Facultad de Informática

19 de abril del 2017

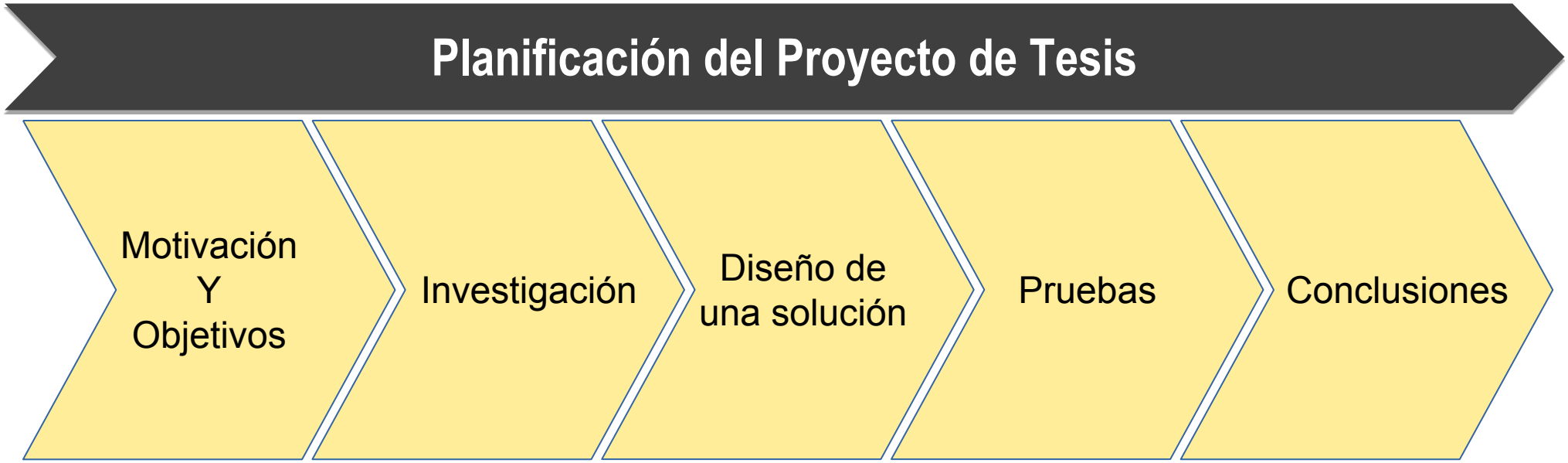
Tesina de Licenciatura en Sistemas

Uso de smartphones para auditar la seguridad de redes inalámbricas

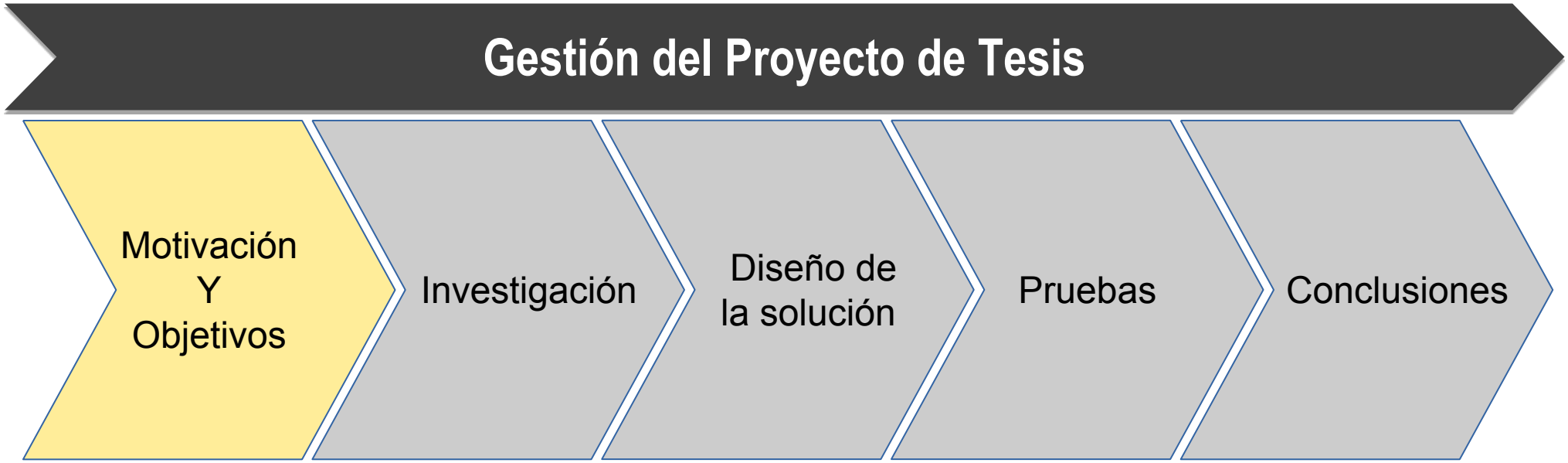
Autores: Bernal, Juan Ignacio – Zurita, Alejandro Enrique

Director: Lic. Venosa, Paula
Co-Director: Lic. Lanfranco, Einar

Planificación



Motivación y Objetivos



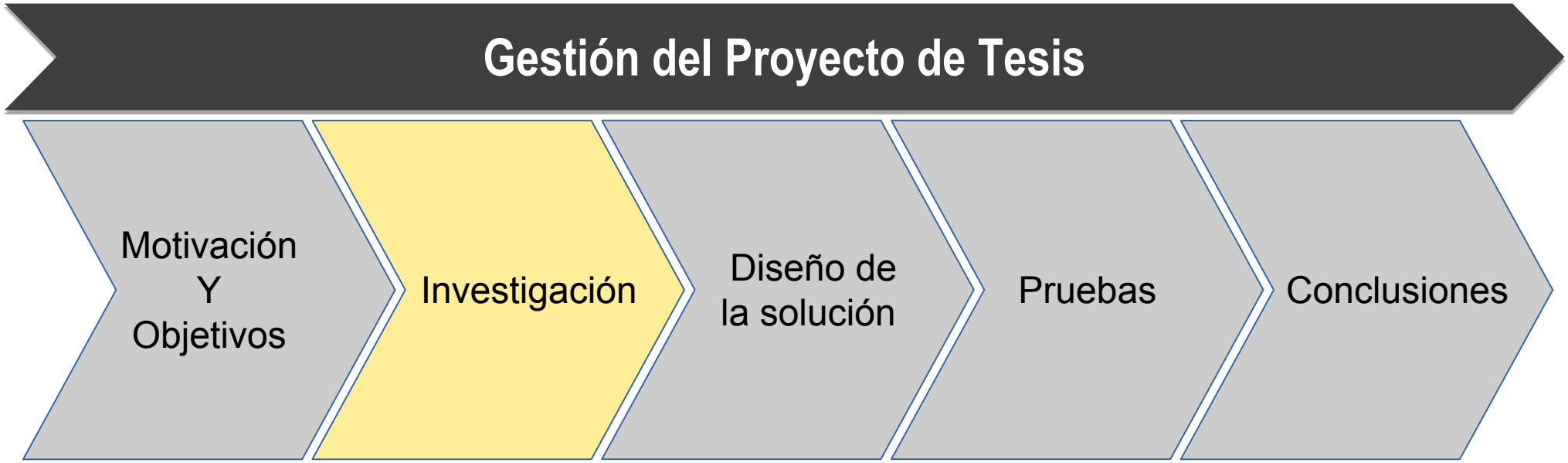
Motivación y Objetivos

- **Motivación**:
  - ¿por qué no utilizar los smartphones para realizar tareas de auditoría de redes inalámbricas?

