

# Hacking de Binários em Hexadecimal

## Trabalho 1

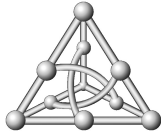
Segurança de Redes — 2018

### 1 Descrição

Uma das técnicas mais conhecidas e usadas para quebrar aplicações e subvertê-las é modificando diretamente o binário gerado. Uma forma de fazer isso é usando um simples editor hexadecimal para modificar o binário sem, necessariamente, alterar o seu código fonte. Essa técnica é muito utilizada na tradução de programas e jogos de computadores (e, para algumas mentes não bem intencionadas, outros fins). Embora seja uma técnica simples, os binários costumam usar estratégias para ocultar as informações como compressão (Huffman, LZ77, etc), tabelas e ponteiros. Isso torna a aplicação geral da técnica muito mais complexa. O objetivo deste trabalho é subverter as ROM's (o dump de um cartucho de video game) do jogo do **Super Mario World** do Super Nintendo para traduzir as mensagens do jogo. A imagem a seguir mostra um exemplo de mensagem do Super Mario:



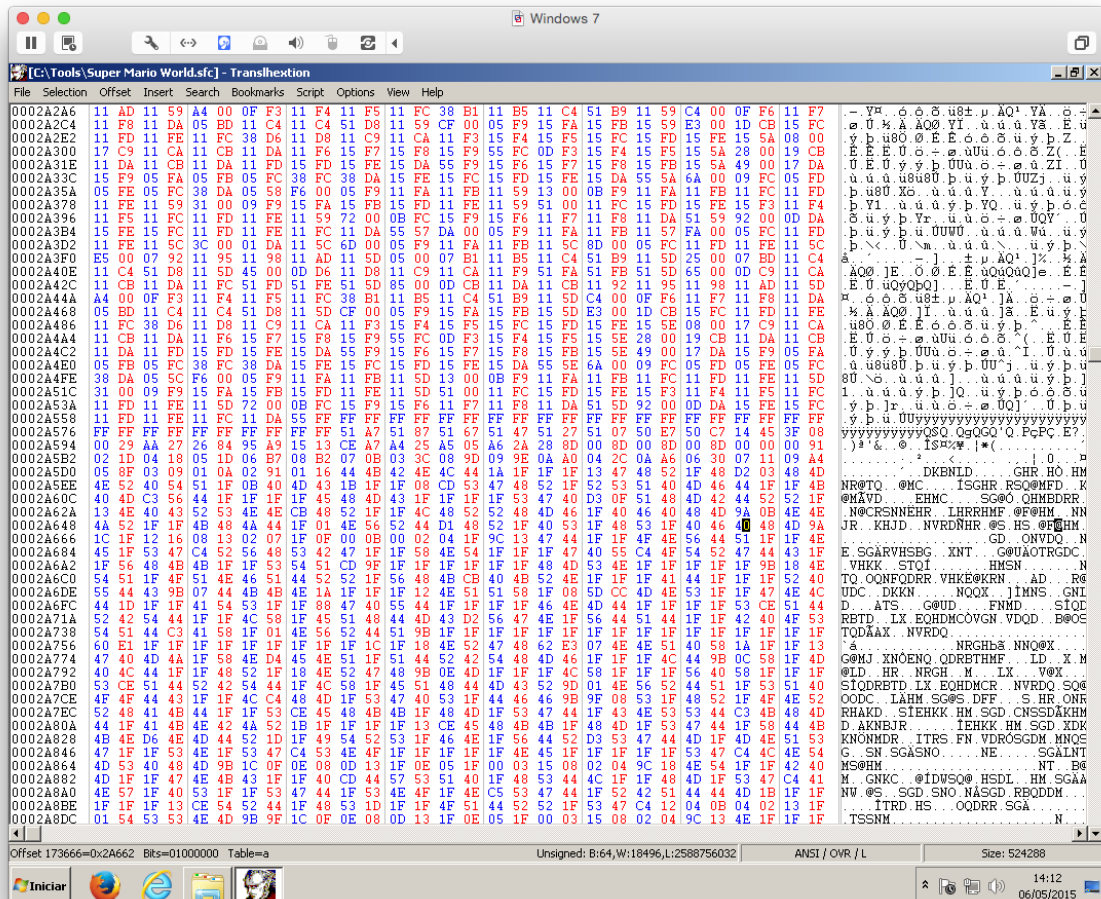
A mensagem na imagem é: Welcome! This is Dinosaur Land. In this strange land we find that Princess Toadstool is missing again! Looks like Bowser is at it again!



## UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

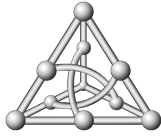
### Faculdade de Computação

O material a seguir mostra como analisar a ROM do Super Mario. Se abrirmos a ROM (binário do Super Mário) do jogo em um editor hexadecimal como o Translhextion16c, é possível abrir o ROM e ver o seu conteúdo:

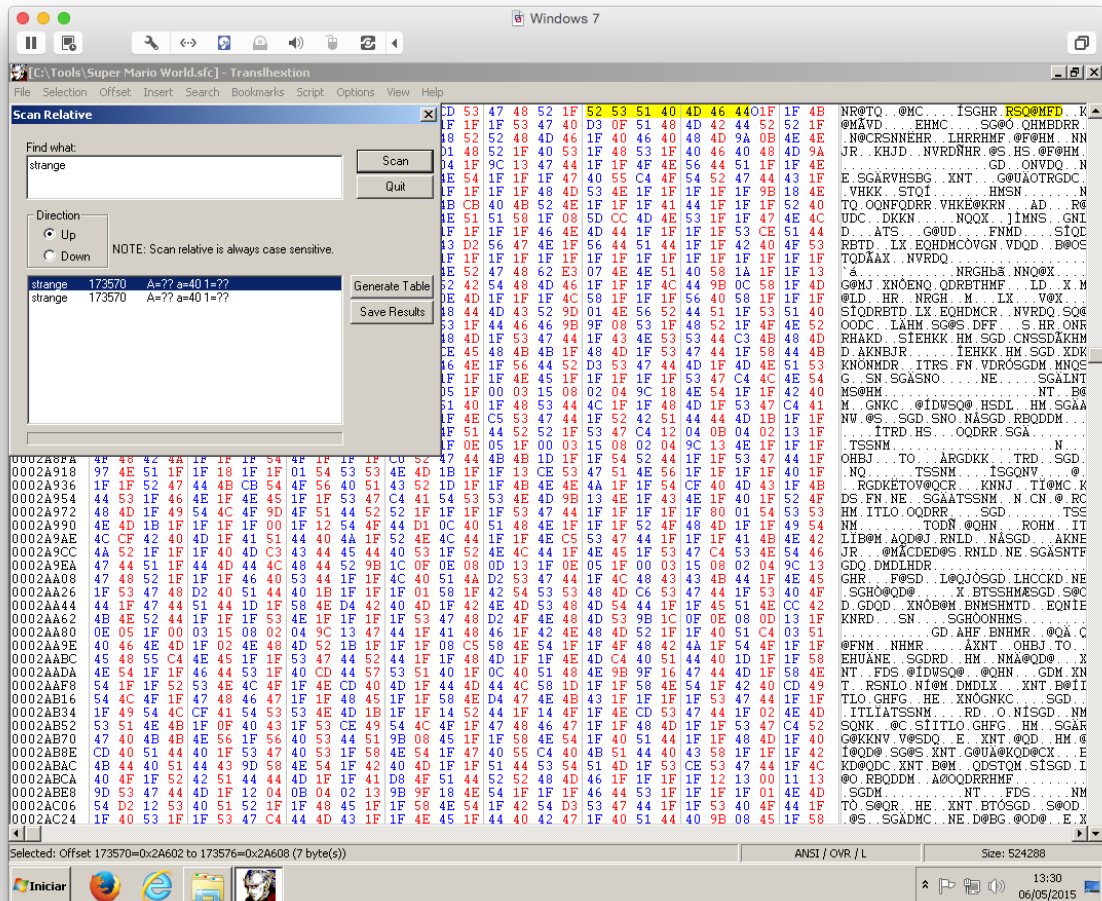


Da para notar que está totalmente incompreensível. Isso é verdade porque não conseguimos interpretar diretamente os valores hexadecimais para letras e caixas de texto de forma simples.

