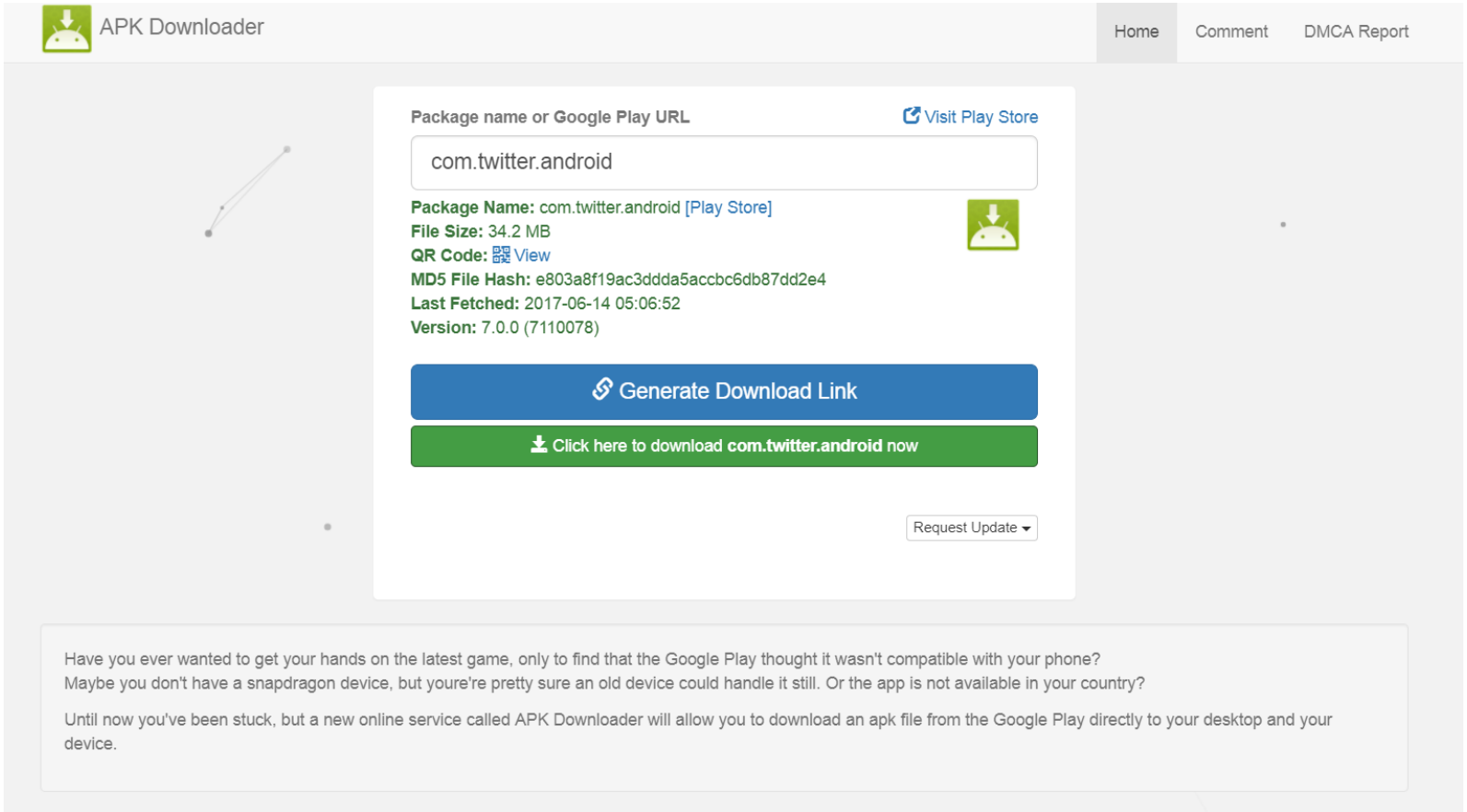
aplicacion por Auditar