- **Consultas con profesionales del área:**
  - Feedback: No se utilizan por ser poco útiles y prácticas.
  - Necesidades reales: Practicidad, facilidad y movilidad.

- **Objetivo Principal:**
  - Desarrollar una aplicación, que permita efectuar la correspondiente etapa de relevamiento de un Pentest de redes inalámbricas desde un dispositivo móvil, con la finalidad de que sea más fácil y práctico realizar las tareas que requieren de movilidad durante la etapa mencionada, en espacios físicos.

Investigación



Investigación

- **Criterios de selección:**
  - **Comunidad de usuarios:** aplicaciones más renombradas
  - **Período de tiempo:** Creadas desde el lanzamiento del Iphone (Junio del 2007) hasta la actualidad
  - **Cualidades:**
    - Preferentemente de uso y código libre
    - Capaz de habilitar el modo monitor
    - Capaz de realizar alguna de las tareas correspondientes a la etapa de relevamiento.

- **Resultado de la Selección:**
  - Kismet para Nokia N900 (noviembre del 2009)
  - BcMon (septiembre del 2012)
  - Android PCAP (diciembre del 2012)
  - PwnAir Pro (mayo del 2014)
  - Android Open Pwn Project (AOPP) (Junio del 2016)

Investigación

- **Criterios de evaluación:**
  - **Historia:** conocer el orígen y contexto de cada aplicación.
  - **Análisis técnico/funcional:** descubrir las dificultades que posee cada aplicación para obtener el modo monitor y hacer uso de sus funcionalidades.

- **Problemáticas encontradas:**
  - **Rooteo y cambio de firmware/ROM para obtener el modo monitor**
  - **Consumo de la placa inalámbrica y la duración de la batería**
  - **Suite de herramientas y su interfaz de consola**

Investigación

- **Problemáticas encontradas:**
  - **Rooteo y cambio de firmware/ROM para obtener el modo monitor**
    - Cantidad limitada de dispositivos disponibles
    - Se requiere conocimiento avanzado y bastante tiempo para poder hacerlo.
      - Convertir el dispositivo en un ladrillo
      - Inestabilidad del sistema y conflictos con otras app
      - Pérdida de datos personales
      - Pérdida de actualizaciones oficiales
      - Pérdida de garantía del dispositivo
    - Disminución de la seguridad del dispositivo por usar app de terceros

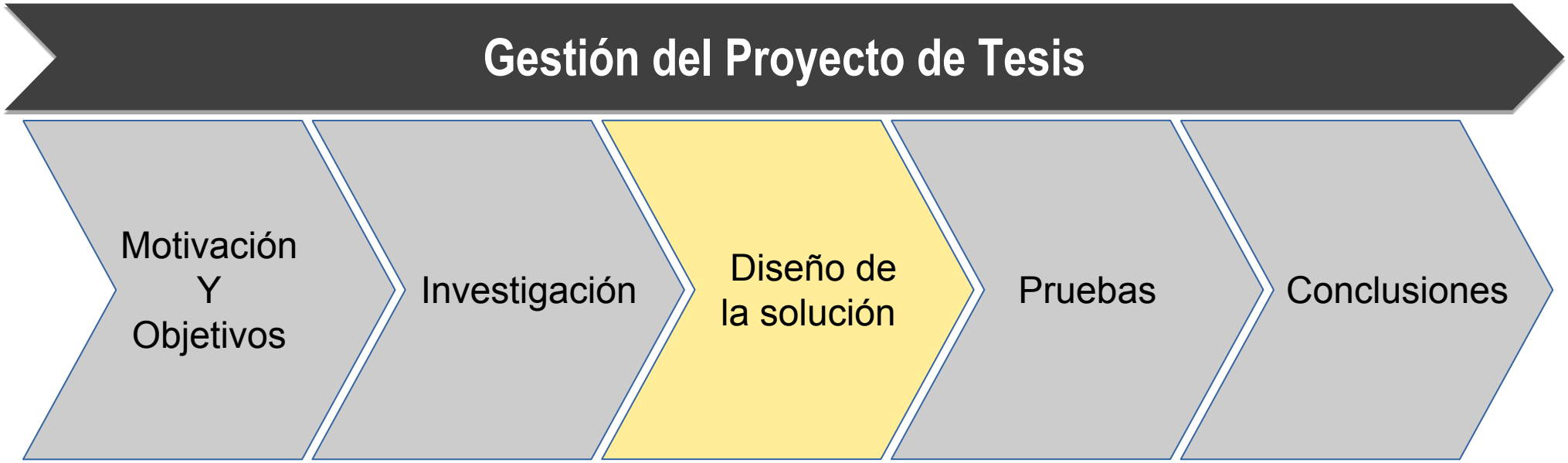
Investigación

- **Problemáticas encontradas:**
  - **Consumo de la placa inalámbrica y la duración de la batería**
    - **Placas internas:**
      - Se inhabilita el uso normal de la misma
      - Se provoca un mal funcionamiento del gestor de energía.
    - **Placas externas:**
      - Alto consumo eléctrico
      - El puerto USB no es capaz de entregar la corriente necesaria
    - Ambas **acortan notablemente la duración de la batería.**
    - **Las baterías no han evolucionado tanto** como el resto de los componentes electrónicos.

Investigación

- **Problemáticas encontradas:**
  - **Suite de herramientas y su interfaz de consola**
    - Se priorizó portar la mayor cantidad de aplicaciones ya existentes, resignando aspectos de usabilidad y eficiencia.
      - **Interfaz de consola** poco práctica para utilizarla desde un dispositivo móvil.
      - Las aplicaciones de PC portadas normalmente **no son diseñadas pensando en la eficiencia de recursos de hardware**.

