Jackpot!

Attacking Arcade Machines

Patrick Sayler

NETSPI™

Introduction

Twitter: @psayler

Blog: blog.netspi.com

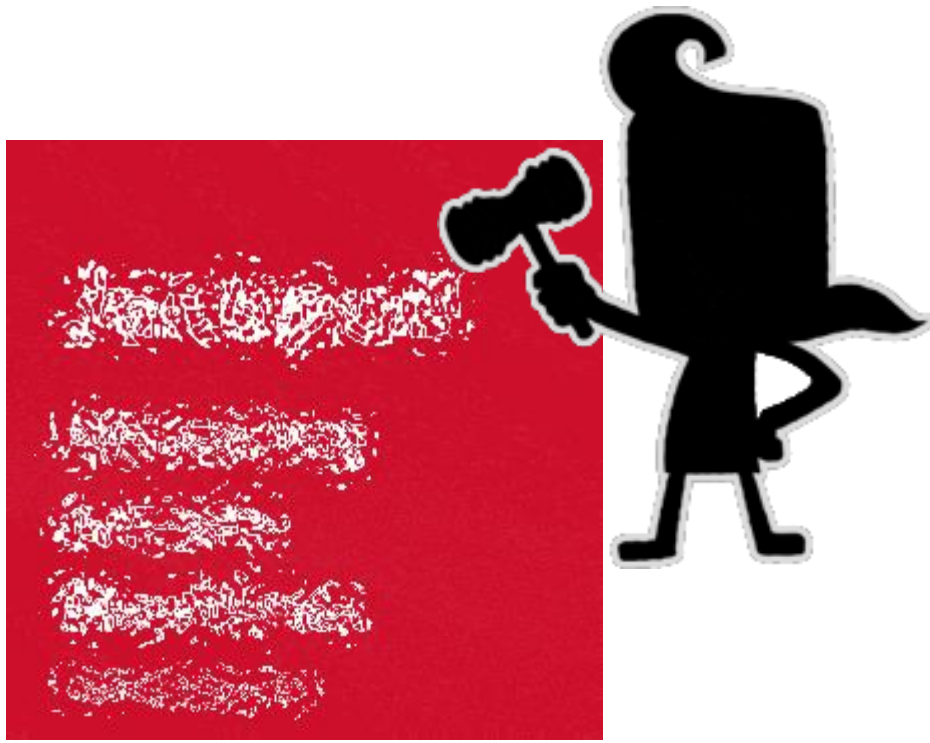
Website: www.netspi.com

Patrick Sayler

- Penetration Tester @ NetSPI
- Social Engineering
  - Phone
  - Email
  - Onsite

Introduction

```
        to make sure that you have the latest version.
Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.0.log", Time: Thu Sep 16 02:07:48 2021
(==) Using system config directory "/usr/share/X11/xorg.conf.d"
(EE) Failed to load module "vmwgfx" (module does not exist, 0)
(EE) vmware: Please ignore the above warnings about not being able to to load mo
dule/driver vmwgfx
(EE) open /dev/fb0: No such file or directory
SELinux: Disabled on system, not enabling in X server
(EE) Failed to initialize GLX extension (Compatible NVIDIA X driver not found)
Xlib:  extension "GLX" missing on display ":0.0".
Xlib:  extension "GLX" missing on display ":0.0".
Xlib:  extension "GLX" missing on display ":0.0".
Xlib:  extension "GLX" missing on display ":0.0".

waiting for X server to shut down ..error setting MTRR (base = 0xe8000000, size
= 0x08000000, type = 1) Invalid argument (22)



Debian GNU/Linux 6.0 SmartSmacker tty1

SmartSmacker login: _
```

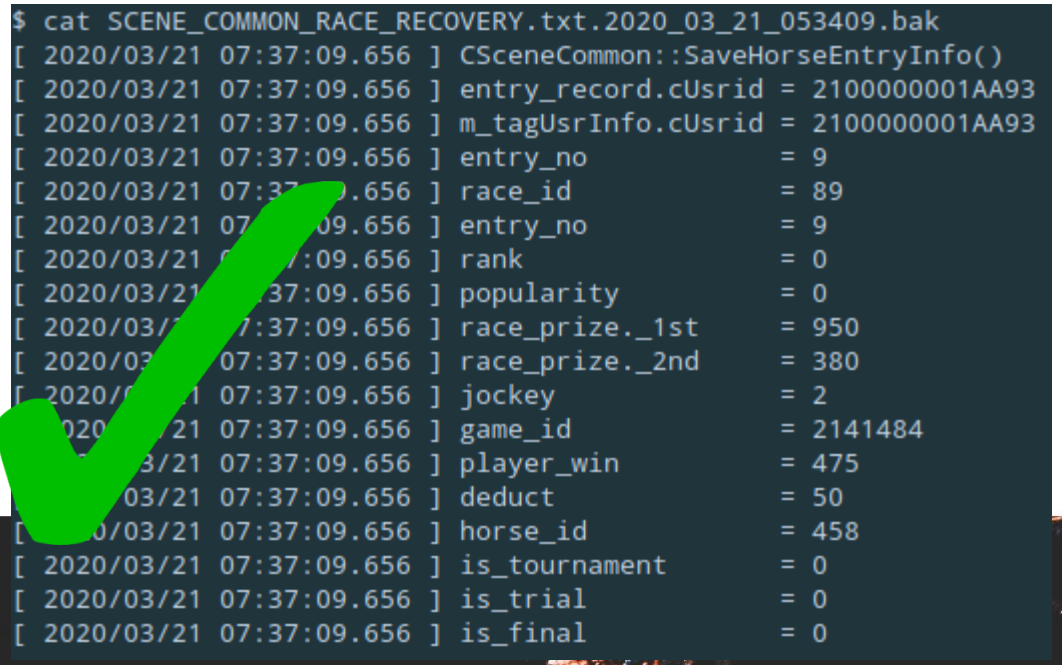


Introduction

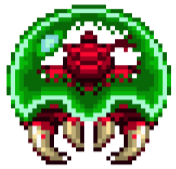
```
Xlib:  extension "GLX" missing on display ":0.0".
Xlib:  extension "GLX" missing on display ":0.0".

waiting for X server to shut down .error setting MTRR (base = 0xe8000000, size =
 0x08000000, type = 1) Invalid argument (22)



Debian GNU/Linux 6.0 SmartSmacker tty1

SmartSmacker login: root
Password:
Last login: Wed Oct  6 01:45:04 KST 2021 on tty1
Linux SmartSmacker 2.6.32-5-686 #1 SMP Mon Jun 13 04:13:06 UTC 2011 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@SmartSmacker:~# cat /etc/issue
Debian GNU/Linux 6.0 \n \l

root@SmartSmacker:~#
```

