Universidad de Granada

Mecanismos de protección de datos en videojuegos

Alumno:
Benito Palacios Sánchez

Tutor:
Dr. D. Pedro García Teodoro
Dpto. Teoría de la Señal, Telemática y Comunicaciones

15 de julio de 2015

Objetivo

Analizar, estudiar y documentar algoritmos de protección de datos implementados en videojuegos.

Índice de contenidos

Índice de contenidos

Motivación

- Los videojuegos son una clave de nuestra cultura actual.
- Su industria es la segunda con más ganancias.
- Preocupación por protección anti-copias, derechos de autor, trampas.

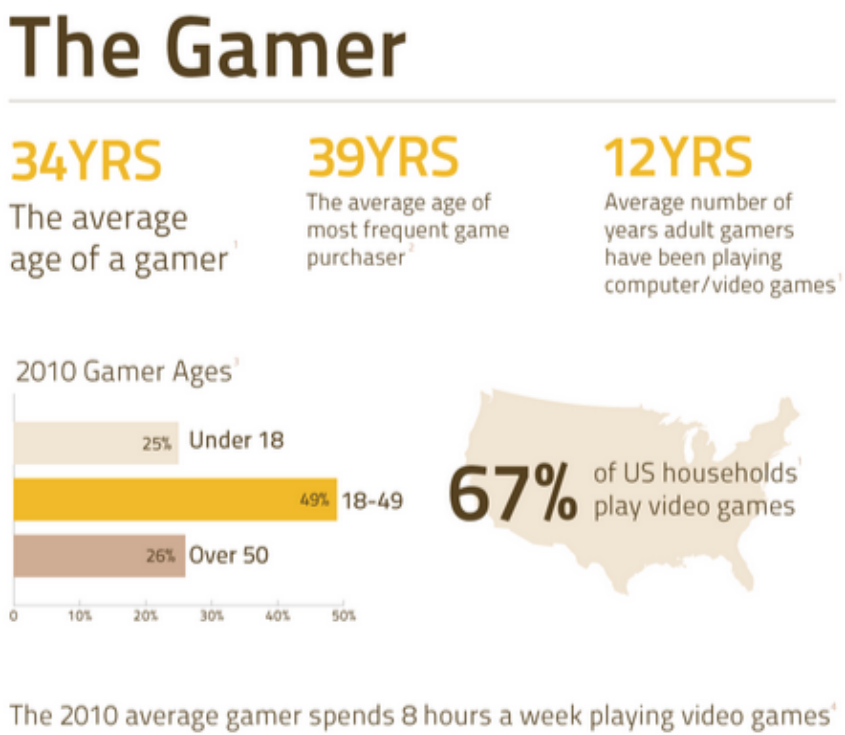


Figura: Estadísticas sobre jugadores en EE. UU. Fuente: `http://www.esrb.org` (2010).

Motivación

- Los videojuegos son una clave de nuestra cultura actual.
- Su industria es la segunda con más ganancias.
- Preocupación por protección anti-copias, derechos de autor, trampas.

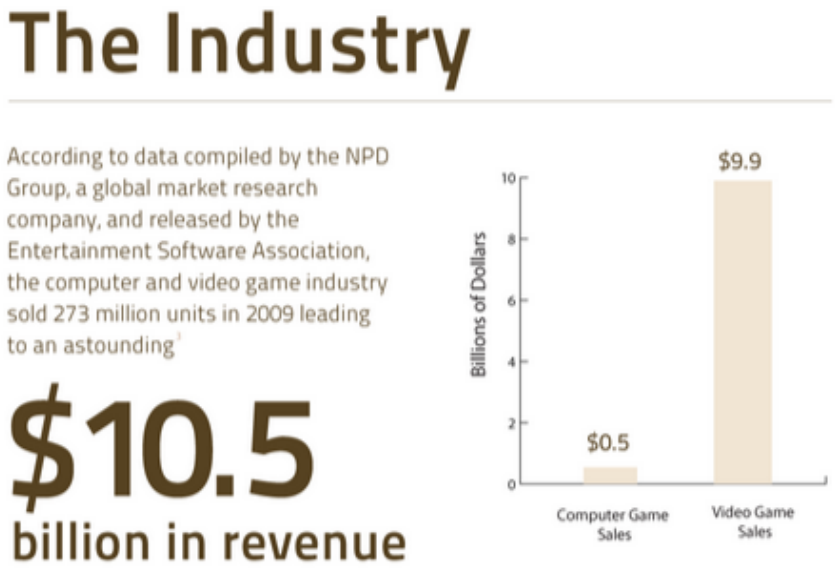


Figura: Estadísticas sobre la industria de videojuegos en EE. UU.
Fuente: `http://www.esrb.org` (2009).

Motivación

- Los videojuegos son una clave de nuestra cultura actual.
- Su industria es la segunda con más ganancias.
- Preocupación por protección anti-copias, derechos de autor, trampas.

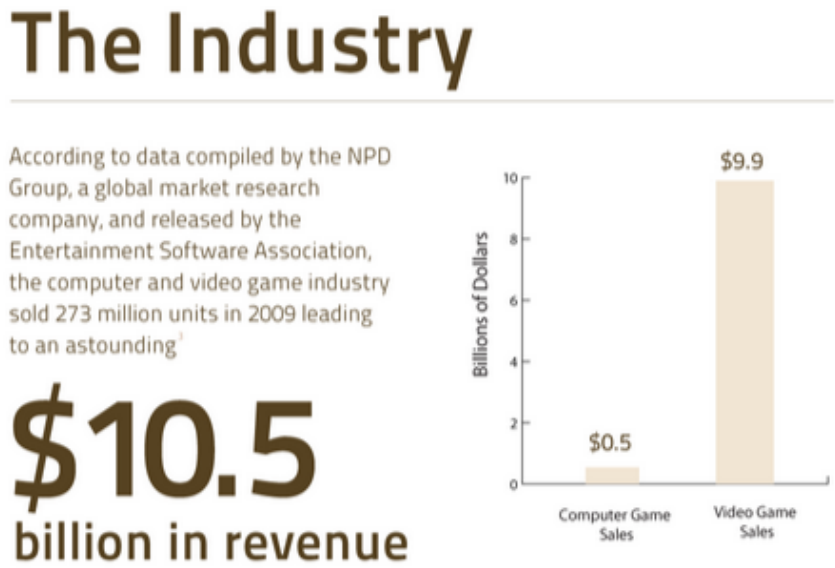


Figura: Estadísticas sobre la industria de videojuegos en EE. UU. Fuente: `http://www.esrb.org` (2009).

ROM Hacking

Ingeniería inversa

La ingeniería inversa es el proceso de analizar un sistema para identificar sus componentes y relaciones y, crear una representación del sistema en otro formato o a un nivel más alto de abstracción.

ROM Hacking

Ingeniería inversa sobre videojuegos. El nombre viene realizar modificaciones (*hacks*) sobre juegos que suelen distribuirse en memorias de solo lectura (*Read Only Memory*).

ROM Hacking

Ingeniería inversa

La ingeniería inversa es el proceso de analizar un sistema para identificar sus componentes y relaciones y, crear una representación del sistema en otro formato o a un nivel más alto de abstracción.

ROM Hacking

Ingeniería inversa sobre videojuegos. El nombre viene realizar modificaciones (*hacks*) sobre juegos que suelen distribuirse en memorias de solo lectura (*Read Only Memory*).

Índice de contenidos

Traducciones no oficiales y Pokémon

- Franquicia de *The Pokémon Company* fundada en 1995. Juegos desarrollados por *Game Freak*.
- Segunda franquicia más exitosa a nivel mundial.
- Nº seguidores + retrasos en lanzamientos $\Rightarrow$ traducción no oficial.

Traducciones no oficiales y Pokémon

- Franquicia de *The Pokémon Company* fundada en 1995. Juegos desarrollados por *Game Freak*.
- Segunda franquicia más exitosa a nivel mundial.
- Nº seguidores + retrasos en lanzamientos ⇒ traducción no oficial.

ugr Universidad de Granada

Traducciones no oficiales y Pokémon

- Franquicia de *The Pokémon Company* fundada en 1995. Juegos desarrollados por *Game Freak*.
- Segunda franquicia más exitosa a nivel mundial.
- Nº seguidores + retrasos en lanzamientos ⇒ traducción no oficial.

Universidad de Granada

Traducciones no oficiales y Pokémon

- Franquicia de *The Pokémon Company* fundada en 1995. Juegos desarrollados por *Game Freak*.
- Segunda franquicia más exitosa a nivel mundial.
- Nº seguidores + retrasos en lanzamientos ⇒ traducción no oficial.