Diseño de la solución



Diseño de la solución

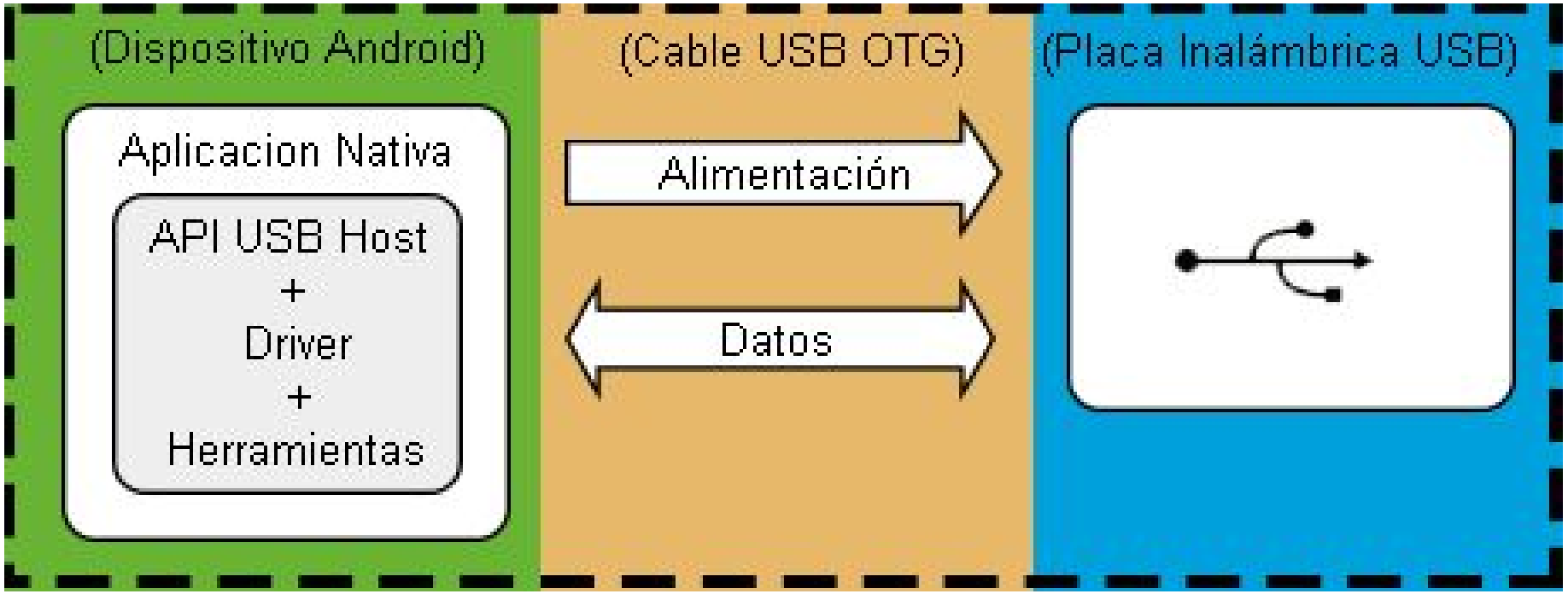
- **Soluciones a las Problemáticas encontradas:**
  - **Rooteo y cambio de firmware/ROM para obtener el modo monitor**
    - Combinar la API USB host de Android + placa inalámbrica USB externa + un driver para Linux portado a Java = **aplicación corre íntegramente en espacio de usuario**, sin permisos especiales o necesidad de alterar el kernel original.
  - **Consumo de la placa inalámbrica y la duración de la batería**
    - Placas inalámbricas externas de bajo consumo + chipset popular entre los fabricantes = ahorro de energía + un mayor número de dispositivos comerciales compatibles.

Diseño de la solución

- **Soluciones a las Problemáticas encontradas:**
  - **Suite de herramientas y su interfaz de consola**
    - Solo funcionalidades que permiten realizar las tareas involucradas en la etapa de relevamiento del Pentest de redes inalámbricas + uso adecuado de recursos de hardware + interfaz gráfica que facilite su uso.

Diseño de la solución

- **Integrando las soluciones -> Arquitectura del Sistema**

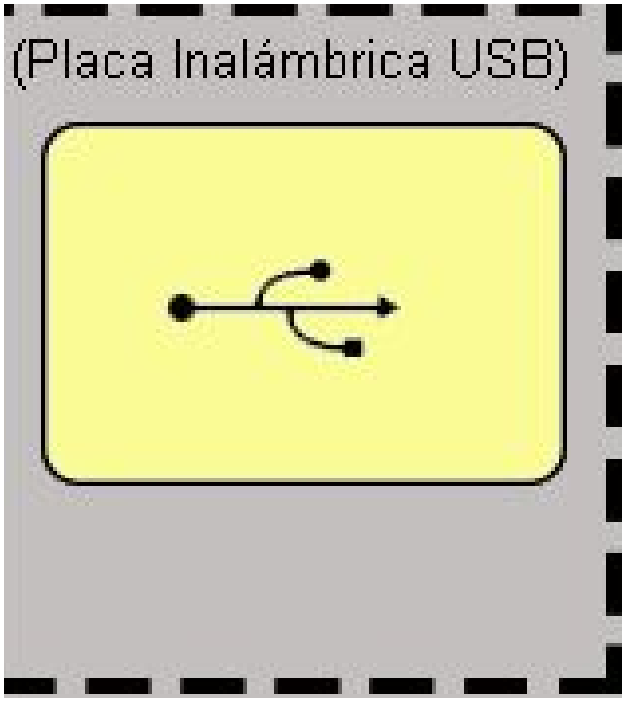


Diseño de la solución

- **Componentes de la Arquitectura**

Placa de red inalámbrica:

- Características deseadas:
  - Bajo Consumo
  - Tamaño Reducido
  - Driver libre
  - Bajo costo
- Resultado Selección:
  - Chipsets Realtek RTL8192CU/RTL8188CUS
  - Precio: entre $100 y $200



Diseño de la solución

- **Componentes de la Arquitectura**

Aplicación Pentest Security App

- Aplicación Android nativa -> Java
- Combina la API USB Host + driver Java + funcionalidades
- Compatible con Android >= 4.0
  - Abarca el 98% de los utilizados en la actualidad
- Licencia GPL versión 3,
- Repositorio:
  - Gitlab.com/zube/pentestsecurityapp

Diseño de la solución

- **Componentes de la Arquitectura**

Android API USB Host

- Permite a la aplicación comunicarse con la placa USB.