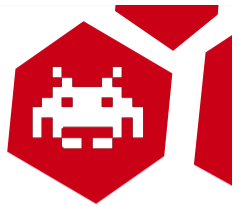
Disclaimer


00175da0: ff75 0d8d 65f4 5b5e 5f89 d05d c38d 7600
00175db0: 508d 45f0 508b 7b04 576a 00e8 f05d faff
00175dc0: 89c2 8b43 1c89 5020 8b45 f001 4304 ba01
00175dd0: 0000 00eb ce8d 7426 008
00175de0: 8b43 048a 0831 d280
00175df0: 74b1 31d2 80f9 297
00175e00: a53c 0176 0980 f9
00175e10: 0c53 e829 fdff
00175e20: 8b4b 1851 53e8
00175e30: 008b 7b14 c743
00175e40: 6a00 53e8 6801
00175e50: 2974 4983 ec08
00175e60: 3708 53e8 78b3
00175e70: 53e8 aabb ffff 83
00175e80: baff ffff ff0f 841
00175e90: 1889 4128 897b 14e9
00175ea0: ebc9 8db4 2600 0000 008d
00175eb0: 5589 e553 83ec 108b 5d08 c743 1c00 0000
00175ec0: 0053 e8a9 feff ff83 c410 31d2 85c0 7415
00175ed0: 8b43 1c85 c074 1983 ec0c 53e8 50fd ffff


$ cat SCENE_COMMON_RACE_RECOVERY.txt.2020_03_21_053409.bak
[2020/03/21 07:37:09.656] CSceneCommon::SaveHorseEntryInfo()
[2020/03/21 07:37:09.656] entry_record.cUsrid = 2100000001AA93
[2020/03/21 07:37:09.656] m_tagUsrInfo.cUsrid = 2100000001AA93
[2020/03/21 07:37:09.656] entry_no = 9
[2020/03/21 07:37:09.656] race_id = 89
[2020/03/21 07:37:09.656] entry_no = 9
[2020/03/21 07:37:09.656] rank = 0
[2020/03/21 07:37:09.656] popularity = 0
[2020/03/21 07:37:09.656] race_prize._1st = 950
[2020/03/21 07:37:09.656] race_prize._2nd = 380
[2020/03/21 07:37:09.656] jockey = 2
[2020/03/21 07:37:09.656] game_id = 2141484
[2020/03/21 07:37:09.656] player_win = 475
[2020/03/21 07:37:09.656] deduct = 50
[2020/03/21 07:37:09.656] horse_id = 458
[2020/03/21 07:37:09.656] is_tournament = 0
[2020/03/21 07:37:09.656] is_trial = 0
[2020/03/21 07:37:09.656] is_final = 0

Disclaimer





Don't Give Credit: Hacking Arcade Machines

Ronald Huizer

- In The Groove 2
- Dancing simulator made by RoXoR games.
- Uses USB dongles to store profiles.

https://downloads.immunityinc.com/infiltrate-archives/Arcade_Attacks.pdf

Overview

- What & Where?
- Environment Setup
- Threats
- Discoveries
- Remediation
- References

What & Where?