No caso dessa ROM em especial, para “enxergarmos” basta criarmos uma tabela que relacione os valores em hexadecimal com as letras correspondentes, ou seja, mapear a tabela ASCII com valores diferentes dos já conhecidos. O Translhextion16c possui um mecanismo de busca relativa que busca usando a relação entre a distância das letras de uma palavra. Então, para acharmos uma “relação”, basta encontrarmos quais cadeias hexadecimais casam com os “valores” encontrados na ROM.



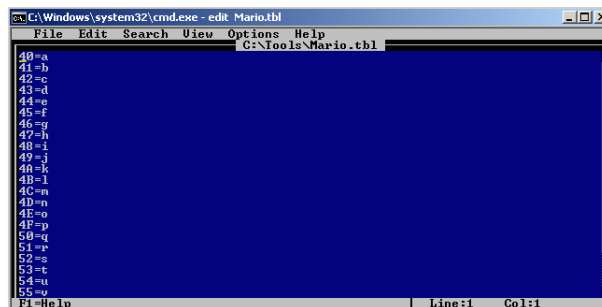
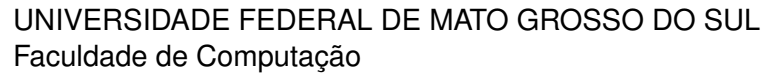
Realizando uma busca relativa vemos que é possível encontrar uma relação entre valores em hexa e letras:



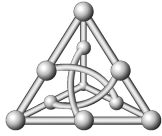
Dessa forma podemos gerar a tabela relativa usando o botão: **Generate Table**.

Com a tabela gerada já é possível “enxergar” parte do texto do jogo diretamente pelo binário: E, dessa forma, montar uma tabela de “equivalência”.

Obviamente a tabela acima está incompleta e não está mapeando caracteres como SPACE (espaço) ou as letras maiúsculas, mas já serve como um exemplo do que é necessário fazer.



1. Criar uma ferramenta (finder.exe), para cada ROM, que receba uma string e retorne a posição na ROM (offset) e os valores hexadecimais encontrados.
2. Criar uma ferramenta (extractor.exe), para cada ROM, que leia o ROM e extraia os textos do jogo de tal forma que seja possível modificar a sua extração (traduzindo os textos) para futura reinserção.



3. Criar uma ferramenta (injector.exe) que injete os textos modificados pela ferramenta anterior diretamente na ROM.

### Parte 2:

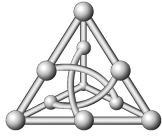
1. Traduzir a mensagem inicial do jogo no seu arquivo extraído.
2. Inserir o texto na ROM editando diretamente o binário.
3. Escrever um relatório de no máximo uma página explicando como foi criada a tabela e as estratégias adotadas para extrair e inserir o texto no binário.

Para testar se a sua ROMhacking teve sucesso use um emulador de SNES como SNES9x (possui versões para Windows, Linux, Android). No MacOSX é possível usar o OpenEmu (que usa o motor do SNES9x). O trabalho é individual e a entrega deverá ser feita no Moodle da disciplina. Todos os programas e o relatório devem ser enviados em um único arquivo .ZIP. Uma observação importante: O jogo pode possuir mais de uma tabela ASCII para representar caracteres!

## 2 Informações Adicionais

Apenas a título de curiosidade, seguem algumas extrações feitas diretamente da ROM usando um programa Python que usa um dicionário para mapear a DTL: Texto 1: Welcome! This is Dinosaur Land. In this strange land we find that Princess Toadstool is missing again! Looks like Bowser is at it again!