Driver Java

- Características: Libre + Java + modo monitor
- Desarrollado por Milen Rangelov
- Modificaciones: se amplió la cantidad de placas compatibles de 4 a 60.
  - Gitlab.com/zube/Rtl8192CardJavaDriver

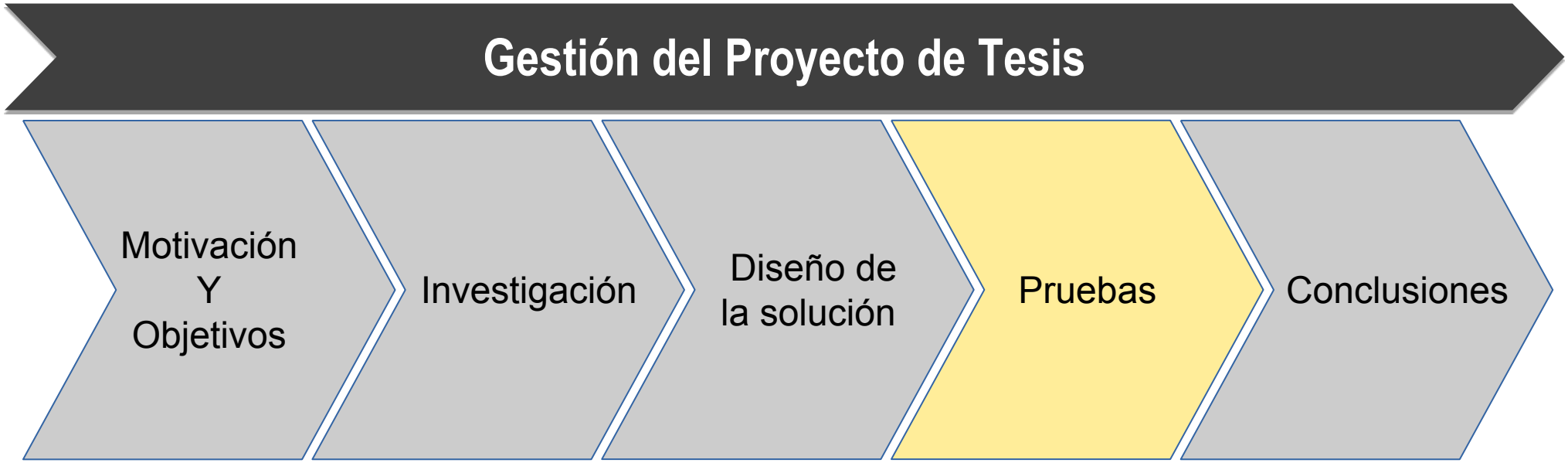
Diseño de la solución

- **Componentes de la Arquitectura**

Suite de Herramientas

- **Sin acceso a la red:**
  - APs de tipo Rogue
  - Tipo de encriptación apropiado para el tipo de red.
  - Balance de carga de los Ap
- **Con acceso a la red:**
  - Deducir qué servicios operan en cada host
- **Exportación de resultados:**
  - Informe
  - Pcap con el tráfico capturado
  - Enviar al servidor el pcap para su posterior análisis

Pruebas


Gestión del Proyecto de Tesis
Motivación Y Objetivos
Investigación
Diseño de la solución
Pruebas
Conclusiones

Pruebas

- **Entorno de Prueba:**
  - **Componentes de Hardware:**
    - **SmartPhone**
      - Motorola G1 XT1032
    - **Cable USB OTG**
    - **Placa de red**
      - TP-LINK Modelo TL-WN725N
    - **Access Point**
      - TP-LINK modelo TL-WR340G
  - **Componentes de Software**
    - **Root Checker**
    - **Pentest Security App**
    - **En una máquina virtual (servidor)**
      - **WebService**
      - **Wireshark**
      - **Aircrack-ng**

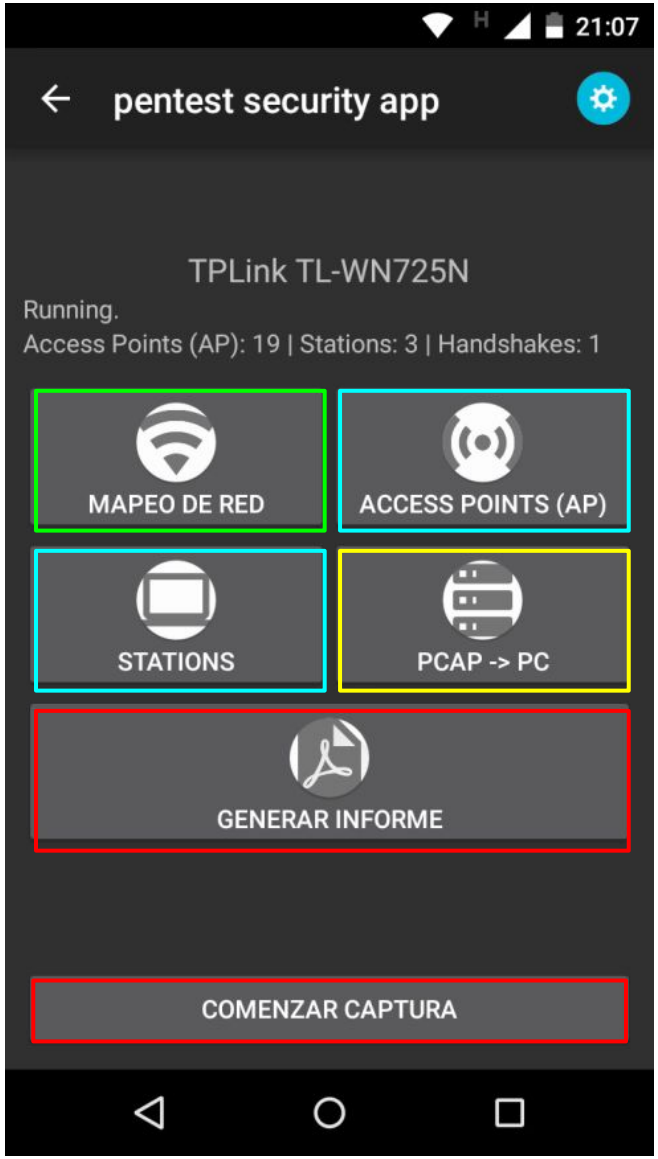
Pruebas

Secciones de la Aplicación			
Tareas de relevamiento cuando se tiene acceso a una red (Utiliza Placa inalámbrica **Interna**)	Tareas de relevamiento cuando **NO** se tiene acceso a una red (Utiliza Placa inalámbrica **Externa**)	Generación de informe y pcap	Exportartacion de resultados

Pruebas

Relevamiento de IP y Puertos de la red a la que se esté conectado

Relevamiento de Stations + Ataques de desautenticación.