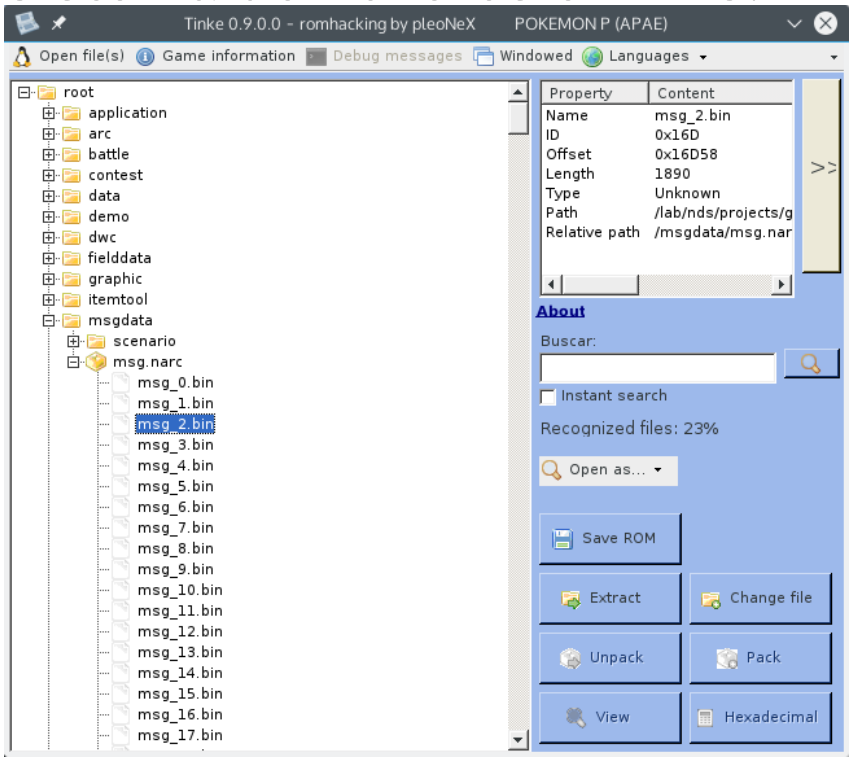
Ficheros en Nintendo DS

Sistema de ficheros en NDS.

Archivo binario con textos.

Ficheros en Nintendo DS

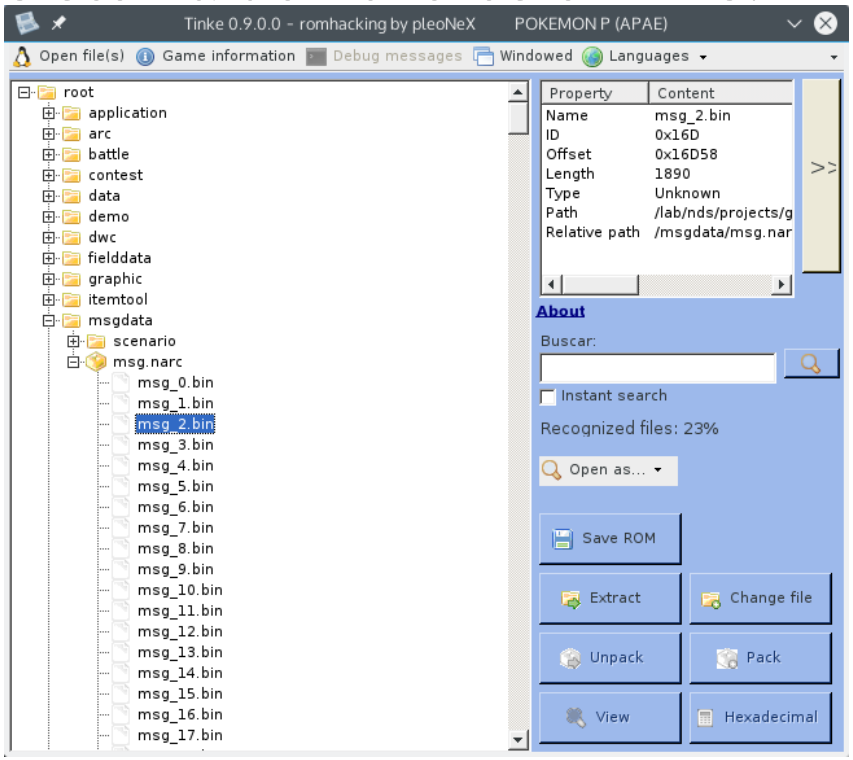
Sistema de ficheros en NDS.



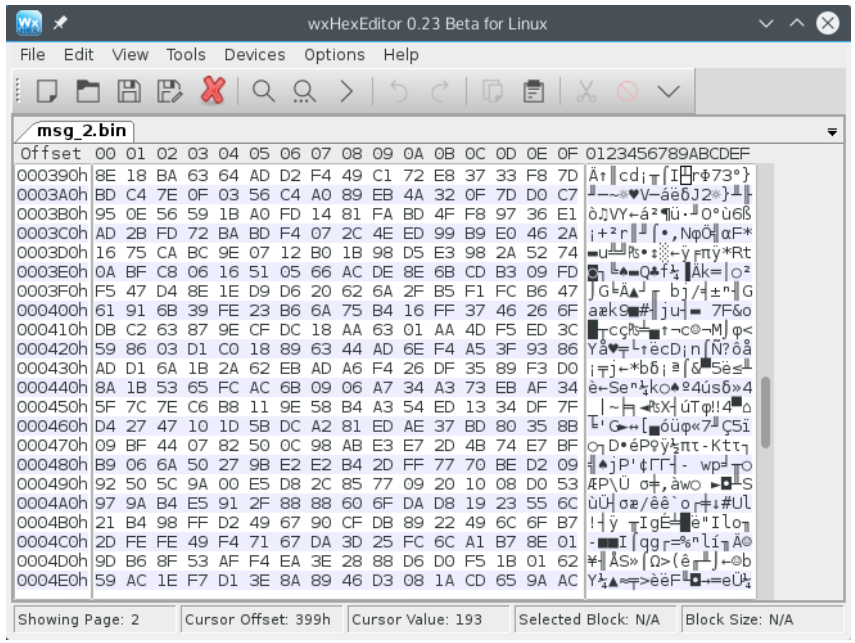
Archivo binario con textos.

Ficheros en Nintendo DS

Sistema de ficheros en NDS.



Archivo binario con textos.

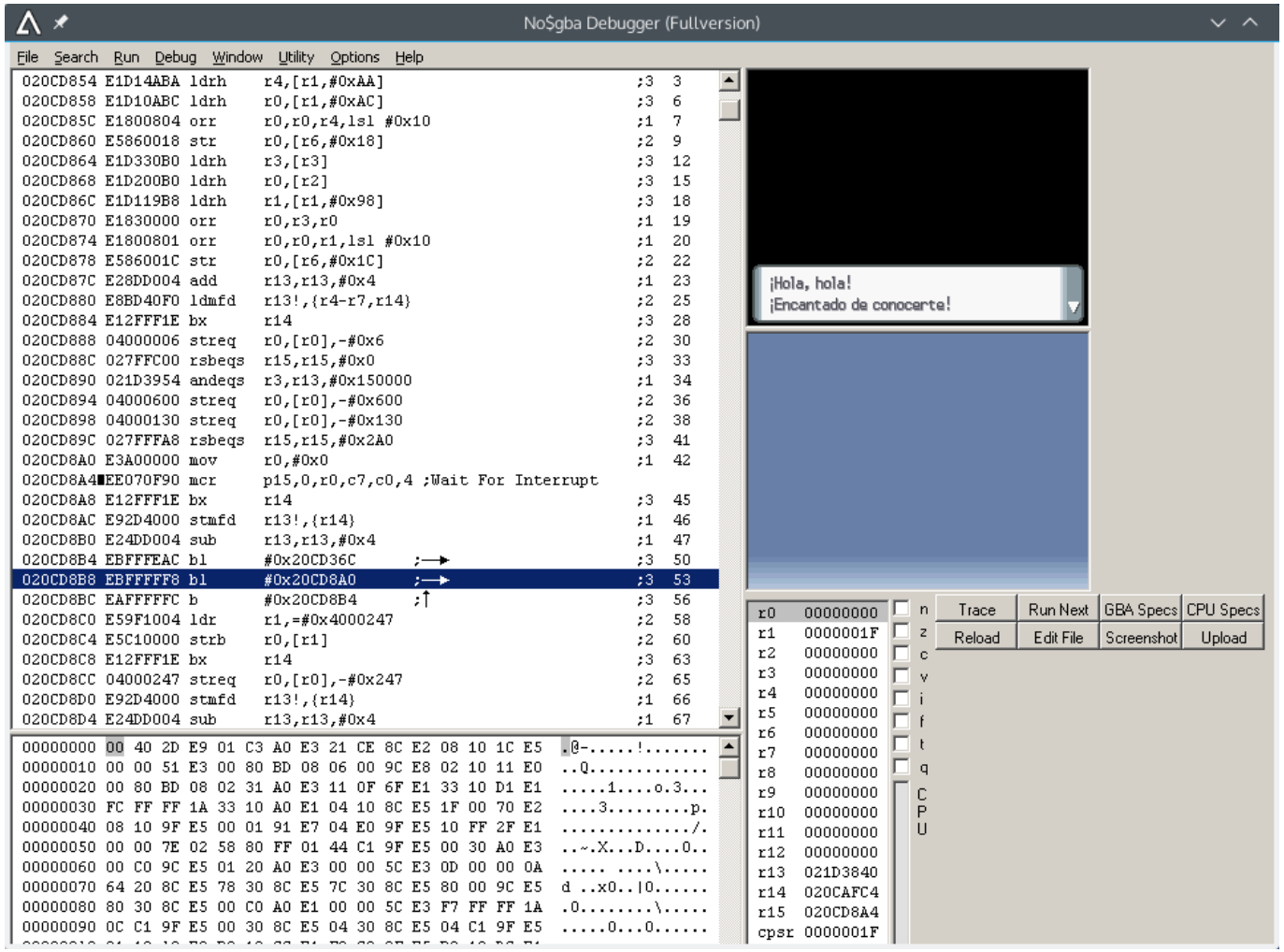


Depuración de juegos

Emulador No$gba para NDS.