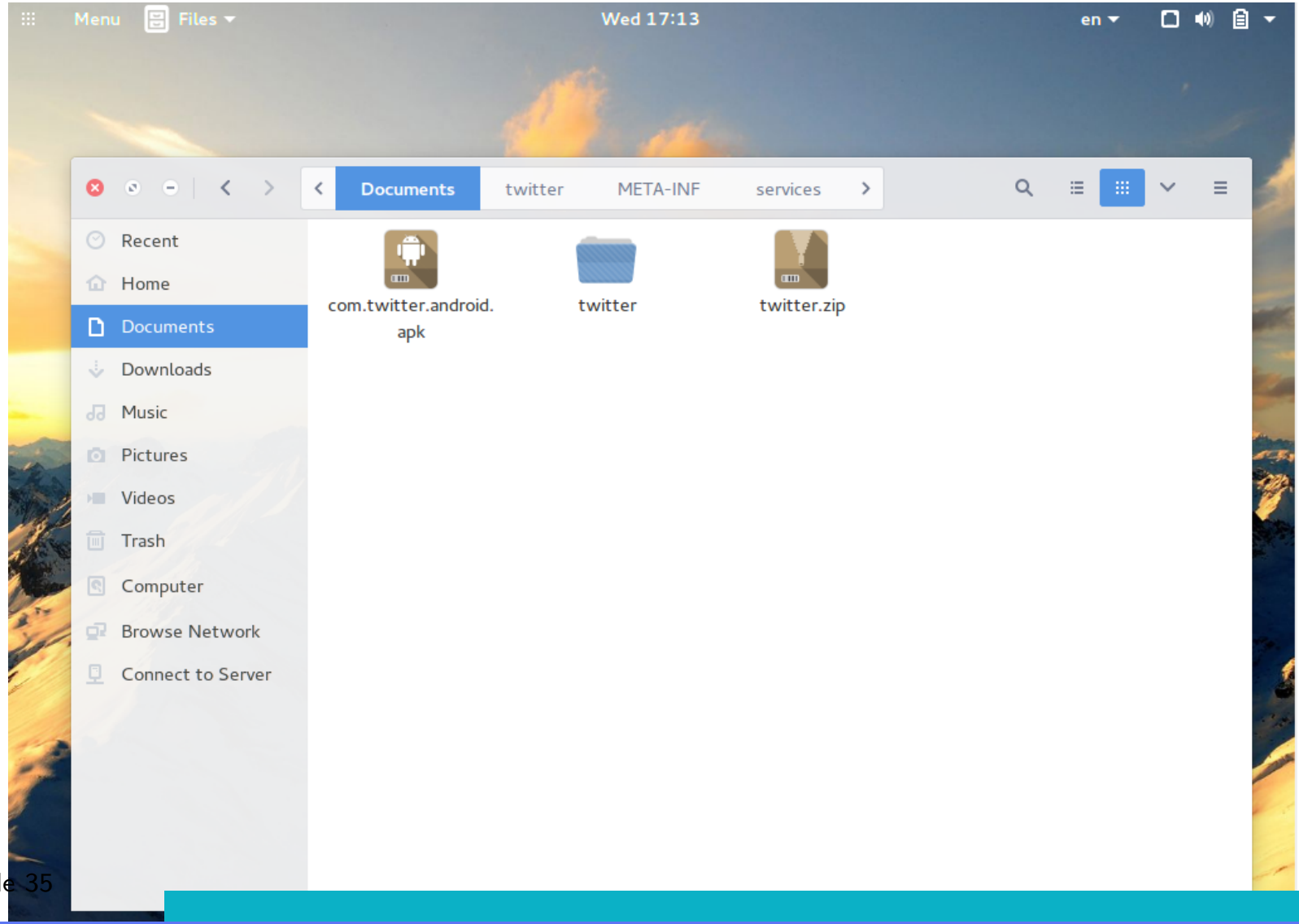
Más de 32 millones de cuentas de Twitter fueron hackeadas