Relevamiento de Ap

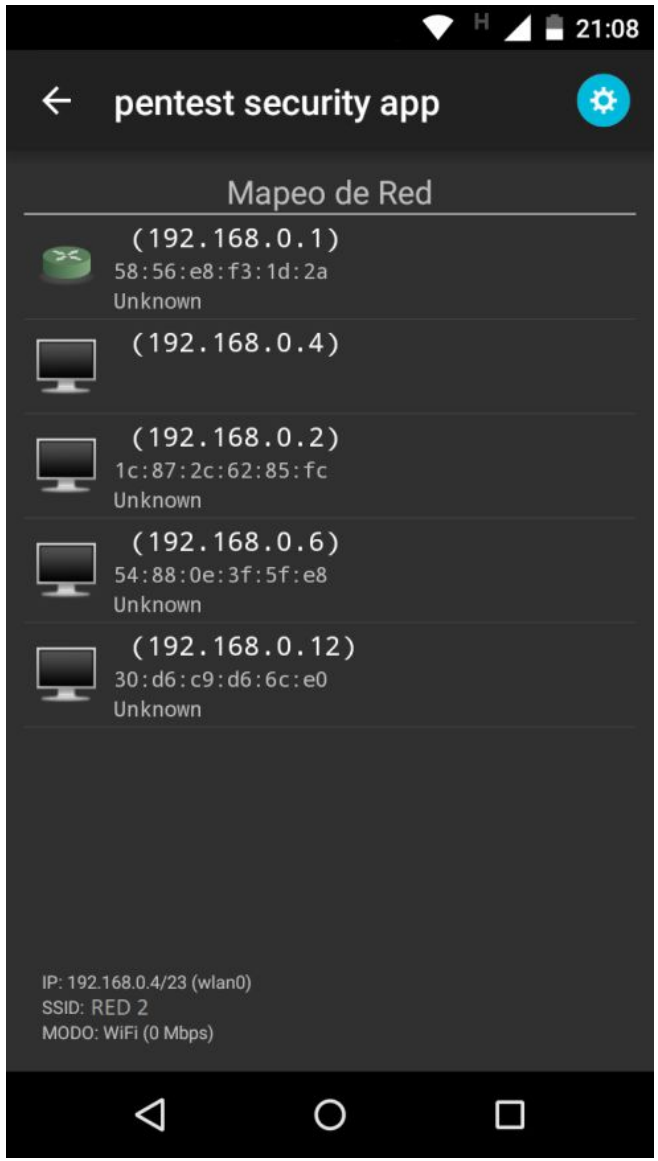
Envío de archivos de informe y pcap a servidor

Genera informe con la información de relevamiento obtenida

Captura el tráfico (en modo monitor) de todas las redes inalámbricas y lo almacena en un archivo pcap.