Depuración de juegos

Emulador No$gba para NDS.

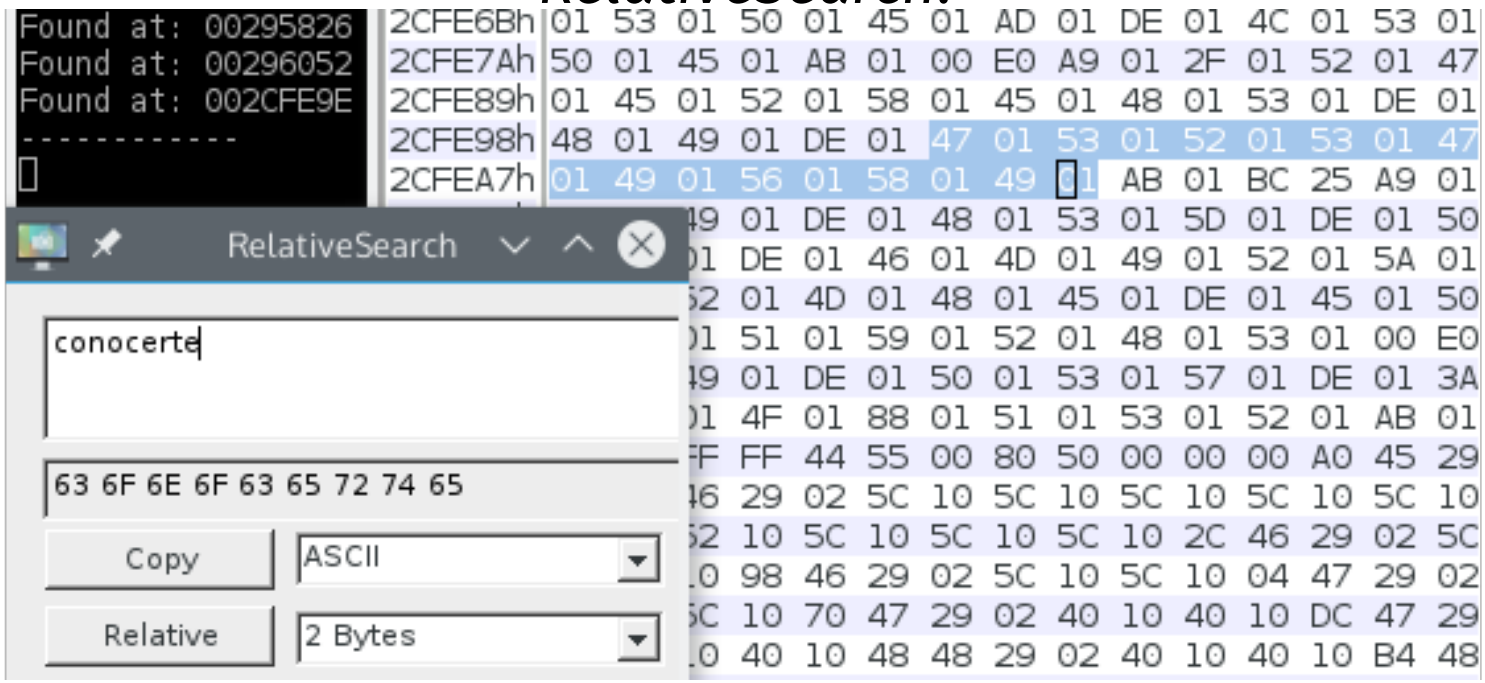


Búsqueda de textos con codificación no estándar

RelativeSearch.

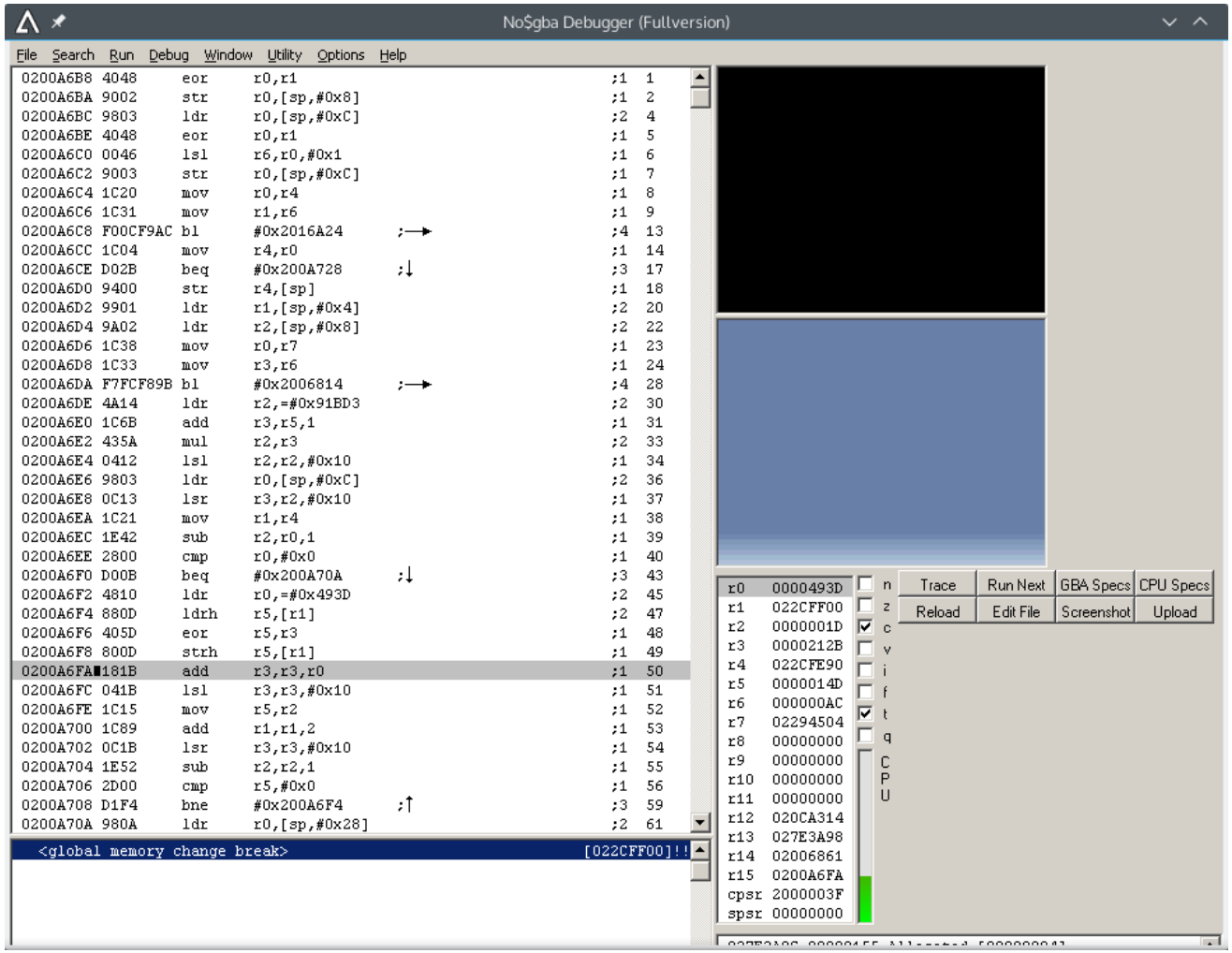
Búsqueda de textos con codificación no estándar

RelativeSearch.