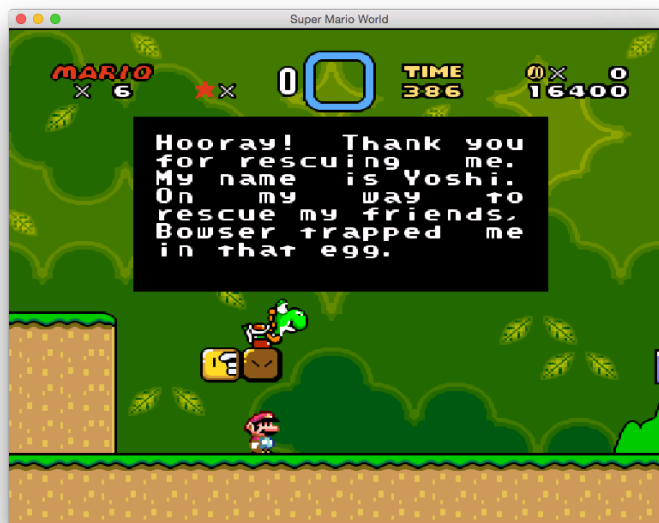




```
Documents - bash - 85x17
bash
Brivaldos-Mac-mini:Src condecor$ python Viewer.py SMario.sfc | grep -A6 Welcome
C91BWelcome! This is
Dinosaur Land. In thi
s strange land we
find that Princess
Toadstool is missing
again! Looks like Bow
ser is at it again! C S
Brivaldos-Mac-mini:Src condecor$
```

E o resultado da extração usando uma tabela previamente criada:

Texto2: Hooray! Thank you for rescuing me. My name is Yoshi. On my way to rescue my friends, Bowser trapped me in that egg.

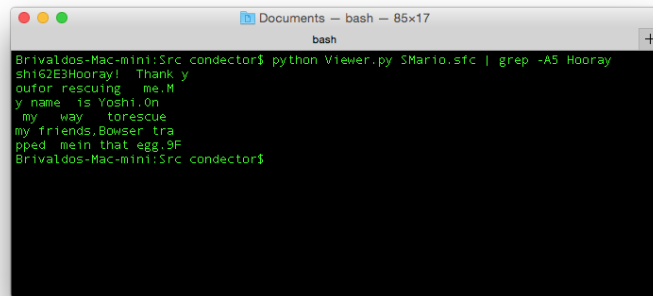
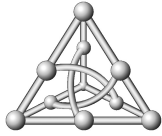


E o resultado da extração usando uma tabela previamente criada:

### 3 Entrega

O trabalho pode se feita em dupla. Instruções para entrega do seu trabalho:

1. **Forma de entrega:** A entrega será realizada diretamente no Sistema de Suporte a Disciplinas ([AVA/UFMS](#)), na disciplina de Redes de Computadores.



```
Documents - bash - 85x17
bash
Brivaldos-Mac-mini:Src condecor$ python Viewer.py 5Mario.sfc | grep -A5 Hooray
sh162EHooray! Thank y
outfor rescuing me.M
y name is Yoshi.On
my way torescue
my friends,Bowser tra
pped mein that egg.9F
Brivaldos-Mac-mini:Src condecor$
```

2. **Atrasos** Trabalhos atrasados não serão aceitos. Não deixe para entregar seu trabalho na última hora. Para prevenir imprevistos como queda de energia, problemas com o sistema, falha de conexão com a internet, sugerimos que a entrega do trabalho seja feita pelo menos um dia antes do prazo determinado.
3. **Erros** Trabalhos com erros de importação receberão nota **ZERO**. Faça todos os testes necessários para garantir que seu programa esteja livre de erros de compilação.
4. **Conduta Ética** O trabalho deve ser feito **INDIVIDUALMENTE OU DUPLA**. Cada estudante tem responsabilidade sobre cópias de seu trabalho, mesmo que parciais. Não faça o trabalho com outros grupos e não compartilhe seu programa ou trechos de seu programa. Você pode consultar seus colegas para esclarecer dúvidas e discutir idéias sobre o trabalho, ao vivo ou no fórum de discussão da disciplina, mas **NÃO** copie o trabalho!

Trabalhos considerados plagiados terão nota **ZERO**. Estudante que se envolver em **DOIS CASOS DE PLÁGIO** estará automaticamente **REPROVADO** na disciplina.