Planificación del Proyecto

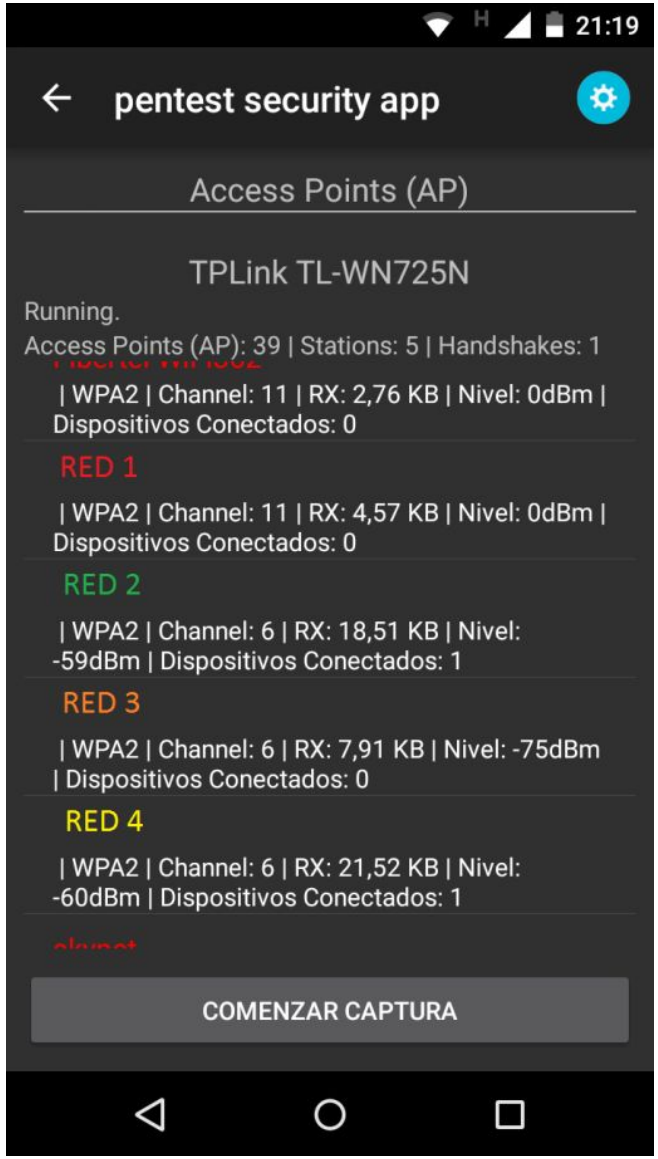
Pruebas

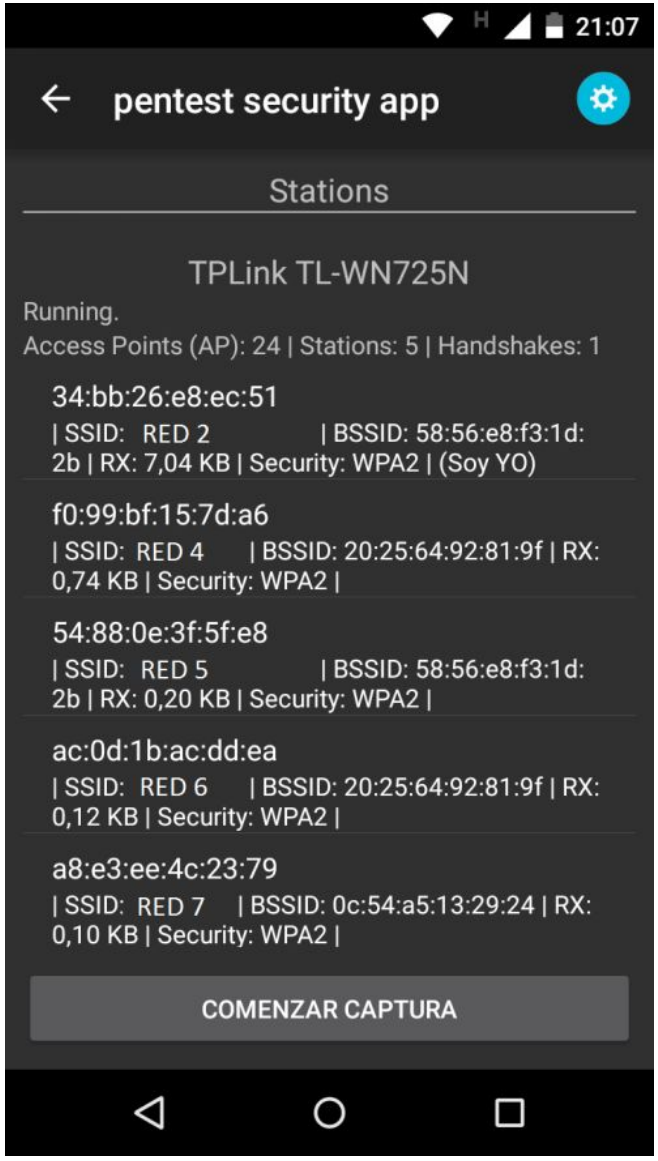

21:08
pentest security app
Mapeo de Red
(192.168.0.1)
58:56:e8:f3:1d:2a
Unknown
(192.168.0.4)
(192.168.0.2)
1c:87:2c:62:85:fc
Unknown
(192.168.0.6)
54:88:0e:3f:5f:e8
Unknown
(192.168.0.12)
30:d6:c9:d6:6c:e0
Unknown
IP: 192.168.0.4/23 (wlan0)
SSID: RED 2
MODO: WiFi (0 Mbps)

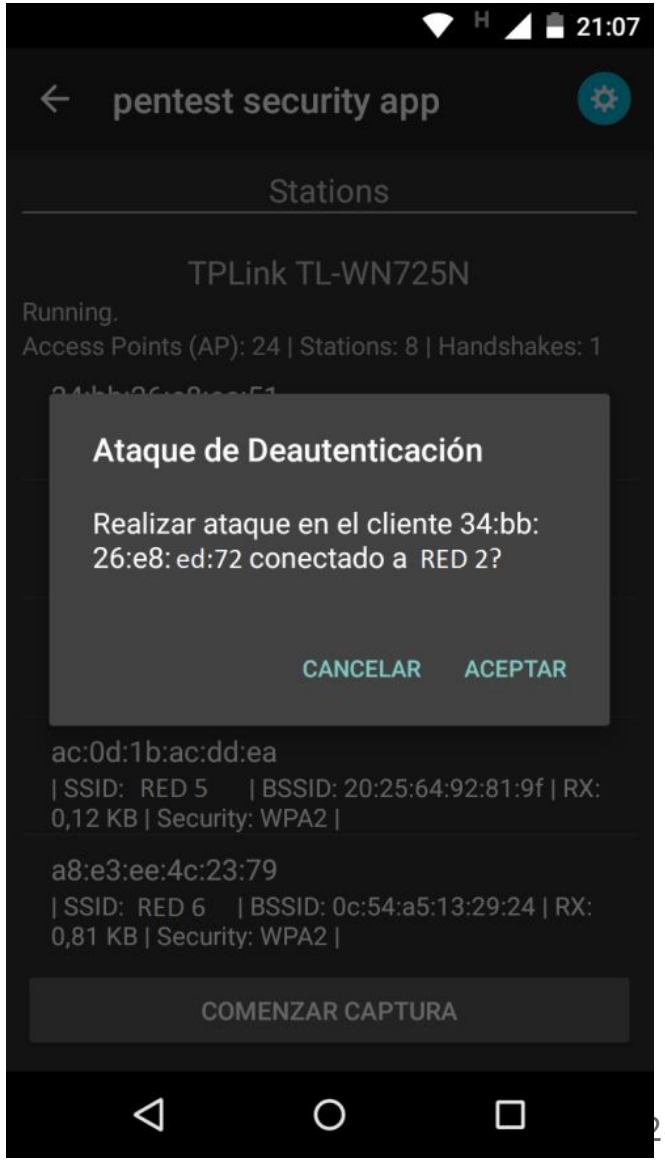

21:08
pentest security app
Puerto Origen 1
Puerto Destino 1024
Puertos mas conocidos
FTP
SSH
Telnet
SMTP
DNS
HTTP
POP3
HTTPS
Tipo de Protocolo
TCP
UDP
BUSCAR


16:57
pentest security app
Puertos Abiertos
135/tcp
tcp
139/tcp
tcp

Pruebas


21:19
pentest security app
Access Points (AP)
TPLink TL-WN725N
Running.
Access Points (AP): 39 | Stations: 5 | Handshakes: 1
| WPA2 | Channel: 11 | RX: 2,76 KB | Nivel: 0dBm | Dispositivos Conectados: 0
RED 1
| WPA2 | Channel: 11 | RX: 4,57 KB | Nivel: 0dBm | Dispositivos Conectados: 0
RED 2
| WPA2 | Channel: 6 | RX: 18,51 KB | Nivel: -59dBm | Dispositivos Conectados: 1
RED 3
| WPA2 | Channel: 6 | RX: 7,91 KB | Nivel: -75dBm | Dispositivos Conectados: 0
RED 4
| WPA2 | Channel: 6 | RX: 21,52 KB | Nivel: -60dBm | Dispositivos Conectados: 1
COMENZAR CAPTURA


21:07
pentest security app
Stations
TPLink TL-WN725N
Running.
Access Points (AP): 24 | Stations: 5 | Handshakes: 1
34:bb:26:e8:ec:51
| SSID: RED 2 | BSSID: 58:56:e8:f3:1d:2b | RX: 7,04 KB | Security: WPA2 | (Soy YO)
f0:99:bf:15:7d:a6
| SSID: RED 4 | BSSID: 20:25:64:92:81:9f | RX: 0,74 KB | Security: WPA2 |
54:88:0e:3f:5f:e8
| SSID: RED 5 | BSSID: 58:56:e8:f3:1d:2b | RX: 0,20 KB | Security: WPA2 |
ac:0d:1b:ac:dd:ea
| SSID: RED 6 | BSSID: 20:25:64:92:81:9f | RX: 0,12 KB | Security: WPA2 |
a8:e3:ee:4c:23:79
| SSID: RED 7 | BSSID: 0c:54:a5:13:29:24 | RX: 0,10 KB | Security: WPA2 |
COMENZAR CAPTURA