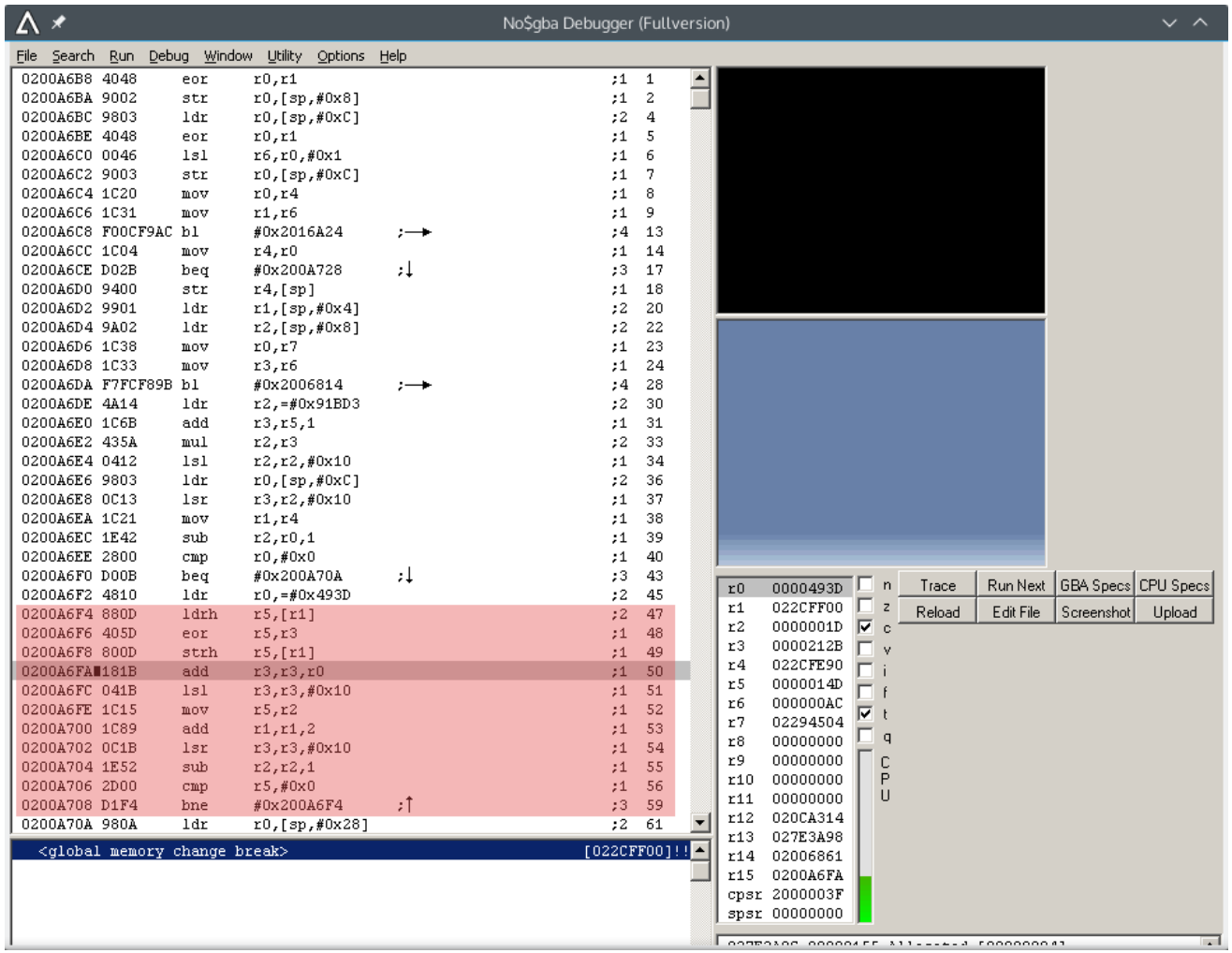
Puntos de interrupción en código

Punto de interrupción.



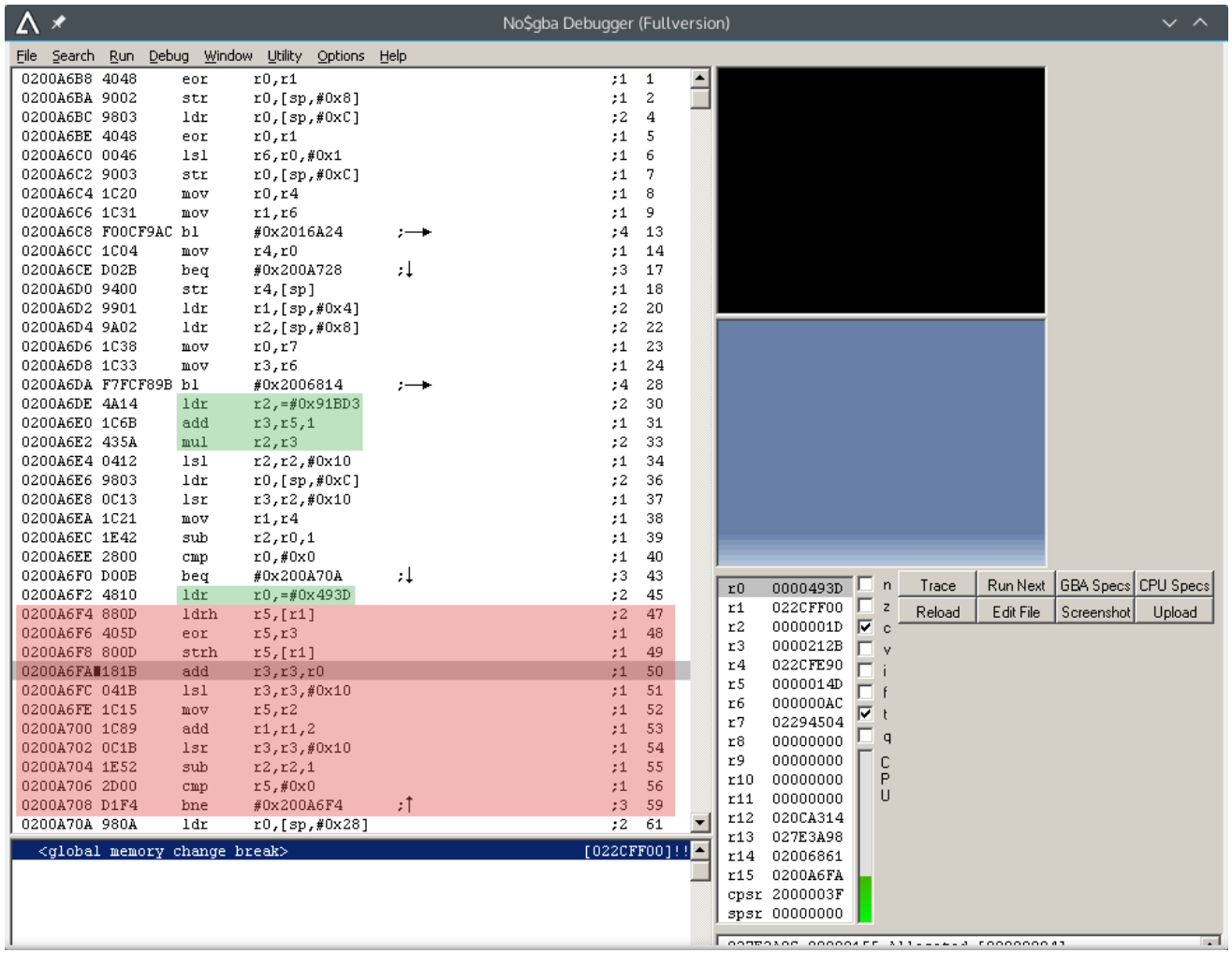
Puntos de interrupción en código

Bucle de descifrado.



Puntos de interrupción en código

Inicialización de clave.



Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  clave = (ushort)(clave + 0x493D);
}
```

Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];
for (int i=data.Length - 1; i>=0; i--){
  data[i] = data[i] ^ clave;
  clave = (uint)(clave * 0x41C64E6D + 0x6073);
}
```

Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  clave = (ushort)(clave + 0x493D);
}
```

Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];
for (int i=data.Length - 1; i>=0; i--){
  data[i] = data[i] ^ clave;
  clave = (uint)(clave * 0x41C64E6D + 0x6073);
}
```

Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  clave = (ushort)(clave + 0x493D);
}
```

Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];
for (int i=data.Length - 1; i>=0; i--){
  data[i] = data[i] ^ clave;
  clave = (uint)(clave * 0x41C64E6D + 0x6073);
}
```

Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  clave = (ushort)(clave + 0x493D);
}
```

Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];
for (int i=data.Length - 1; i>=0; i--){
  data[i] = data[i] ^ clave;
  clave = (uint)(clave * 0x41C64E6D + 0x6073);
}
```

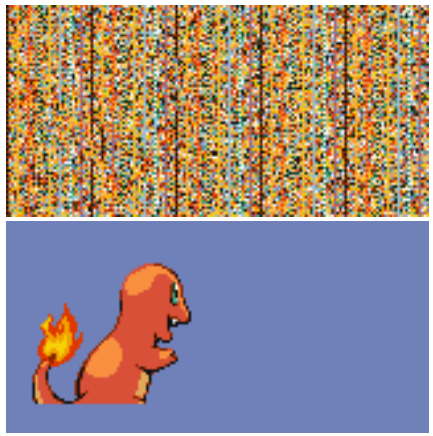
Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  clave = (ushort)(clave + 0x493D);
}
```

Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];
for (int i=data.Length - 1; i>=0; i--){
  data[i] = data[i] ^ clave;
  clave = (uint)(clave * 0x41C64E6D + 0x6073);
}
```



Archivos ofuscados en Pokémon Blanco y Negro

- Archivos ofuscados:
  - Sin nombre ni clasificación.
- Textos:
  - Codificación UTF-16.
  - Cifrado XOR, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  ushort temp = clave & 0x1FFF;
  clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
  - Cambio de formato.