Pruebas con exploits

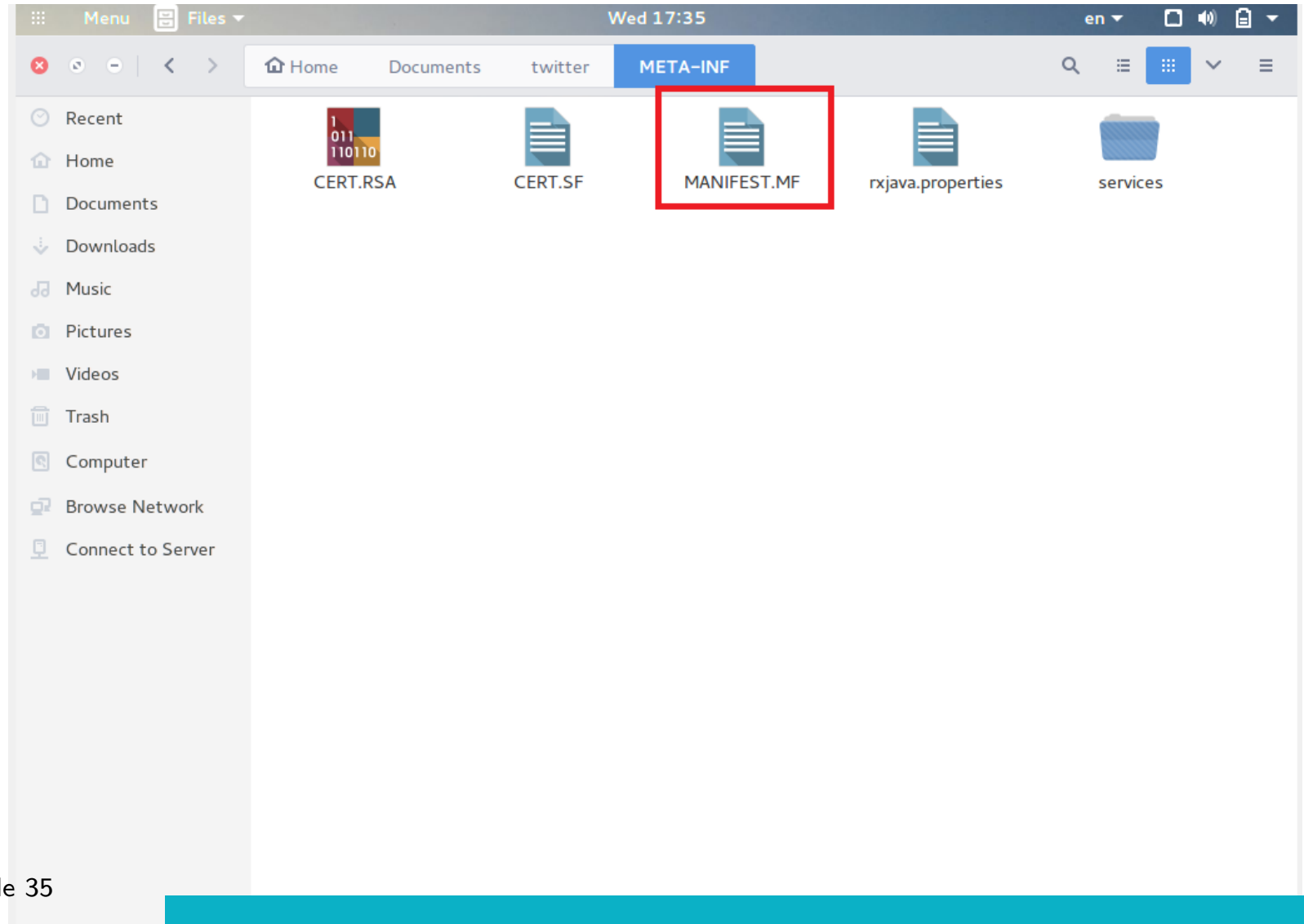
decompilado de la aplicacion



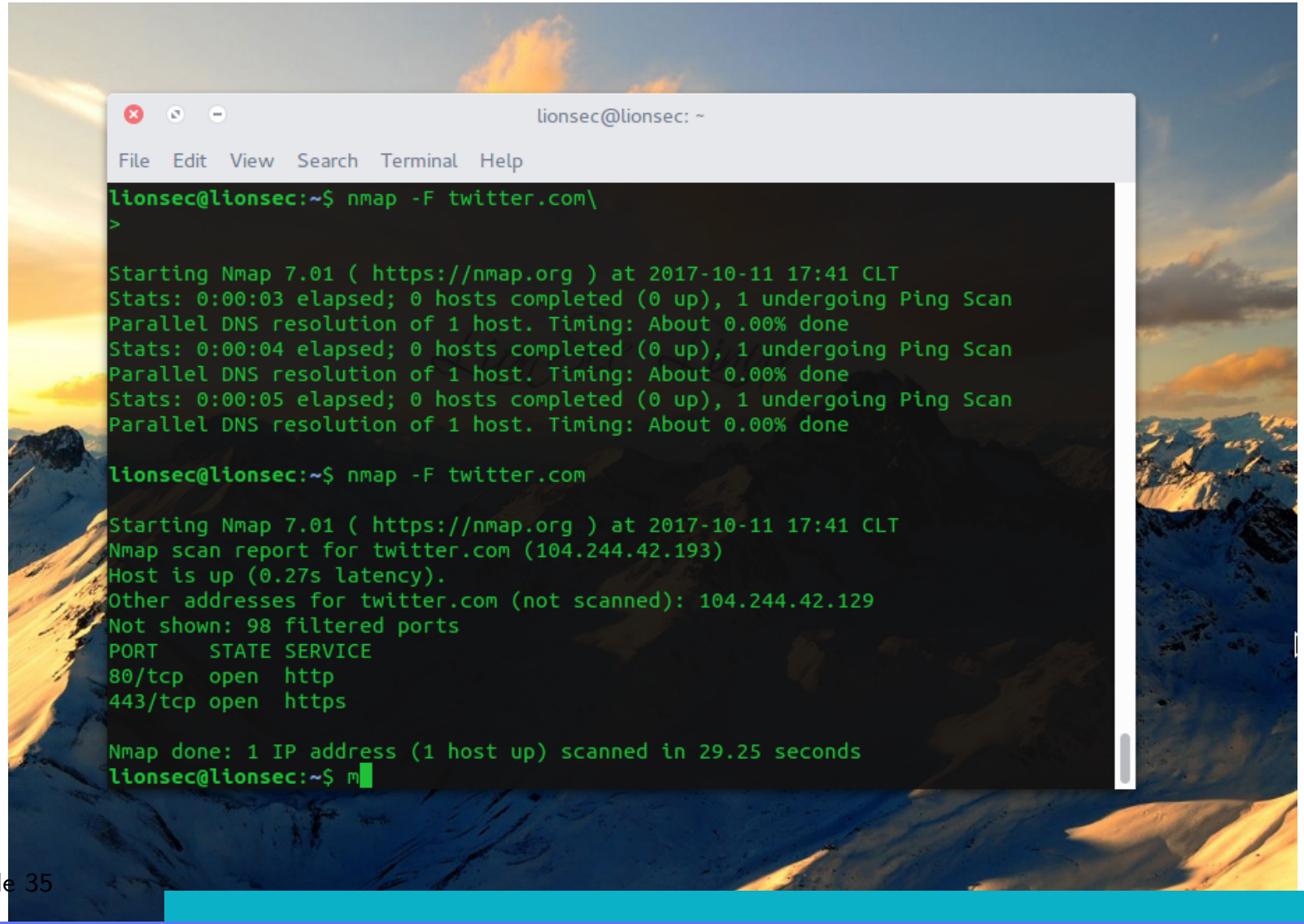
decompilado de la aplicacion



decompilado de la aplicacion



Puertos escaneados



que es SQLmap

Pruebas de inyecciones SQL

¿Que es SQLmap? Sqlmap
es una herramienta desarrollada en
el lenguaje python y es muy util para
hacer inyeccciones sql automatizados.