My Games

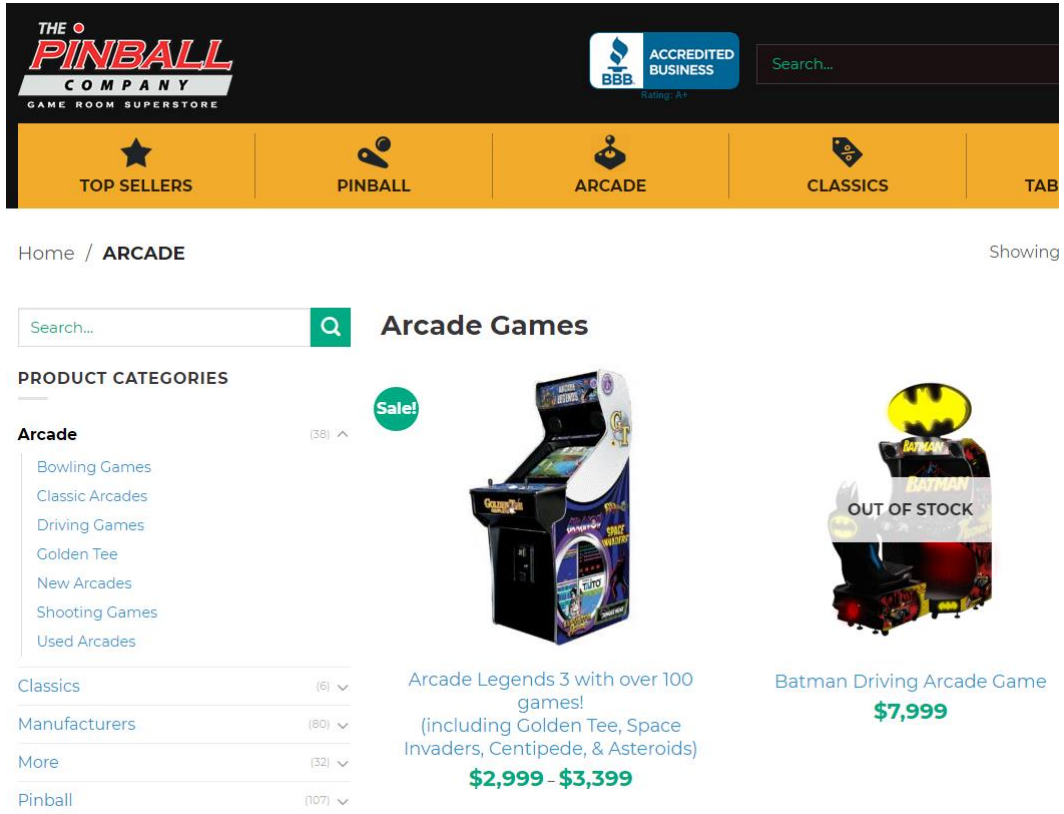

ANDAMIRO SMART SMACKER
MCU MK-4193
Warning

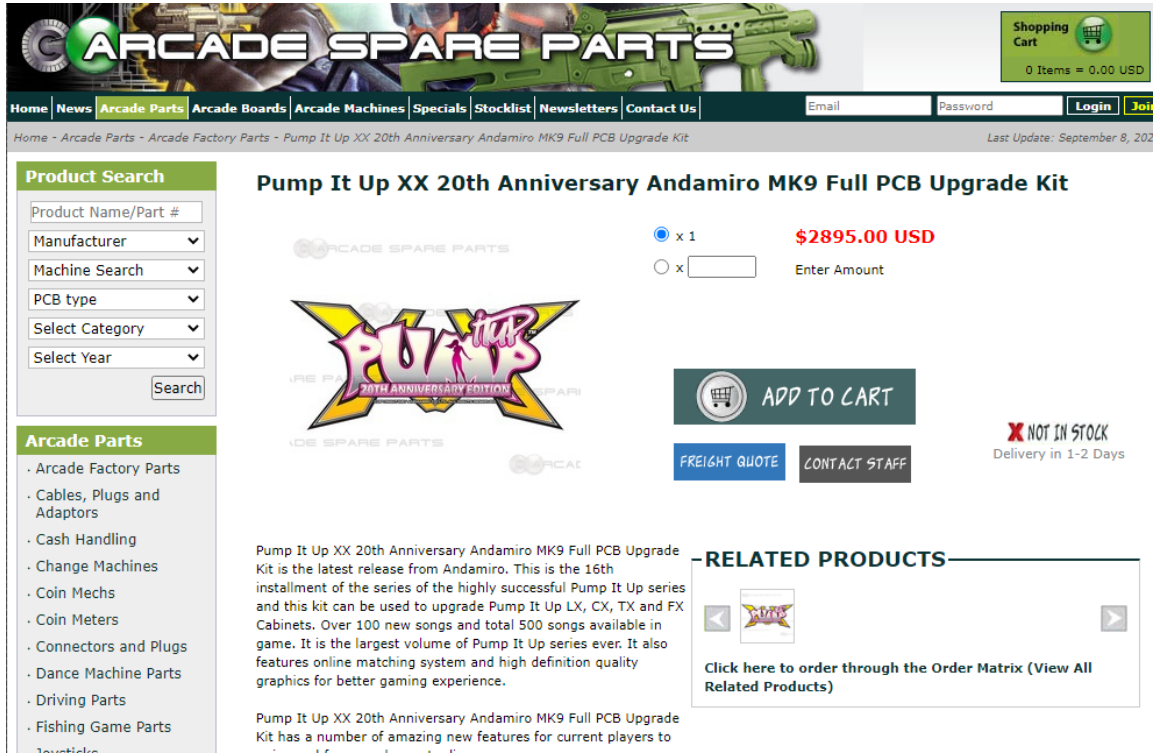

MEGATOUCH MAXX
SAPPHIRE 2
INSERT BILL HERE


TICKET OUTLET


PUMP IT UP
DANCER
DANCER
ANDAMIRO
ANDAMIRO
Get on the floor

Distributors





Resale Sites

ebay

OfferUp

buy. sell. simple.

$3,595

☆ Sep 5 STARGATE Arcade Machine by WILLIAMS 1981 is in excellent condition $3,595 (Deerfield north chicagoland)

$1,200

☆ Sep 5 muticade arcade games $1,200 (Glenview north chicagoland)

$150

☆ Sep 5 Arcade game slot machines $150 (Glenview north chicagoland)

$1,200

☆ Sep 5 muticade arcade games $1,200 (Glenview north chicagoland)

Resale Sites

ebay

OfferUp

buy. sell. simple.

NMLS #330511

better

RUSH 2049 SPECIAL EDITION ATARI REPLACEMENT HARD DRIVE FOR ARCADE GAME WORKING

Condition: Used

Quantity: 1 6 available / 15 sold

Price: US $34.95

Buy It Now

Add to cart

♡ Add to Watchlist

Limited quantity remaining | More than 70% sold | Free shipping

Shipping: FREE Expedited Shipping | See details
Located in: La Puente, California, United States
Ships to: United States and many other countries | See details

Delivery: Estimated between Thu. Sep. 23 and Sat. Sep. 25 to

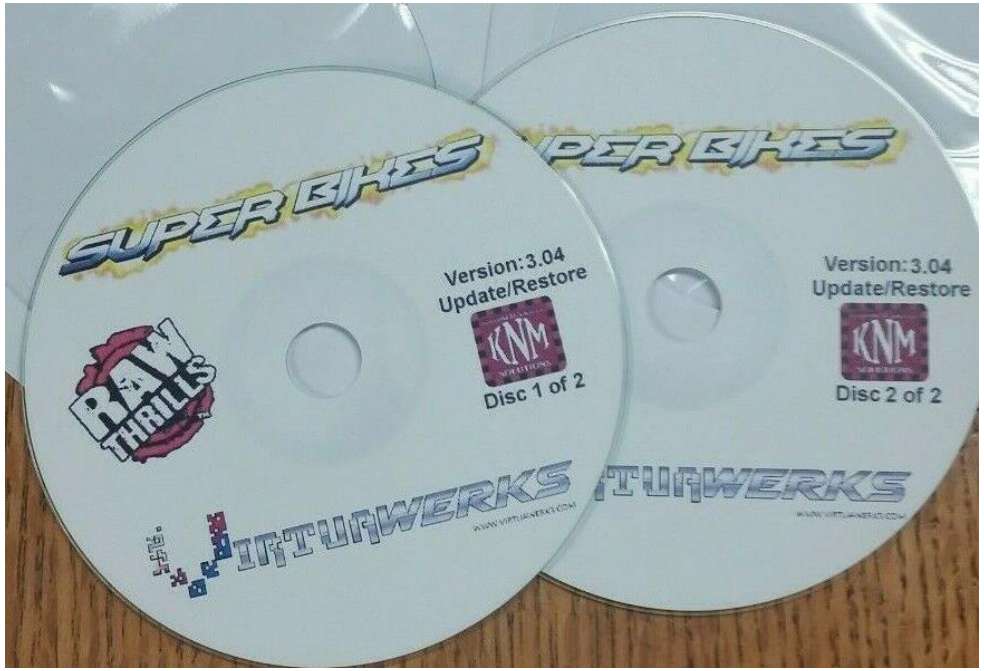
Payments: PayPal G Pay VISA

PayPal CREDIT

YAHOO! JAPAN

ヤフオク!

Recovery Images



ICE

Adrenaline Amusements

AMI Entertainment

Andamiro

Apple Industries

Bay Tek Entertainment

Benchmark Games, Inc.