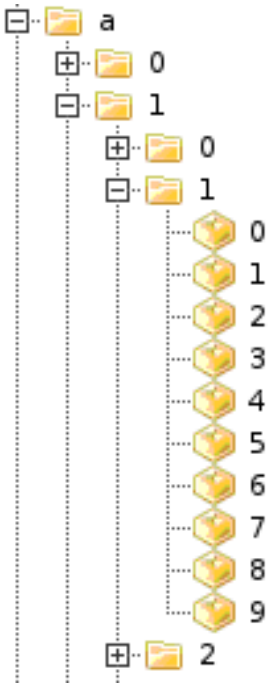
Archivos ofuscados en Pokémon Blanco y Negro

- Archivos ofuscados:
  - Sin nombre ni clasificación.
- Textos:
  - Codificación UTF-16.
  - Cifrado XOR, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  ushort temp = clave & 0x1FFF;
  clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
  - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro

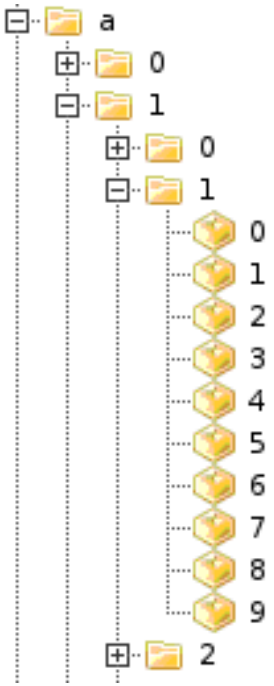


- Archivos ofuscados:
  - Sin nombre ni clasificación.
- Textos:
  - Codificación UTF-16.
  - Cifrado XOR, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  ushort temp = clave & 0x1FFF;
  clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
  - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro

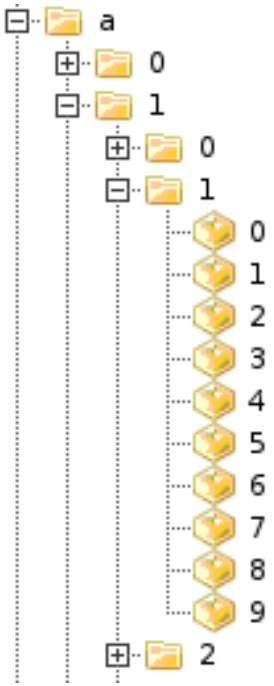


- Archivos ofuscados:
  - Sin nombre ni clasificación.
- Textos:
  - Codificación UTF-16.
  - Cifrado XOR, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  ushort temp = clave & 0x1FFF;
  clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
  - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro

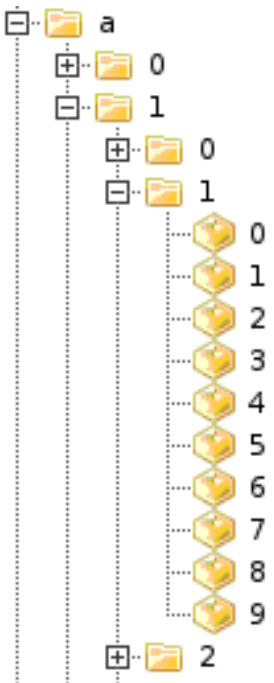


- Archivos ofuscados:
  - Sin nombre ni clasificación.
- Textos:
  - Codificación `UTF-16`.
  - Cifrado `XOR`, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  ushort temp = clave & 0x1FFF;
  clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
  - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro

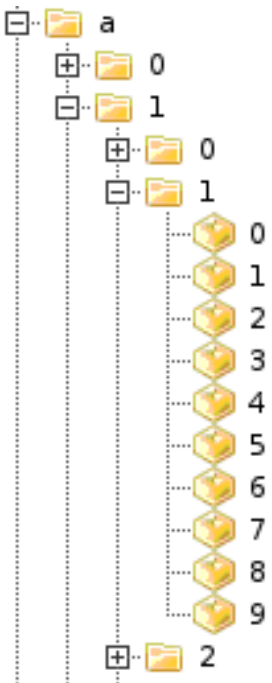


- Archivos ofuscados:
  - Sin nombre ni clasificación.
- Textos:
  - Codificación `UTF-16`.
  - Cifrado `XOR`, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  ushort temp = clave & 0x1FFF;
  clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
  - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro

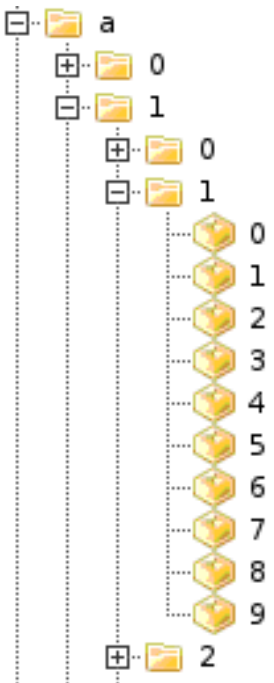


- Archivos ofuscados:
  - Sin nombre ni clasificación.
- Textos:
  - Codificación `UTF-16`.
  - Cifrado `XOR`, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  ushort temp = clave & 0x1FFF;
  clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
  - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro



- Archivos ofuscados:
  - Sin nombre ni clasificación.
- Textos:
  - Codificación `UTF-16`.
  - Cifrado `XOR`, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
  data[i] = data[i] ^ clave;
  ushort temp = clave & 0x1FFF;
  clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
  - Cambio de formato.

Mecanismos en otros juegos

Algoritmos de protección encontrados en otros juegos:

- *Pokémon HeartGold y SoulSilver*: Igual que *Pokémon Perla y Diamante*.
- *Pokémon Conquest*: Cifra y codifica textos. Imágenes con formatos no estándar.
- *Ninokuni - El Mago de las Tinieblas*: Cifra estadísticas de personajes y monstruos. Añade algoritmos de integridad en el archivo de guardado.

Mecanismos en otros juegos

Algoritmos de protección encontrados en otros juegos:

- *Pokémon HeartGold y SoulSilver*: Igual que *Pokémon Perla y Diamante*.
- *Pokémon Conquest*: Cifra y codifica textos. Imágenes con formatos no estándar.
- *Ninokuni - El Mago de las Tinieblas*: Cifra estadísticas de personajes y monstruos. Añade algoritmos de integridad en el archivo de guardado.

Mecanismos en otros juegos

Algoritmos de protección encontrados en otros juegos:

- *Pokémon HeartGold y SoulSilver*: Igual que *Pokémon Perla y Diamante*.
- *Pokémon Conquest*: Cifra y codifica textos. Imágenes con formatos no estándar.
- *Ninokuni - El Mago de las Tinieblas*: Cifra estadísticas de personajes y monstruos. Añade algoritmos de integridad en el archivo de guardado.

Índice de contenidos

Ninokuni: La ira de la Bruja Blanca

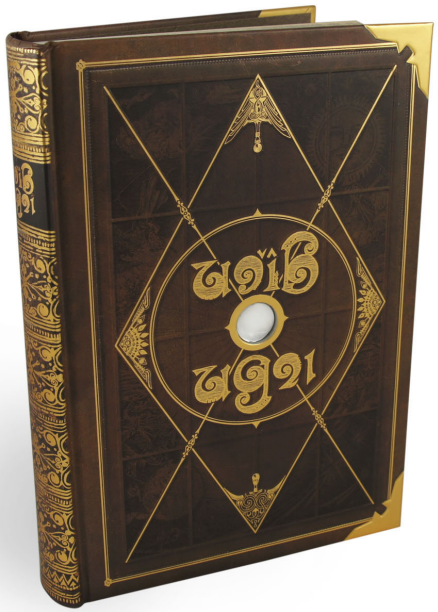
- Versión para PS3 con ligeros cambios. Llegó a América y Europa.
- Libro digitalizado en alta calidad.
- No hay algoritmos de protección, pero su formato no es estándar.
  - El resto de ficheros (texto, audio, etc) sí están cifrados.

Ninokuni: La ira de la Bruja Blanca

- Versión para PS3 con ligeros cambios. Llegó a América y Europa.
- Libro digitalizado en alta calidad.
- No hay algoritmos de protección, pero su formato no es estándar.
  - El resto de ficheros (texto, audio, etc) sí están cifrados.

Ninokuni: La ira de la Bruja Blanca

- Versión para PS3 con ligeros cambios. Llegó a América y Europa.
- Libro digitalizado en alta calidad.
- No hay algoritmos de protección, pero su formato no es estándar.
  - El resto de ficheros (texto, audio, etc) sí están cifrados.



Ninokuni: La ira de la Bruja Blanca

- Versión para PS3 con ligeros cambios. Llegó a América y Europa.
- Libro digitalizado en alta calidad.
- No hay algoritmos de protección, pero su formato no es estándar.
  - El resto de ficheros (texto, audio, etc) sí están cifrados.