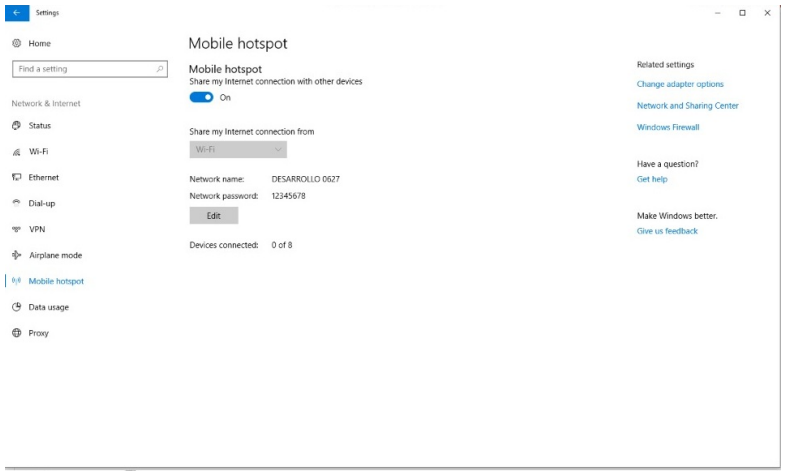
Inyeccción SQL

Pruebas de inyecciones SQL

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

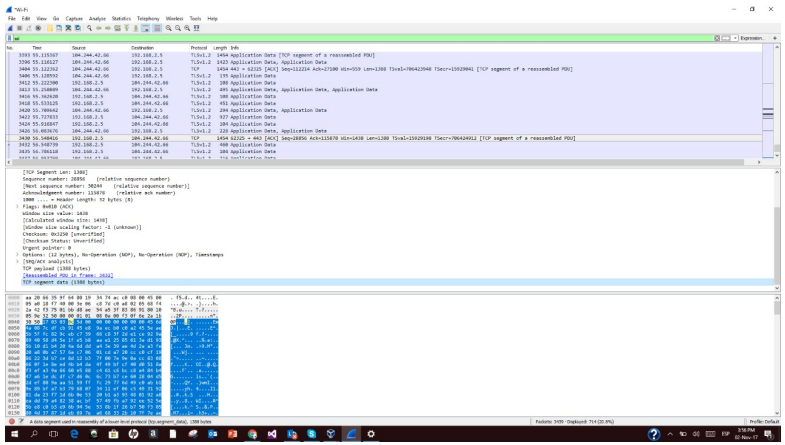
Prueba de Man in the middle

punto de acceso al computador



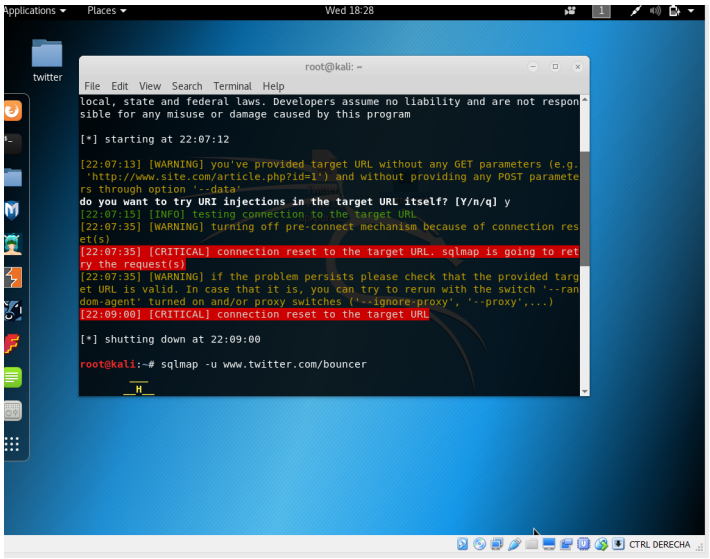
Prueba de Man in the middle

Prueba
de man in the middle con wireshark



Pruebas con SQLmap

Pruebas de inyecciones SQL

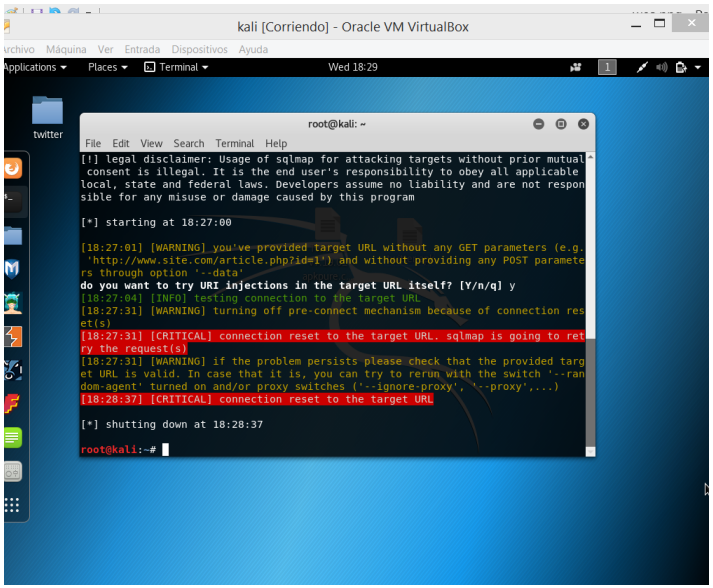


escaneos de las cuentas con SQLmap la la direccion twitter.com/account

Pruebas con SQLmap

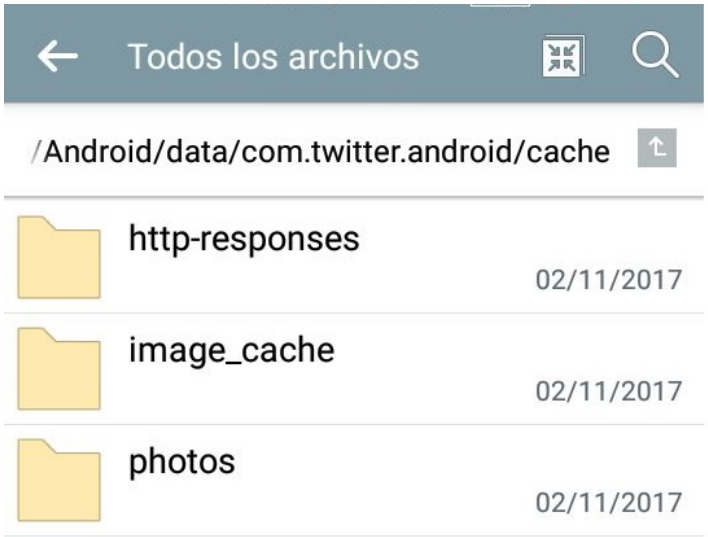
Pruebas de inyecciones SQL

escaneos de las cuentas
con SQLmap con twitter.com/follow



archivos en el telefono

carpetas internas de twitter

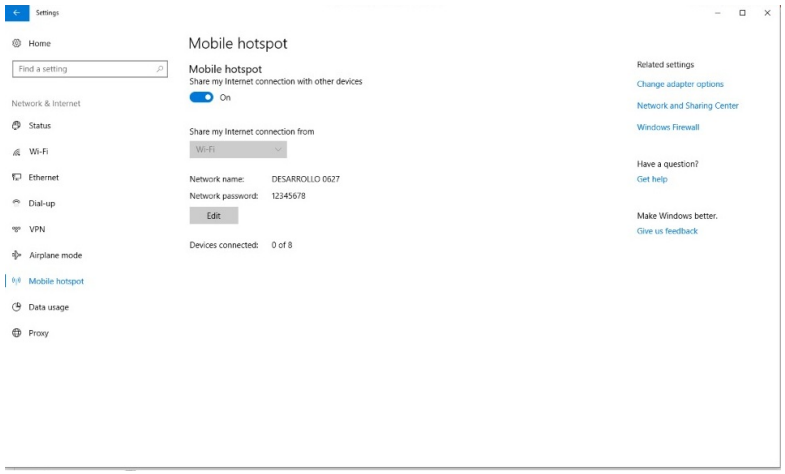


archivos en el telefono

archivos en android de twitter