21:07
pentest security app
Stations
TPLink TL-WN725N
Running.
Access Points (AP): 24 | Stations: 8 | Handshakes: 1
Ataque de Deautenticación
Realizar ataque en el cliente 34:bb:26:e8:ed:72 conectado a RED 2?
CANCELAR
ACEPTAR
ac:0d:1b:ac:dd:ea
| SSID: RED 5 | BSSID: 20:25:64:92:81:9f | RX: 0,12 KB | Security: WPA2 |
a8:e3:ee:4c:23:79
| SSID: RED 6 | BSSID: 0c:54:a5:13:29:24 | RX: 0,81 KB | Security: WPA2 |
COMENZAR CAPTURA

Pruebas

pentest security app

Informe de Analisis Realizado

Fecha: 23-02-2017

Usuario:
Direccion:
Telefono:
Mail:

Mapeo de Red

Obteniendo dirección IP de "visitantes"

	IP	MAC	Puertos
	10.169.199.5	00:00:00:00:00:00	

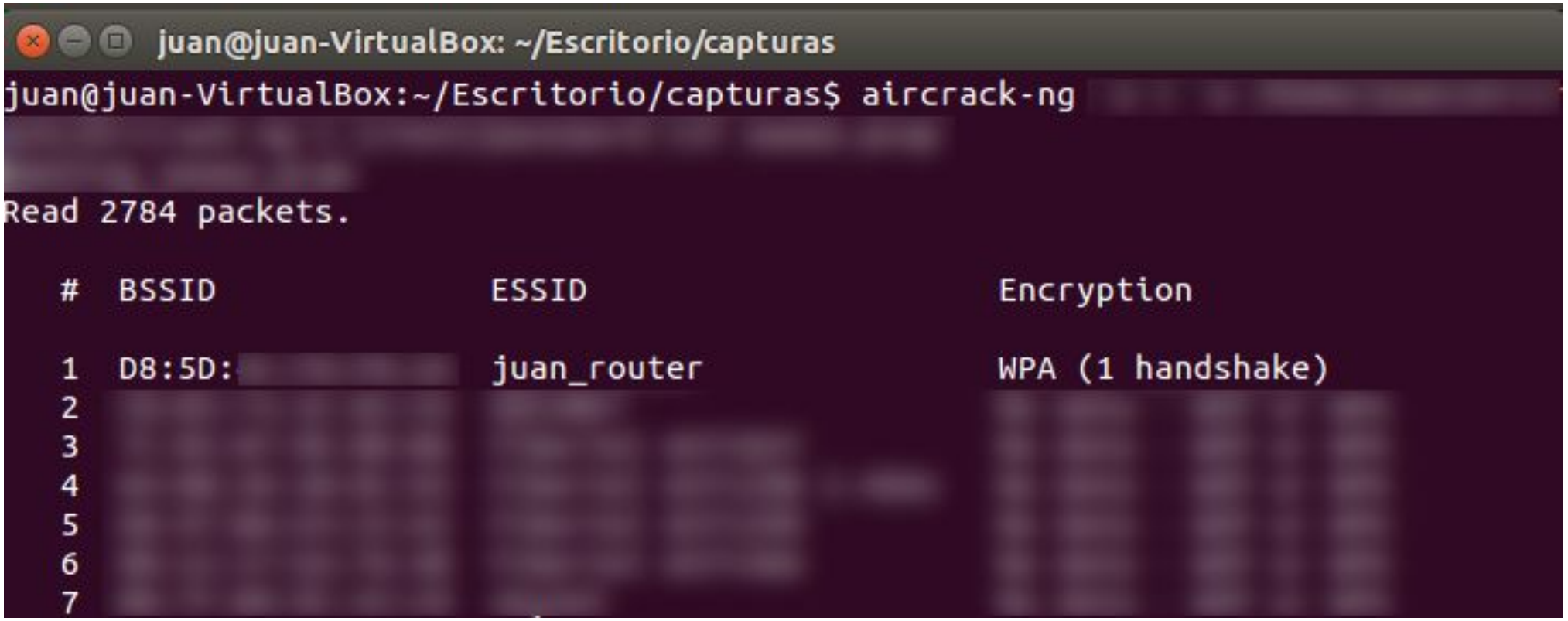
Access Points (AP)

SSID	Cifrado	Canal	RX	Nivel	Disp. Conectados
511-alumnos	WPA	1	0.93 KB	0dBm	0
	WEP	0	0.27 KB	-74dBm	0