Guitar Hero: On Tour

- Ficheros comprimidos con formato propietario. ✓
  - El algoritmo ocupa 1.900 instrucciones máquina. ✓
- No hay compresión en las siguientes ediciones. ✗
- Formato canciones: `Vorbis OGG`. ✗

Guitar Hero: On Tour

- Ficheros comprimidos con formato propietario. ✓
  - El algoritmo ocupa 1.900 instrucciones máquina. ✓
- No hay compresión en las siguientes ediciones. ✗
- Formato canciones: `Vorbis OGG`. ✗

```
LDR     R1, =aInvalidWindowS            ; "invalid window size"
MOV     R0, #0x1B
STR     R1, [R9,#0x18]
STR     R0, [R8]
```

Figura: Mensajes de error en el código. ✗

Guitar Hero: On Tour

- Ficheros comprimidos con formato propietario. ✓
  - El algoritmo ocupa 1.900 instrucciones máquina. ✓
- No hay compresión en las siguientes ediciones. ✗
- Formato canciones: `Vorbis OGG`. ✗

```
LDR     R1, =aInvalidWindowS            ; "invalid window size"
MOV     R0, #0x1B
STR     R1, [R9,#0x18]
STR     R0, [R8]
```

Figura: Mensajes de error en el código. ✗

Guitar Hero: On Tour

- Ficheros comprimidos con formato propietario. ✓
  - El algoritmo ocupa 1.900 instrucciones máquina. ✓
- No hay compresión en las siguientes ediciones. ✗
- Formato canciones: `Vorbis OGG`. ✗

```
LDR     R1, =aInvalidWindowS            ; "invalid window size"
MOV     R0, #0x1B
STR     R1, [R9,#0x18]
STR     R0, [R8]
```

Figura: Mensajes de error en el código. ✗

Duet

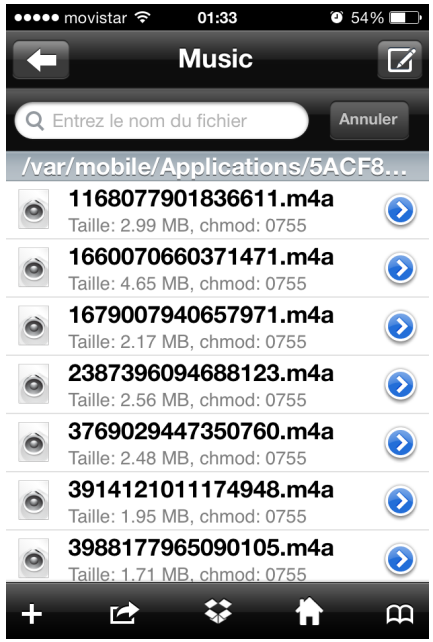
- Juego para plataformas móviles (Android, iOS).
- La banda sonora se vende en iTunes por 3.99€.
- Se encuentra desprotegida en la carpeta del juego en formato estándar.

Duet

- Juego para plataformas móviles (Android, iOS).
- La banda sonora se vende en iTunes por 3.99€.
- Se encuentra desprotegida en la carpeta del juego en formato estándar.

Duet

- Juego para plataformas móviles (Android, iOS).
- La banda sonora se vende en iTunes por 3.99€.
- Se encuentra desprotegida en la carpeta del juego en formato estándar.



Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en *e-books*. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación `MPEG`. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en *e-books*. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en *e-books*. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en *e-books*. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en *e-books*. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación `MPEG`. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en *e-books*. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación `MPEG`. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Índice de contenidos

Captura de paquetes

Estrategia *man-in-the-middle*

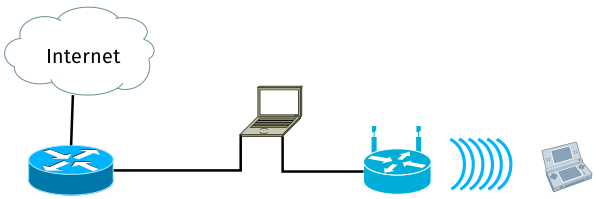


Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet,u32 len);
void save_adhocPacket(u8* packet,
  u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

`HandleDebugEvent_Execute()` en `debug.cpp`.

Captura de paquetes

Estrategia *man-in-the-middle*

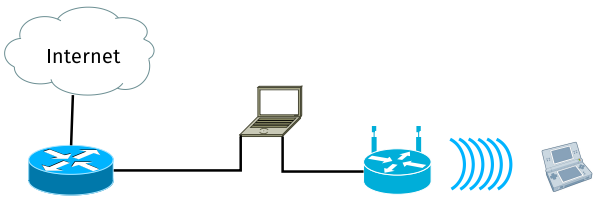


Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet,u32 len);
void save_adhocPacket(u8* packet,
  u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

`HandleDebugEvent_Execute()` en `debug.cpp`.

Captura de paquetes

Estrategia *man-in-the-middle*

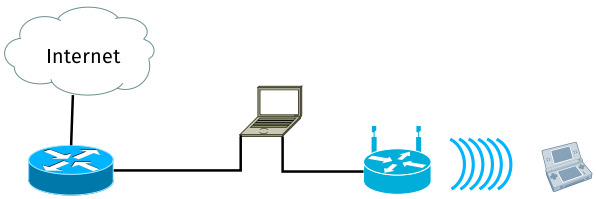


Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet,u32 len);
void save_adhocPacket(u8* packet,
  u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

`HandleDebugEvent_Execute()` en `debug.cpp`.

Captura de paquetes

Estrategia *man-in-the-middle*

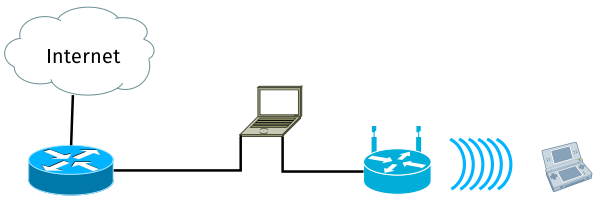


Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet,u32 len);
void save_adhocPacket(u8* packet,
  u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

`HandleDebugEvent_Execute()` en `debug.cpp`.

Captura de paquetes

Estrategia *man-in-the-middle*

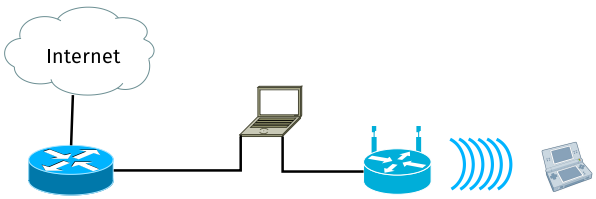


Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet,u32 len);
void save_adhocPacket(u8* packet,
  u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

`HandleDebugEvent_Execute()` en `debug.cpp`.

Captura de paquetes

Estrategia *man-in-the-middle*

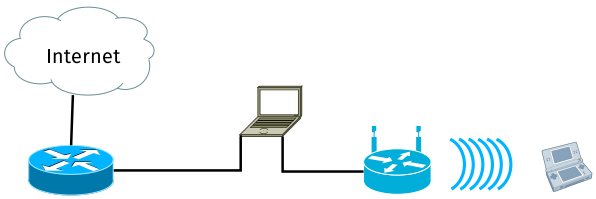


Figura: *Man-in-the-middle*

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet,u32 len);
void save_adhocPacket(u8* packet,
  u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

`HandleDebugEvent_Execute()` en `debug.cpp`.

```
Reading: /store/Juegos/NDS/Ninokuni [CLEAN].nds
Found in Overlay9_2.bin at 0x020986B8
Press Enter to continue.
------------------------------
```