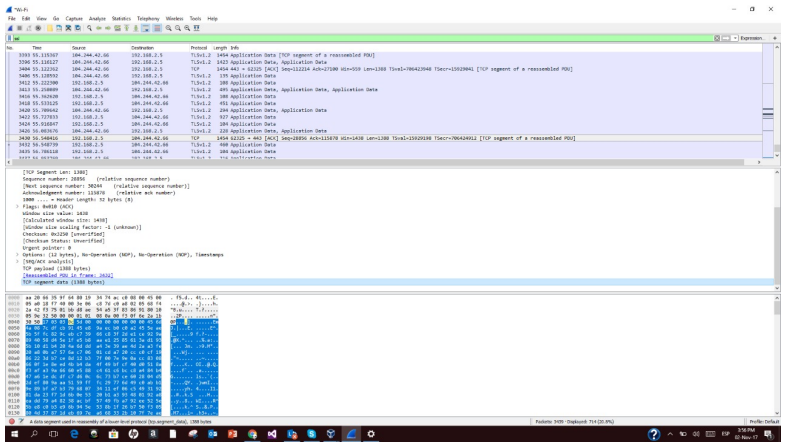
Prueba de Man in the middle

punto de acceso al computador



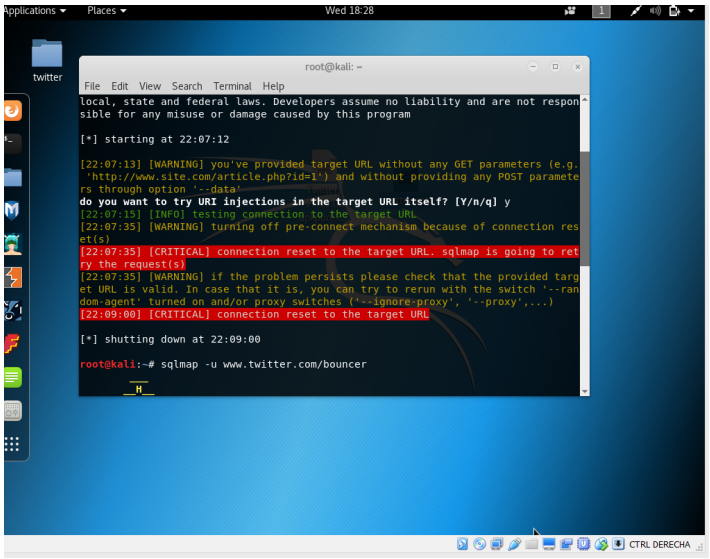
Prueba de Man in the middle

Prueba
de man in the middle con wireshark



Pruebas con SQLmap

Pruebas de inyecciones SQL

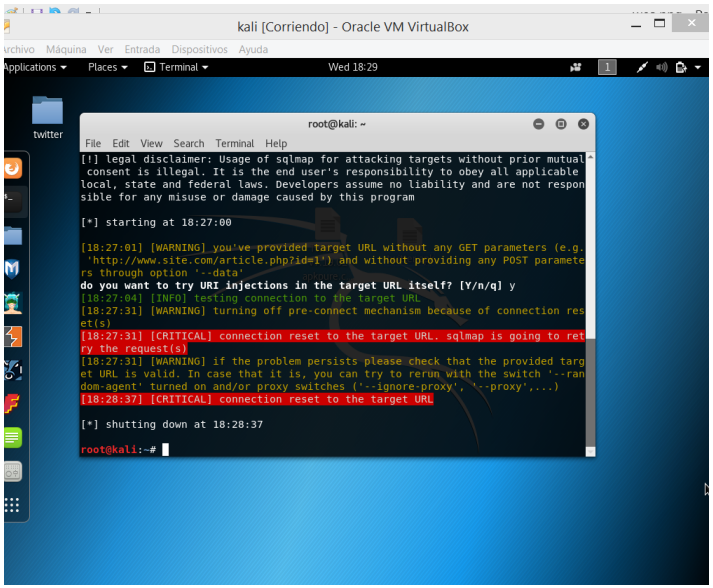


escaneos de las cuentas con SQLmap la la direccion twitter.com/account

Pruebas con SQLmap

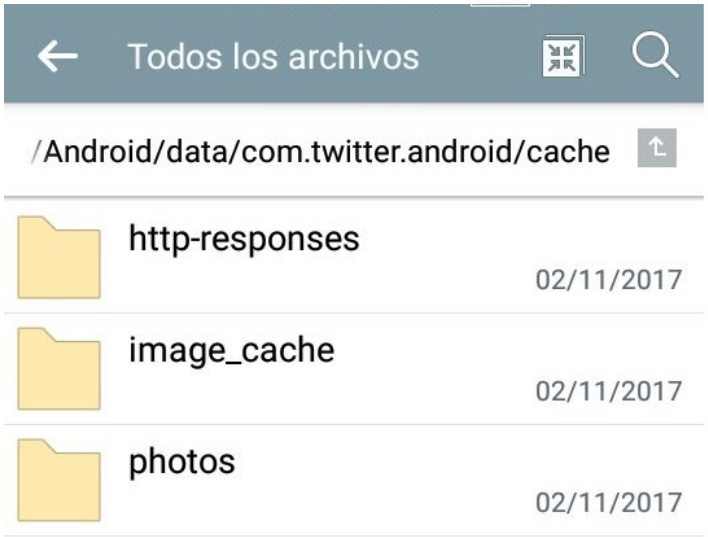
Pruebas de inyecciones SQL

escaneos de las cuentas
con SQLmap con twitter.com/follow



archivos en el telefono

carpetas internas de twitter



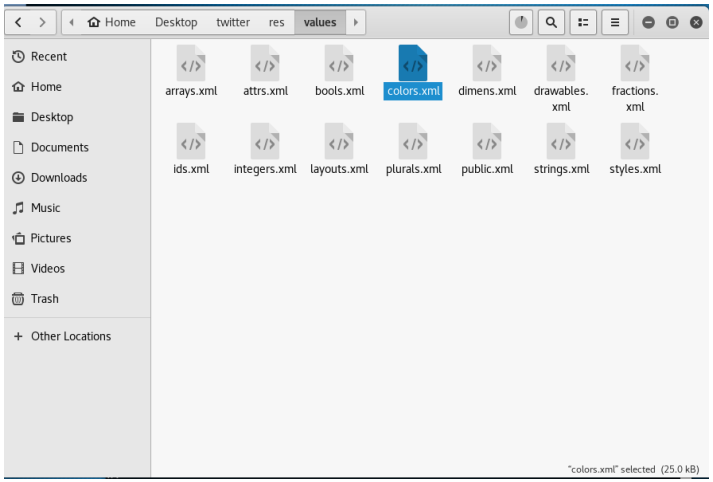
archivos en el telefono

archivos en android de twitter

Compilación de la aplicación

Cambio de valores en la aplicación

archivo de
la aplicación que contiene los colores