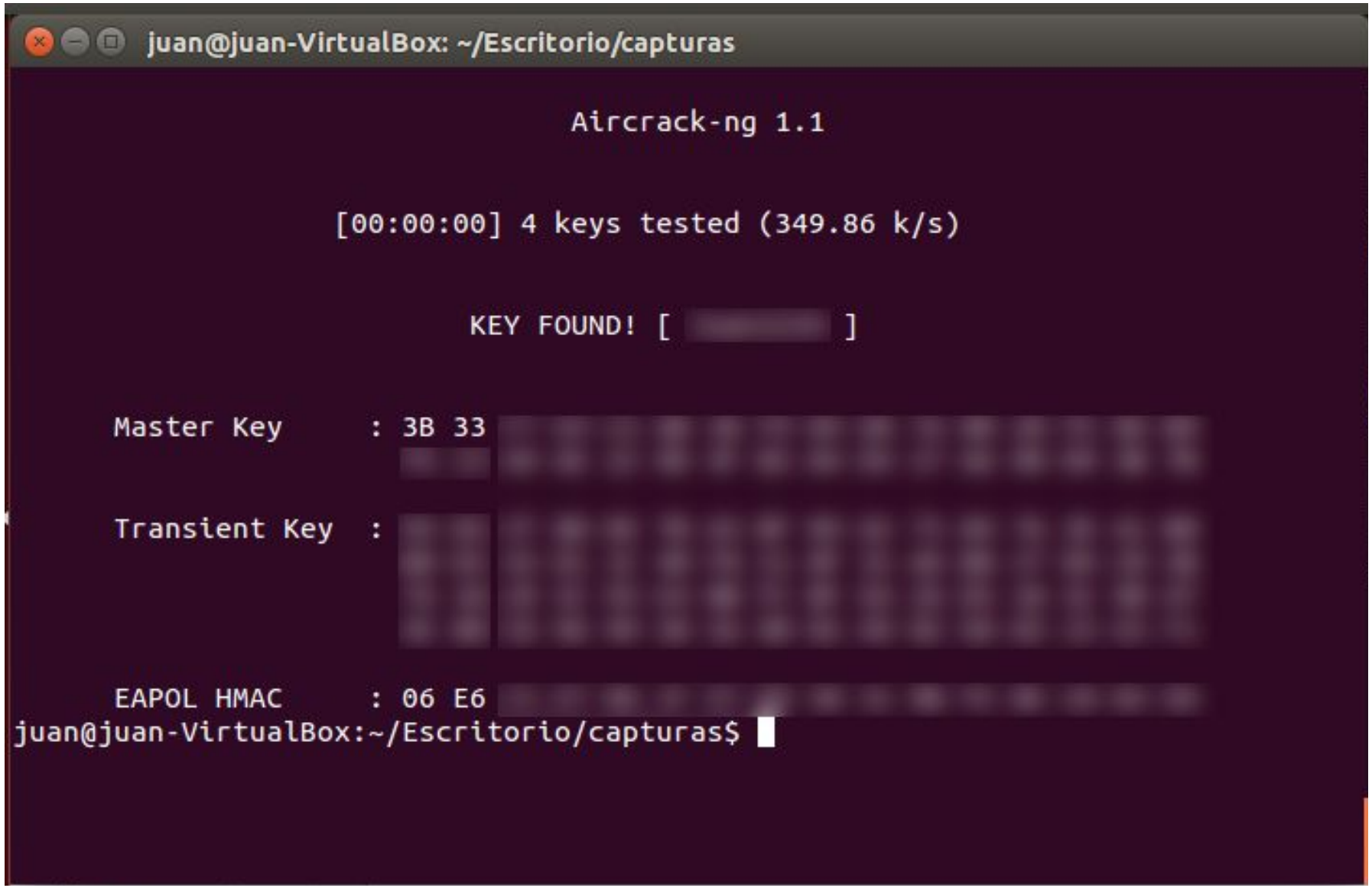
Pruebas

- **Caso de Prueba:**
  - **Objetivo:**
    - Verificar que la aplicación captura correctamente el tráfico de la red
  - **Propuesta:**
    - Capturar un handshake de autenticación de la red “juan_router” y analizarlo mediante la suite de herramientas Aircrack-ng.
  - **Resultado esperado**
    - Si Aircrack devuelve la clave configurada en el AP analizado, queda demostrado que la información recopilada por la aplicación Pentest Security App es válida.

Pruebas


juan@juan-VirtualBox: ~/Escritorio/capturas
juan@juan-VirtualBox:~/Escritorio/capturas$ aircrack-ng
Read 2784 packets.
BSSID ESSID Encryption
1 D8:5D: juan_router WPA (1 handshake)
2
3
4
5
6
7

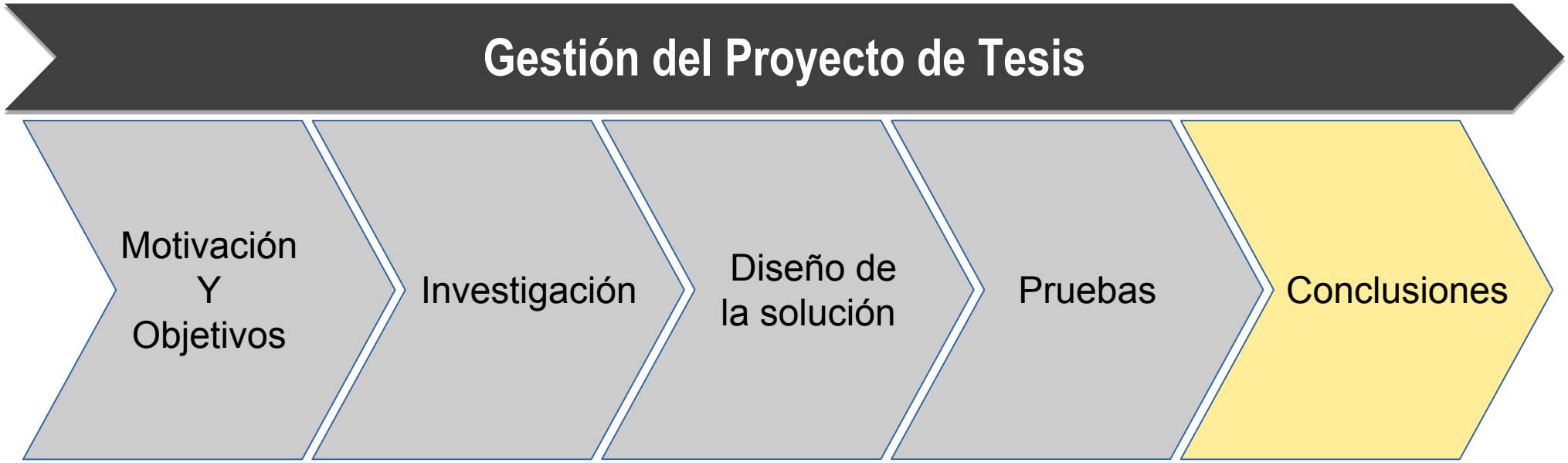
Pruebas


juan@juan-VirtualBox: ~/Escritorio/capturas
Aircrack-ng 1.1
[00:00:00] 4 keys tested (349.86 k/s)
KEY FOUND! [ ]
Master Key : 3B 33
Transient Key :
EAPOL HMAC : 06 E6
juan@juan-VirtualBox:~/Escritorio/capturas$

Pruebas

- **Resultados obtenidos en otras pruebas anteriores:**
  - **Relevamiento de AP de Fibertel**
    - **Dos conclusiones:**
      - **La mayoría de las contraseñas numéricas**
        - **10 dígitos**
        - **Podría requerir 1 semana aprox. para obtener la clave**
      - **Queda justificado el porqué no se incorpora esta funcionalidad a la app móvil.**

Pruebas


Gestión del Proyecto de Tesis
Motivación Y Objetivos
Investigación
Diseño de la solución
Pruebas
Conclusiones

Conclusiones

- **Conclusiones**
  - **La aplicación desarrollada alcanza los objetivos planteados al inicio de la tesina representando una solución superadora respecto de las aplicaciones preexistentes:**
    - **Facilita y hace más seguro el proceso de instalación al prescindir del acceso root y la modificación del firmware del dispositivo.**
    - **Es compatible con el 98% de los smartphones que usan Android.**
    - **Hace un uso más responsable de la batería, combinando un chipset inalámbrico de bajo consumo eléctrico y aplicaciones de bajo procesamiento.**
    - **Mejora la usabilidad al incorporar una interfaz nativa de Android y la portabilidad al utilizar placas inalámbricas de dimensiones reducidas.**
    - **Tiene un bajo costo de implementación**

Conclusiones

- **Trabajo Futuro**
  - **Incorporar la posición geográfica de los AP, reflejando los resultados en un plano edilicio del lugar auditado.**
  - **Incorporar nuevos drivers**
  - **Desarrollar web services que brinden funcionalidad para llevar a cabo el resto de las etapas de un pentest de redes inalámbricas.**
  - **Incorporar otros formatos de presentación de la información obtenida.**
  - **Escaneo por Netbios para mejorar la identificación de los dispositivos encontrados**

Muchas Gracias