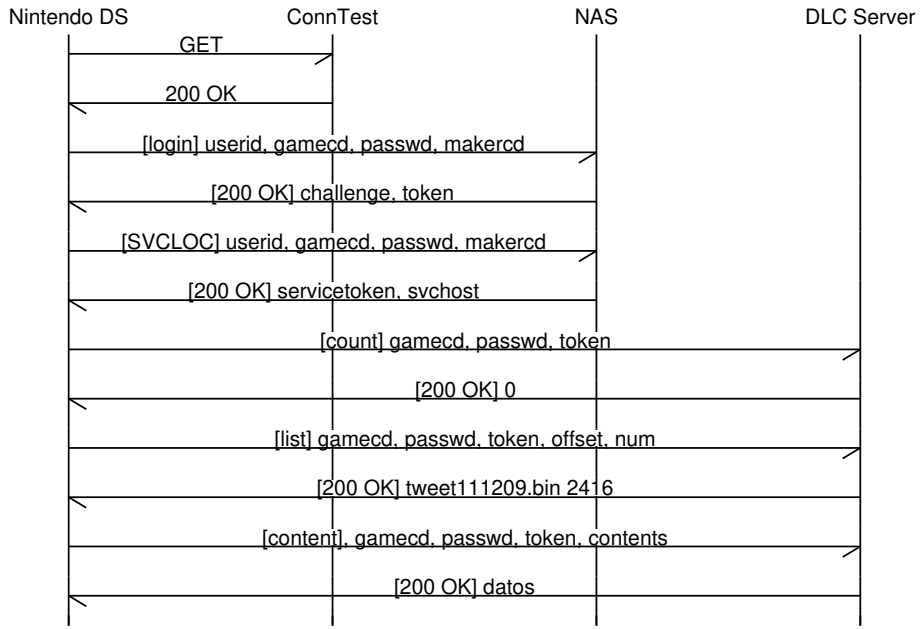
Figura: *RC4Finder.*

Servidores para Nintendo DS

Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

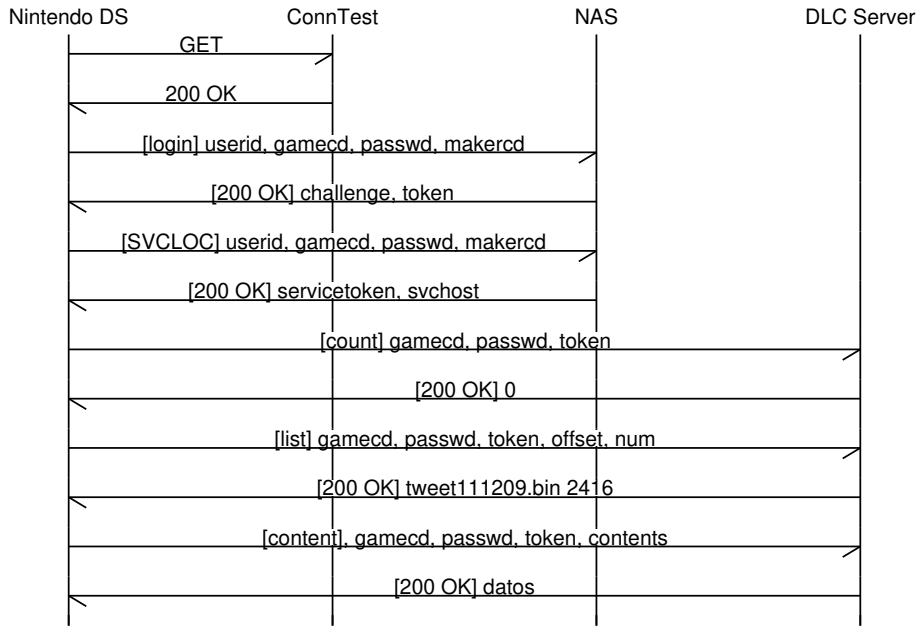
Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

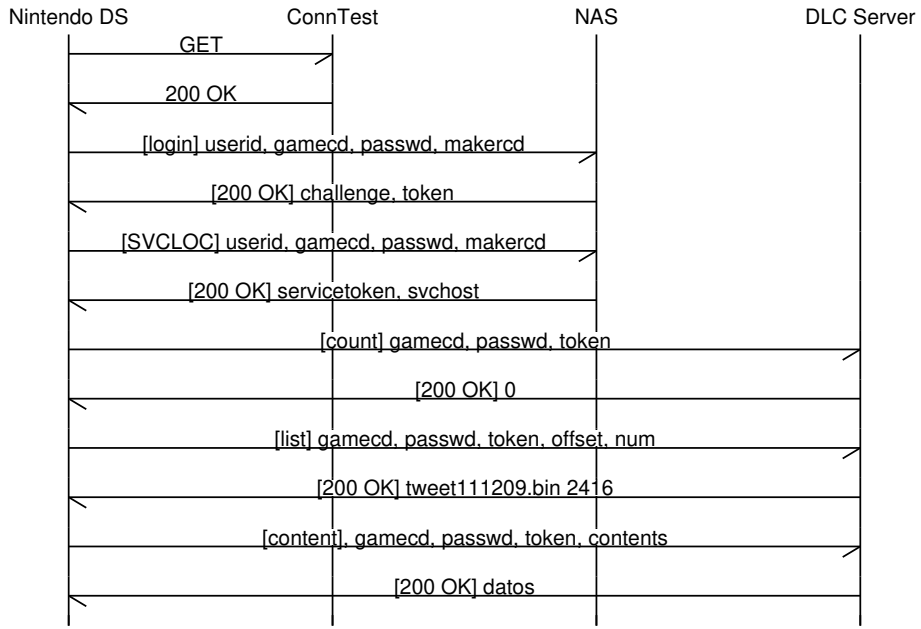
Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

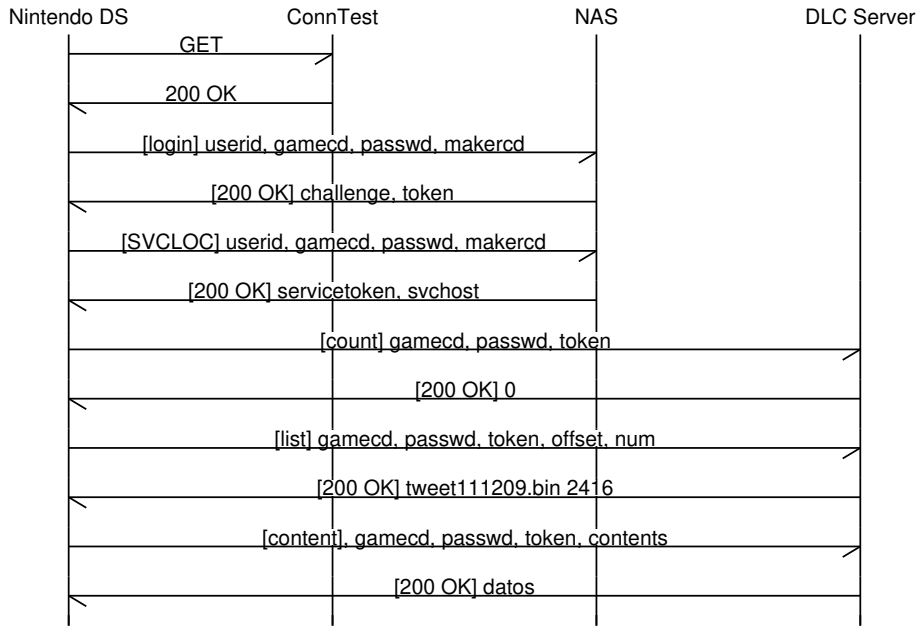
Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

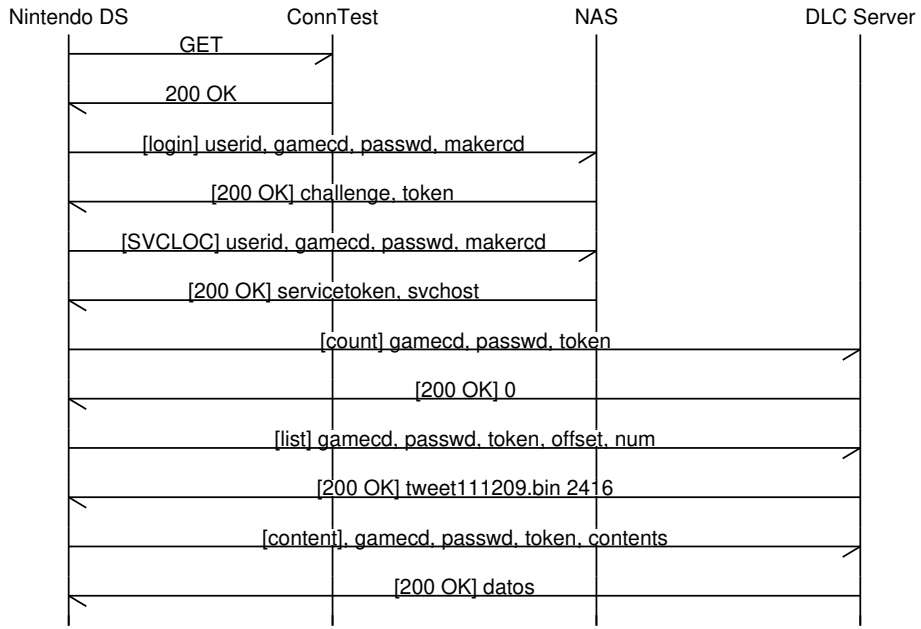
Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

Preguntados

Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

Preguntados

Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

Preguntados

Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

Preguntados

Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.


```
{'id':4880,"category":"HISTORY",'text':"..C..mo se denominaba en la Edad Media al hijo
tenido fuera del matrimonio?",'answers':
['Fogardo","Bastardo","Hu..rfano","Primog..nito'],'correct_answer":1,'media_type":"NORMAL
"}},{"question":{"id":4004,'category":'GEOGRAPHY","text":"..Qu.. colores tiene la bandera
de M..xico?",'answers':['Azul, amarillo y rojo","Azul, verde y rojo","Blanco, verde y
rojo","Amarillo, verde y
rojo'],'correct_answer":2,"media_type":"NORMAL"},"powerup_question":
```


Figura: Preguntas, respuesta y solución de una partida

Preguntados

Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.


```
{'id':4880,"category":"HISTORY","text":"..C..mo se denominaba en la Edad Media al hijo
tenido fuera del matrimonio?",'answers':
['Fogardo","Bastardo","Hu..rfano","Primog..nito'],'correct_answer":1,"media_type":"NORMAL
"}},{"question":{"id":4004,'category":'GEOGRAPHY","text":"..Qu.. colores tiene la bandera
de M..xico?",'answers':['Azul, amarillo y rojo","Azul, verde y rojo","Blanco, verde y
rojo","Amarillo, verde y
rojo'],'correct_answer":2,"media_type":"NORMAL"},"powerup_question":
```


Figura: Preguntas, respuesta y solución de una partida

Preguntados

Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.


```
{'id':4880,"category":"HISTORY","text":"..C..mo se denominaba en la Edad Media al hijo
tenido fuera del matrimonio?",'answers':
['Fogardo","Bastardo","Hu..rfano","Primog..nito'],'correct_answer":1,"media_type":"NORMAL
"}},{"question":{"id":4004,'category":'GEOGRAPHY","text":"..Qu.. colores tiene la bandera
de M..xico?",'answers':['Azul, amarillo y rojo","Azul, verde y rojo","Blanco, verde y
rojo","Amarillo, verde y
rojo'],'correct_answer":2,"media_type":"NORMAL"},"powerup_question":
```


Figura: Preguntas, respuesta y solución de una partida

Duet

- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

Duet

- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

Duet

- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

Duet

- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

Duet

- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

306	TFPremiumUnlocked	0	12	1
307	TFEncoreUnlocked	0	12	1

Figura: Filas con estado de los contenidos extras

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con `RSA`.