Bobs Space Racers

Bromley

Chicago Gaming

Environment Setup

Backup

Safety Measure

- Avoid testing original drive
- Difficult to replace
- Out of print

Forensic Approach

- Compromised records
- Data loss

Image Backup - Listing Disks

Linux:

 # fdisk -l

```
Disk /dev/sdd: 74.5 GiB, 80026361856 bytes, 156301488 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x46849f4c

Device     Boot     Start       End   Sectors  Size Id Type
/dev/sdd1  *           63   2104514   2104452    1G  7 HPFS/NTFS/exFAT
/dev/sdd2        2104515 145468574 143364060 68.4G  f W95 Ext'd (LBA)
/dev/sdd5        2104578  84019949  81915372 39.1G  7 HPFS/NTFS/exFAT
/dev/sdd6       84020013 114736229  30716217 14.7G  7 HPFS/NTFS/exFAT
/dev/sdd7      114736293 145468574  30732282 14.7G  7 HPFS/NTFS/exFAT
```

Image Backup - Listing Disks

Mac:

 # diskutil -list

```
[TRUNCATED]
/dev/disk2 (external, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *5.0 TB     disk2
   1:                        EFI EFI                     209.7 MB   disk2s1
   2:          Apple_CoreStorage TimeMachine             1.2 TB     disk2s2
   3:                 Apple_Boot Boot OS X               134.2 MB   disk2s3
   4:       Microsoft Basic Data Backup                  3.8 TB     disk2s4
```

Image Backup - Sample DD Command

Linux:

```
root@mrjackpots # dd if=/dev/sdb of=my_game_disk.img
```

Mac:

```
root@mrjackpots # dd if=/dev/disk4 of=my_game_disk.img
```

Image Backup - Sample DD Command

Linux:

```
root@mrjackpots # dd if=/dev/sdb of=my_game_disk.img
```

Mac:

```
root@mrjackpots # dd if=/dev/disk4 of=my_game_disk.img
```

Image Backup - Sample DD Command

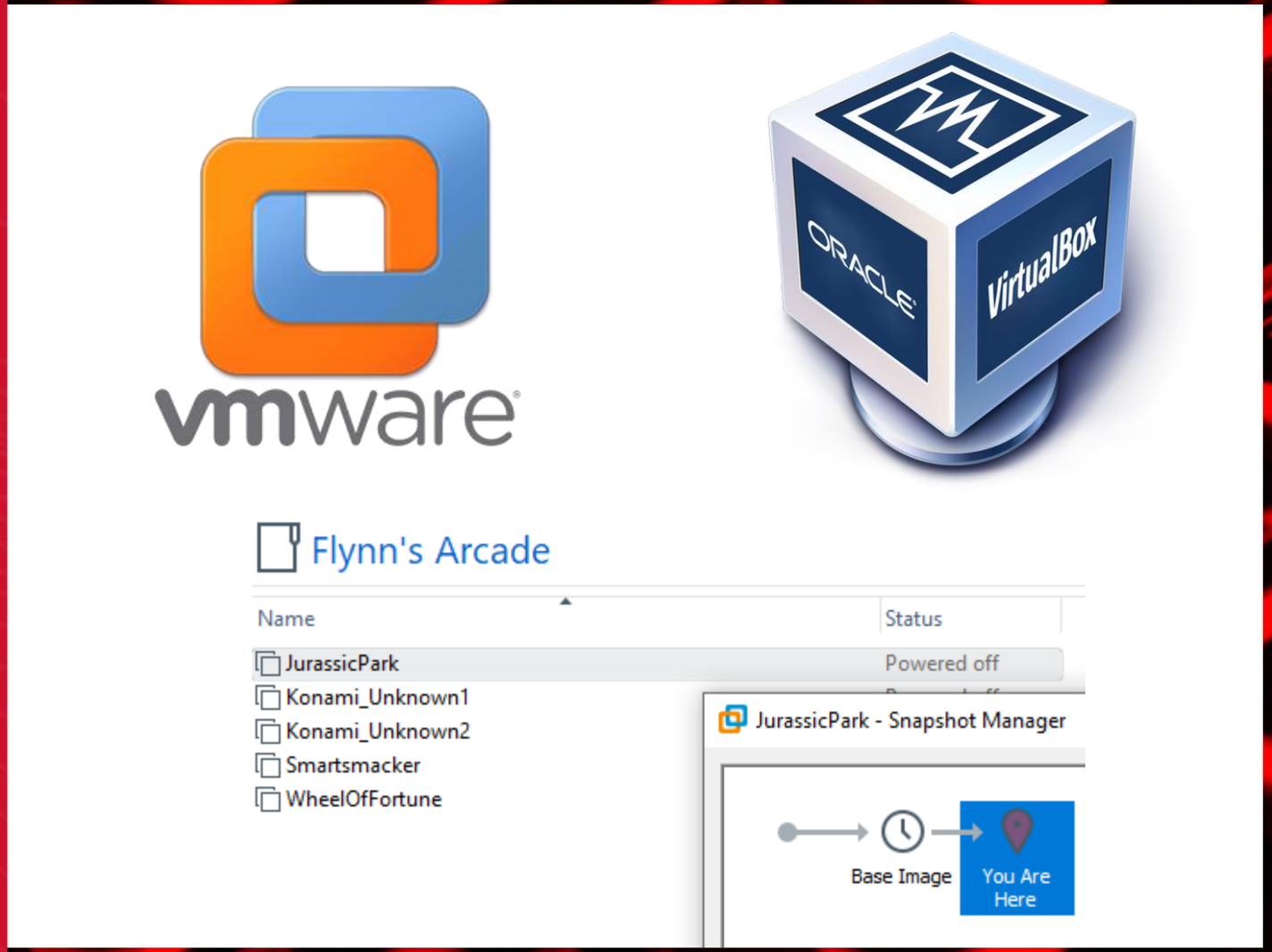
Linux:

```
root@mrjackpots # dd if=/dev/sdb of=my_game_disk.img
```

Mac:

```
root@mrjackpots # dd if=/dev/disk4 of=my_game_disk.img
```

Virtualization



Sample Command - VBoxConvert

VirtualBox:

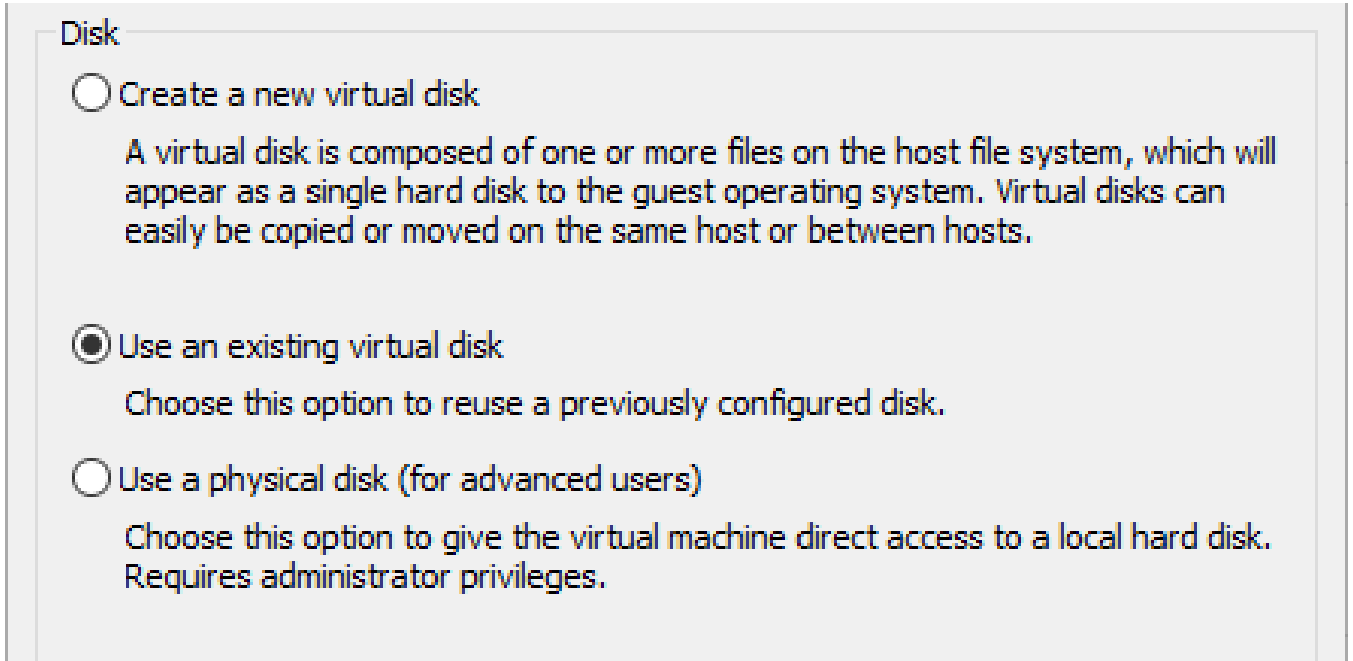
```
# VBoxManage convertdd my_game_disk.img my_game_disk.vmdk --format VMDK
```

Boot from Drive

- Test against live system
- May not be playable

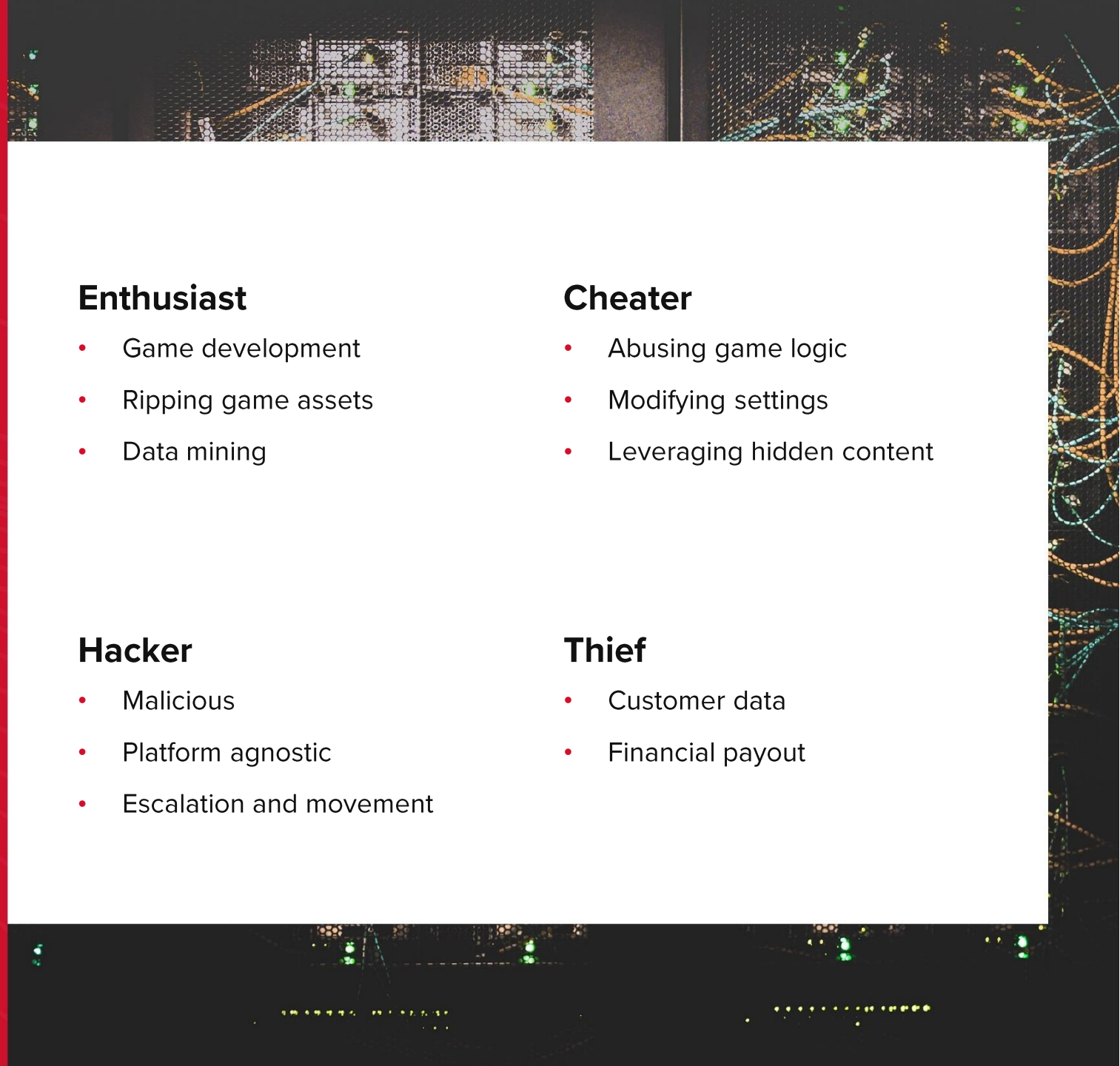
Attach to VM

- Mount and explore filesystem
- Cannot monitor active services



Threats

Threats



Enthusiast

- Game development
- Ripping game assets
- Data mining

Cheater

- Abusing game logic
- Modifying settings
- Leveraging hidden content

Hacker

- Malicious
- Platform agnostic
- Escalation and movement

Thief

- Customer data
- Financial payout

Threats

GAMER

HACKER

THIEF

Discoveries

Smart Smacker

Andamiro

Release Date:

2014

Game:

Trivia

Smart Smacker

```
root@mrjackpots:~# nmap -Pn 192.168.183.136
Starting Nmap 7.70 ( https://nmap.org ) at
2021-10-05 20:36 EDT
Nmap scan report for 192.168.183.136
Host is up (0.0058s latency).
All 1000 scanned ports on 192.168.183.136
are closed
MAC Address: 00:0C:29:17:8D:DC (VMware)

Nmap done: 1 IP address (1 host up) scanned
in 3.11 seconds
```

Smart Smacker - Filesystem

```
root@mrjackpots:/mnt# mount /dev/sdb1 /mnt/andamiro_smartsmacker/

root@mrjackpots:/mnt# ls andamiro_smartsmacker/
bin  boot  dev  etc  home  initrd.img  lib  lost+found  media  mnt  opt  proc
root  sbin  selinux  Smart_Smacker  srv sys  tmp  usr  var  vmlinuz

root@mrjackpots:/mnt/andamiro_smartsmacker/# cat etc/issue
Debian GNU/Linux 6.0 \n \l
```

Smart Smacker - Game Directory

```
# cat etc/rc.local
#!/bin/sh -e
[TRUNCATED]

cd /Smart_Smacker
./usbdaemon
xinit ./Global xterm -- -s 0 -dpms

exit 0
```

```
# ls -lah Smart_Smacker/
total 2.7M
drwxr-xr-x  6 root root 4.0K Dec 17  2012 .
drwxr-xr-x 22 root root 4.0K Jun 27  2011 ..
-rwxr-xr-x  1 root root 2.6M Dec 14  2012 Global
drwxr-xr-x  8 root root 4.0K Oct 11  2011 graphic
drwxr-xr-x  7 root root 4.0K Dec 14  2012 level
drwxr-xr-x  3 root root 4.0K Oct 12  2011 resource
-rw-rw-rw-  1 root root  200 Mar 28 10:25 setup.dat
drwxr-xr-x 20 root root 4.0K Oct 12  2011 sound
-rwxr-xr-x  1 root root  57K Jun 27  2011 usbdaemon
```

Smart Smacker - USB Key

```
# strings usbdaemon
[TRUNCATED]
null tables %d
/var/run/microdog
usbdaemon already running!!
/var/run/microdog/u.daemon
/dev/tty
[TRUNCATED]
SendBeginCodeandSerial
USBARandom
USBASendCommand
RXOneByteD
Send_HostID_Password_DogAddr_DogBytes
[TRUNCATED]
```

Smart Smacker - Game Directory

```
# ls -lah Smart_Smacker/
total 2.7M
drwxr-xr-x  6 root root 4.0K Dec 17  2012 .
drwxr-xr-x 22 root root 4.0K Jun 27  2011 ..
-rwxr-xr-x  1 root root 2.6M Dec 14  2012 Global
drwxr-xr-x  8 root root 4.0K Oct 11  2011 graphic
drwxr-xr-x  7 root root 4.0K Dec 14  2012 level
drwxr-xr-x  3 root root 4.0K Oct 12  2011 resource
-rw-rw-rw-  1 root root  200 Mar 28 10:25 setup.dat
drwxr-xr-x 20 root root 4.0K Oct 12  2011 sound
-rwxr-xr-x  1 root root  57K Jun 27  2011 usbdaemon
```

Smart Smacker - Game Assets

```
Smart_Smacker# ls -lah resource/
total 788M
drwxr-xr-x 3 root root 4.0K Oct 12  2011 .
drwxr-xr-x 6 root root 4.0K Dec 17  2012 ..
drwxr-xr-x 9 root root 4.0K Oct 12  2011 bga
-rwxr--r-x 1 root root 132M Oct 11  2011 resource0
-rwxr--r-x 1 root root 653M Apr 18  2012 resource3
-rwxr--r-x 1 root root 2.0M Oct 11  2011 system.fnt
-rwxr--r-x 1 root root 513K Oct 11  2011 system_small.fnt
```

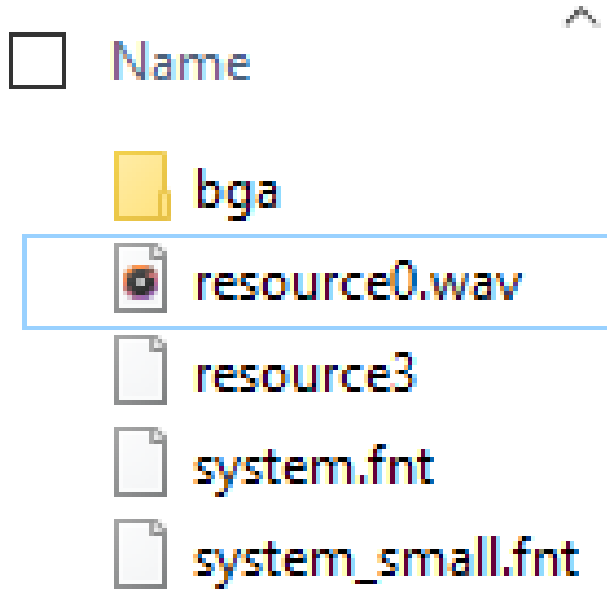
Smart Smacker - Game Audio

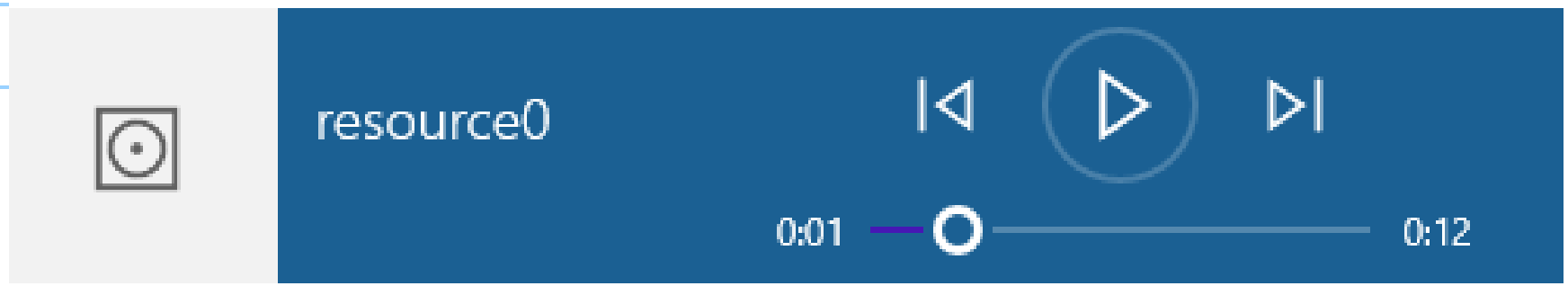
```
Smart_Smacker/resource# file resource0
resource0: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo
44100 Hz

Smart_Smacker/resource# xxd resource0
00000000: 5249 4646 24a4 2200 5741 5645 666d 7420  RIFF$."."WAVEfmt
00000010: 1000 0000 0100 0200 44ac 0000 10b1 0200  ........D.......
00000020: 0400 1000 6461 7461 00a0 2200 ffff 0300  ....data.."".....
00000030: 0200 feff feff 0100 0100 feff 0000 0200  ................
00000040: ffff ffff 0200 0100 fdff ffff 0300 ffff  ................
[TRUNCATED]
```