Compilación de la aplicación

Cambio de valores en la aplicación

cambio dentro del archivo

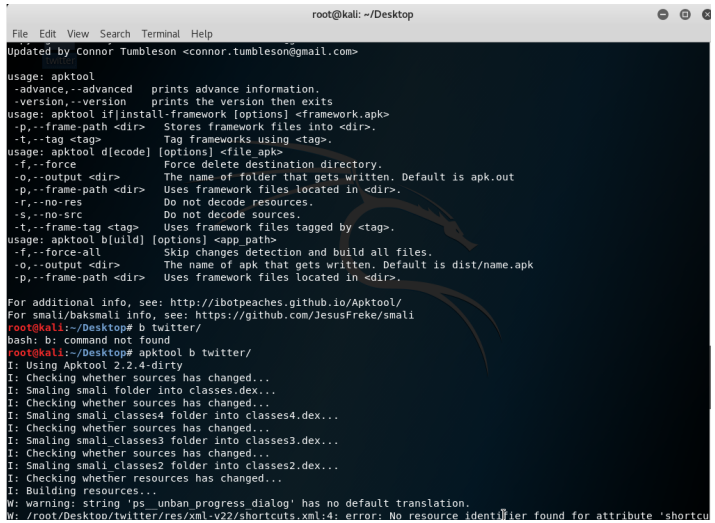
```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <color name="app_background">@color/black</color>
    <color name="badge_protected">@color/text_black</color>
    <color name="badge_verified">@color/twitter_blue</color>
    <color name="border_color">@color/tertiary</color>
    <color name="deep_gray">#ff657786</color>
    <color name="deep_gray_30">#4d657786</color>
    <color name="deep_gray_50">#80657786</color>
    <color name="faded_gray">#ffe6ecf0</color>
    <color name="faint_gray">#fff5f8fa</color>
    <color name="focused_bg">@color/faded_gray</color>
    <color name="footer_logo">@color/medium_gray</color>
    <color name="global_ripple_selector_color">#1d000000</color>