Solución de Nintendo:

- Comprobar integridad con `HMAC`.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con `RSA`.

Solución de Nintendo:

- Comprobar integridad con `HMAC`.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con `RSA`.

Solución de Nintendo:

- Comprobar integridad con `HMAC`.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con `RSA`.

Solución de Nintendo:

- Comprobar integridad con `HMAC`.
- Solo si con *Download Play*.

Índice de contenidos

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado `XOR`.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado `XOR`.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado `XOR`.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
  - Implementaciones largas (1.900 líneas).
  - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado `XOR`.
  - No usar claves estáticas.
- Codificación de caracteres no estándar.
  - Desordenar caracteres.
  - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

ugr Universidad de Granada

Seguridad en comunicaciones

- HTTPS vs HTTP.
  - Cerrar puertos de servidores.
  - Diseño del protocolo.
- Autenticación con contraseña vs reto.
  - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
  - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
  - Cerrar puertos de servidores.
  - Diseño del protocolo.
- Autenticación con contraseña vs reto.
  - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
  - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
  - Cerrar puertos de servidores.
  - Diseño del protocolo.
- Autenticación con contraseña vs reto.
  - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
  - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
  - Cerrar puertos de servidores.
  - Diseño del protocolo.
- Autenticación con contraseña vs reto.
  - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
  - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
  - Cerrar puertos de servidores.
  - Diseño del protocolo.
- Autenticación con contraseña vs reto.
  - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
  - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
  - Cerrar puertos de servidores.
  - Diseño del protocolo.
- Autenticación con contraseña vs reto.
  - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
  - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
  - Cerrar puertos de servidores.
  - Diseño del protocolo.
- Autenticación con contraseña vs reto.
  - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
  - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
  - Cerrar puertos de servidores.
  - Diseño del protocolo.
- Autenticación con contraseña vs reto.
  - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
  - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Índice de contenidos

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender LaTeX.

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender LaTeX.

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador `ARM`.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender LaTeX.

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador `ARM`.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender LaTeX.

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador `ARM`.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender LaTeX.

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender LaTeX.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Trabajo futuro

- Estudios:
  - Seguridad en videoconsolas y sus *exploits*.
  - Algoritmos de integridad en archivos de guardado.
  - Mecanismos anti-copia físicos y digitales.
  - Protocolos de micropagos en videojuegos.
  - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
  - Implementar mecanismos estudiados.
  - Explorador de juegos avanzado.
  - Depurador de código remoto.

Gracias por su atención

Repositorio en GitHub: `https://github.com/pleonex/AiroRom`

Índice de contenidos

7 Apéndice

- Metodología
- Traducciones no oficiales
- Contenidos con derechos de autor
- Servicios en línea

Andew Huang - Hacking the Xbox. An introduction to Reverse Engineering

In general, I hack because it is quite satisfying to know that somebody's life was made better by something I built. I feel it is my obligation to apply my talents and return to society what it has given me. I also enjoy the challenge of exploration. I want to understand electronics as deeply as I can. Black boxes frustate me; nothing gets my curiosity going more than a box that I'm not allowed to open or understand. As a result, I have a fiduciary interest in cryptography and security methods.

Averiguar codificación desde tipografía

Pokémon Perla y Diamante

Pokémon HeartGold y SoulSilver

Pokémon Conquest

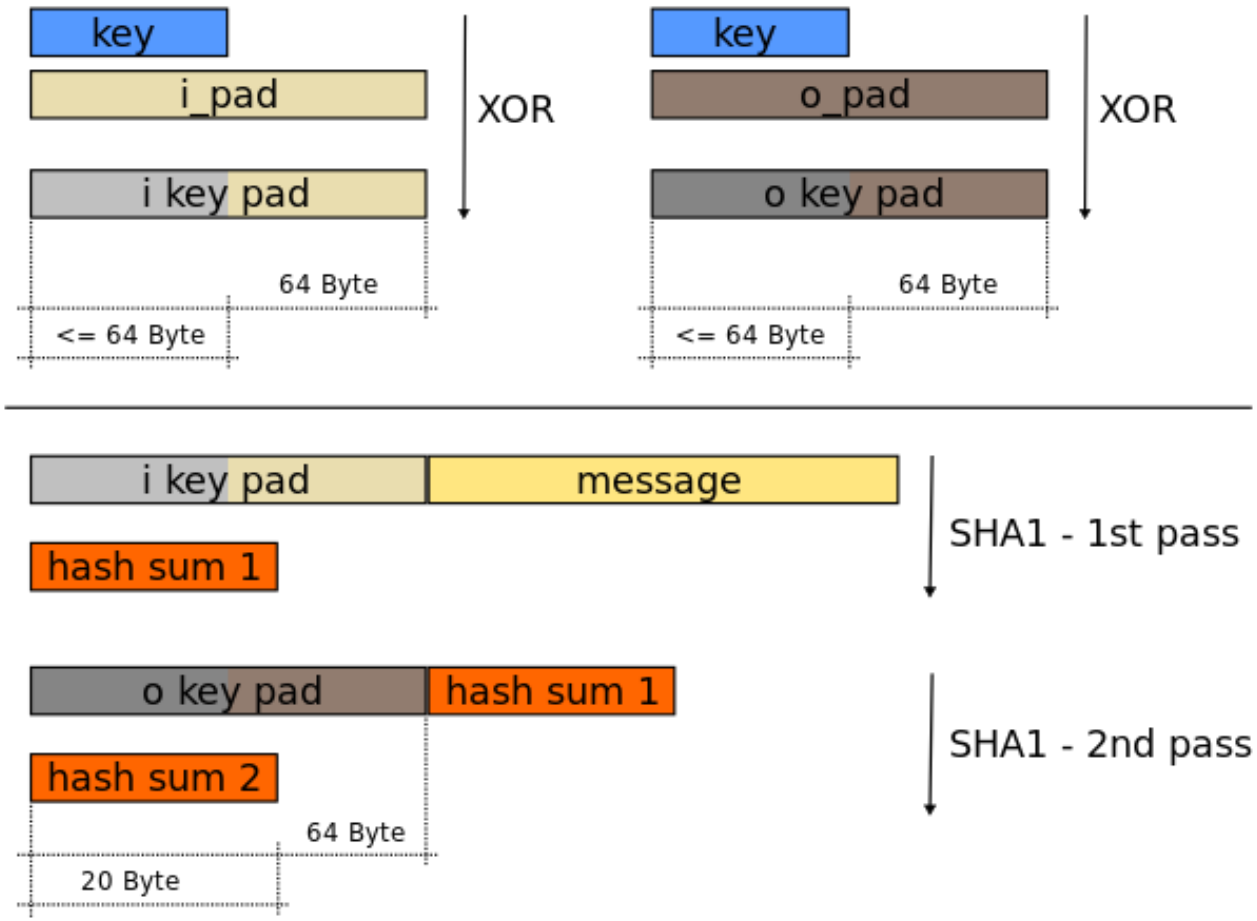
Ninokuni: El Mago de las Tinieblas

100 Classic Book Collection

Elite Beat Agents

Guitar Rock

HMAC


key
i_pad
XOR
i key pad
64 Byte
<= 64 Byte
key
o_pad
XOR
o key pad
64 Byte
<= 64 Byte
i key pad
message
hash sum 1
SHA1 - 1st pass
o key pad
hash sum 1
hash sum 2
64 Byte
20 Byte
SHA1 - 2nd pass

Servidores de Nintendo

Token generando aplicando `MD5` a:

- `MD5` del $challenge_{NAS}$.
- $challenge_{consola}$.
- 48 espacios en blanco.
- $challenge_{servidor}$.
- $token_{NAS}$.
- `MD5` del $challenge_{NAS}$.

100 Classic Book Collection

Ninokuni: El Mago de las Tinieblas