    <color name="light_gray">#ffccd6dd</color>
    <color name="list_bg">@color/clear</color>
    <color name="medium_gray">#ffaab8c2</color>
    <color name="medium_gray_50">#80aab8c2</color>
```

Compilación de la aplicación

Cambio de valores en la aplicación

intento

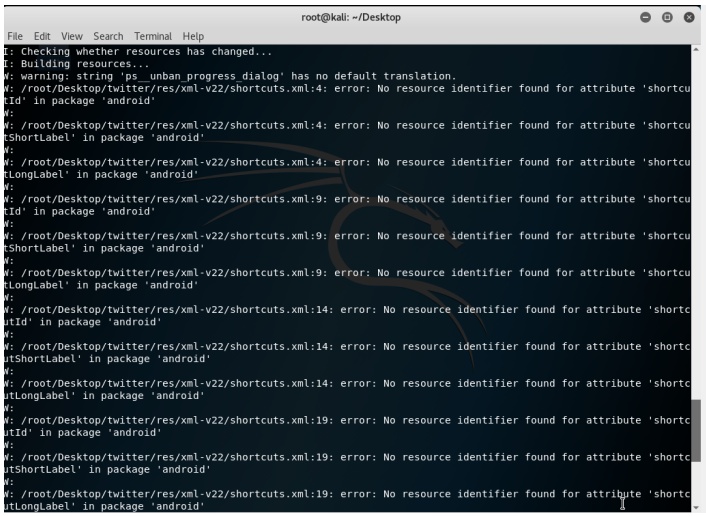
de contracción de la aplicación



Compilación de la aplicación

Cambio de valores en la aplicación

fallo al intentar compilar una aplicación ya que detecto que habían archivos que tenían modificaciones



ataqque Ddos

Investigación sobre ataque DDos

¿se puede realizar un ataque
de denegación de servicio a Twitter?

ataqque Ddos

Investigación sobre ataque DDos

segun
la revista especializada en informatica
aproximadamente entre 250
y 500 computadores. (García, 2017)