52 49 46 46 ?? ?? ?? ?? 57 41 56 45	RIFF????WAVE	0	wav	Waveform Audio File Format

https://en.wikipedia.org/wiki/List_of_file_signatures

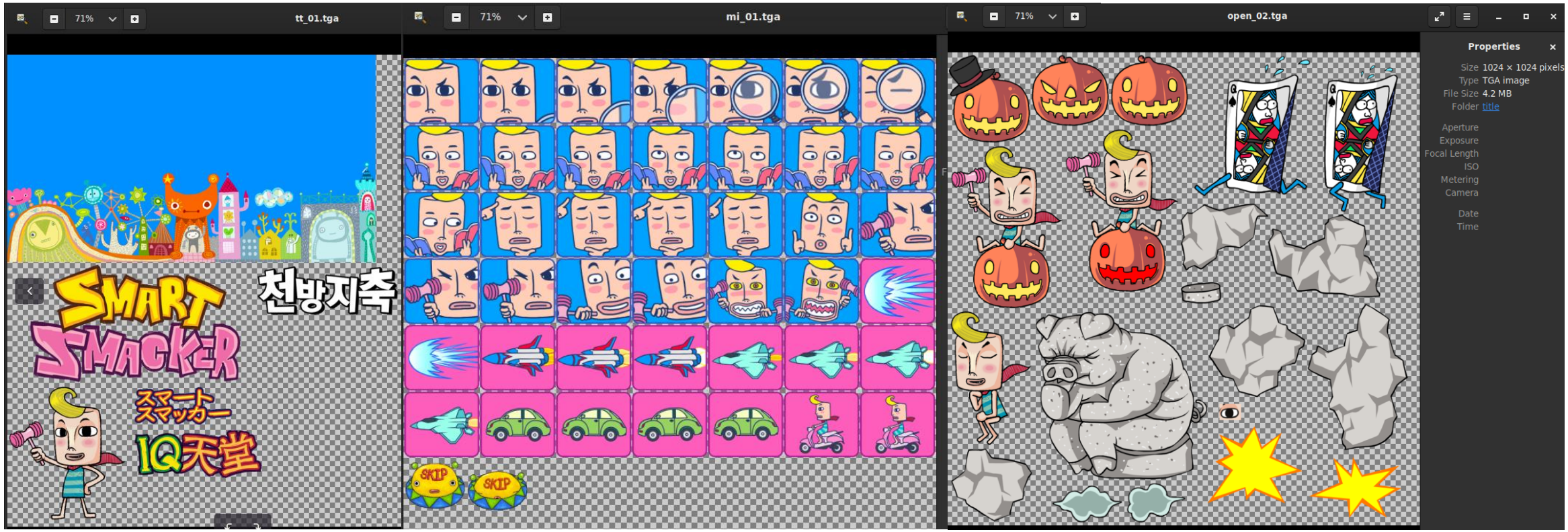
Smart Smacker - Game Audio





Smart Smacker - Game Audio

Smart Smacker - Game Art



Smart Smacker - Game Settings

```
Smart_Smacker/resource# ls level
chinese  english  japanese  korean  minigame_speed.txt   thailand

Smart_Smacker/resource# cat minigame_speed.txt
## 0(Very Fast ), 1( Fast ), 2( Normal ), 3( Slow ), 4( Very Slow

[illegible] = 0
[illegible] = 3
[illegible] = 0
[illegible] = 0
[illegible] = 2
[illegible] = 1
[illegible] = 0
[illegible] = 1
[illegible] = 3
[illegible] = 3
```

Smart Smacker - Game Settings

```
Smart_Smacker/level/english# ls -lah
[TRUNCATED]
drwxr-xr-x  2 root root 4.0K Oct 11  2011 glasswindow
drwxr-xr-x  2 root root 4.0K Oct 11  2011 halloween
drwxr-xr-x  2 root root 4.0K Oct 11  2011 hand_foot
drwxr-xr-x  2 root root 4.0K Oct 11  2011 icecream
[TRUNCATED]
```


```
Smart_Smacker/level/english# ls halloween/
easy.txt  hard.txt  normal.txt  very_easy.txt  very_hard.txt
```

Smart Smacker - Game Settings

Smart_Smacker/level/english# cat halloween/very_hard.txt

```
## Halloween.txt - 2010/11/24 - 15:45 Write

Test_Mode = S
## S : ◘ø◘◘, C : L◘ø◘◘, R : ◘◘◘◘◘◘◘

Test_Level = 0
## 0 ~ 9


Time_Limit_S = 1000 / 1000 / 1000 / 1000 / 1000 / 1000 / 1000 / 1000 / 1000 / 1000
Time_Limit_C = 1000 / 1000 / 1000 / 1000 / 1000 / 1000 / 1000 / 1000 / 1000 / 1000
## ◘◘◘◘ ◘ð◘ S-◘◘, C-L◘◘ (1/100◘◘)

Question_S = 30 / 30 / 35 / 35 / 40 / 40 / 45 / 45 / 50 / 50
Cut_Line_S = 35 / 40 / 45 / 55 / 60 / 65 / 70 / 72 / 78 / 80
## ◘◘ ◘◘◘◘ ◘◘◘◘ ◘◘, L[◘◘◘◘

Question_C = 30 / 30 / 35 / 35 / 40 / 40 / 45 / 45 / 50 / 50
Cut_Line_C = 35 / 40 / 45 / 55 / 60 / 65 / 70 / 72 / 78 / 80
## L◘◘ ◘◘◘◘ ◘◘◘◘ ◘◘, L[◘◘◘◘

Appear_Type = 0 / 0 / 1 / 1 / 2 / 2 / 3 / 3 / 3 / 3
## ◘◘◘ ◘◘◘◘ ◘◘◘◘(0 ~ 3 ◘◘◘◘) (0 - ◘◘◘◘, 1 - ◘밟◘◘ ◘◘◘, 2 - ◘◘◘ ◘◘ ◘◘◘◘, 3 - ◘◘◘ ◘◘◘◘ ◘◘◘)

Move_Speed = 0 / 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9
## ◘◘◘ ◘◘ ◘◘◘ (0 ~ 9 ◘◘◘◘)
```

https://www.youtube.com/watch?v=mtMy6vrSJQw

Jurassic Park

Raw Thrills

Release Date:

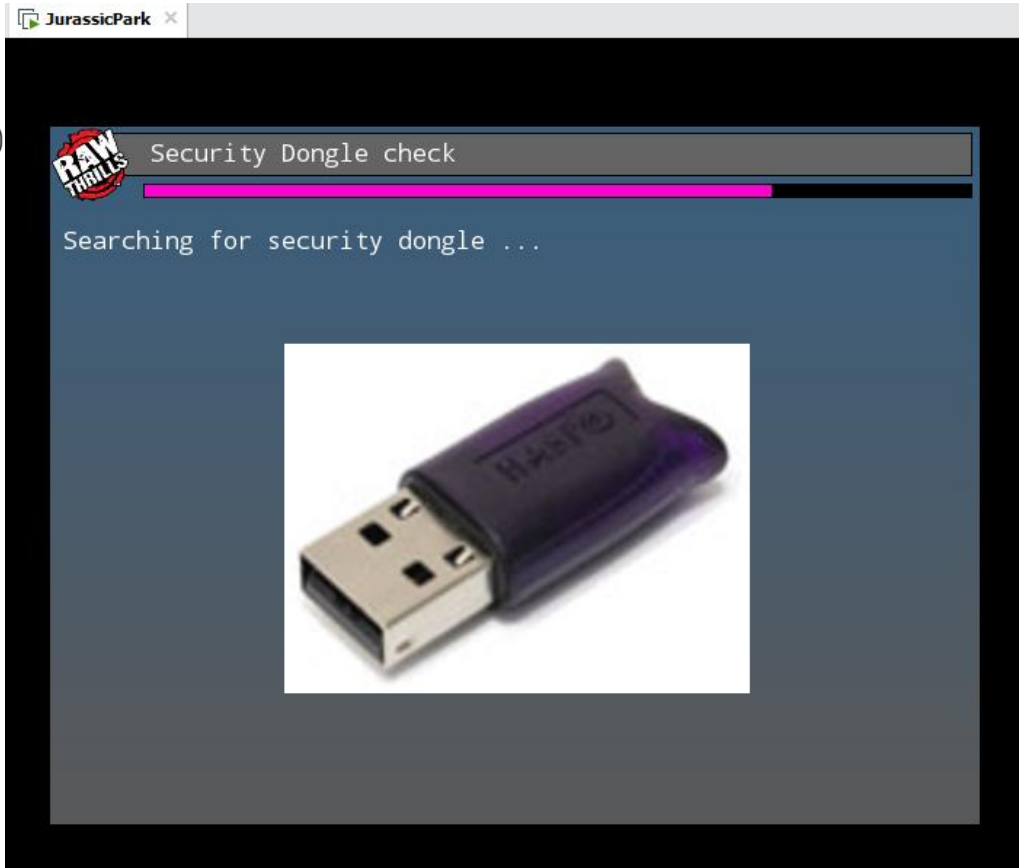
2015

Game:

Rail Shooter

Jurassic Park - Network

```
root@mrjackpots:~# nmap -Pn 192.168.183.135
Starting Nmap 7.70 ( https://nmap.org ) at 2021-0
Nmap scan report for 192.168.183.135
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1947/tcp open  sentinelsrm
MAC Address: 00:0C:29:B8:91:11 (VMware)
```



Jurassic Park - Network

```
root@mrjackpots:~# smbclient -U "" -L 192.168.183.135
Enter WORKGROUP\'s password:

    Sharename       Type      Comment
    ---------       ----      -------
    driveroot       Disk
    pm              Disk
    pm_collection   Disk
    IPC$            IPC       IPC Service (raw-production server (Samba,
                              Ubuntu))
```

Jurassic Park - Network

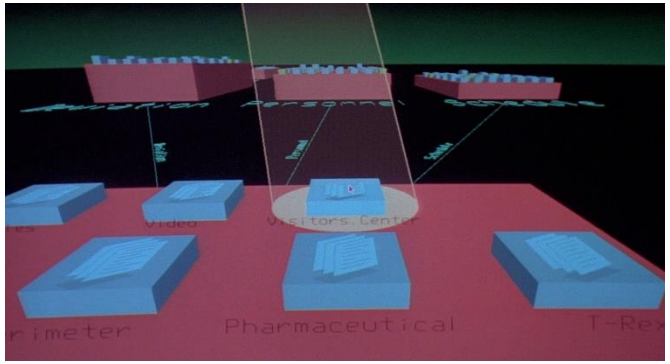
```
root@mrjackpots:~# nmap --script smb-enum-users -p445 192.168.183.135
[TRUNCATED]
Host script results:
| smb-enum-users:
|   RAW-PRODUCTION\raw (RID: 1000)
|     Full name:   raw
|     Description:
|     Flags:       Normal user account
|   RAW-PRODUCTION\root (RID: 1001)
|     Full name:   root
|     Description:
|_    Flags:       Normal user account

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
```

Jurassic Park - Network

```
root@mrjackpots:~# smbclient -U "raw" \\\\192.168.183.135\\driveroot
Enter WORKGROUP\raw's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jan 29 19:03:42 2018
  ..                                  D        0  Mon Jan 29 19:03:42 2018
  pm                                  D        0  Sun Sep  5 20:08:32 2021
  boot                                D        0  Mon Jan 29 16:44:41 2018
  run                                 D        0  Mon Sep 20 20:23:08 2021
  [TRUNCATED]
        24639868 blocks of size 1024. 14341832 blocks available
smb: \> cd pm
smb: \pm\> ls
NT_STATUS_ACCESS_DENIED listing \pm\*
```

Jurassic Park - Network

```
root@mrjackpots:~# ssh raw@192.168.183.135
raw@192.168.183.135's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

407 packages can be updated.
352 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Tue Sep 21 00:23:08 2021 from 192.168.183.139
raw@raw-production:~$ whoami
raw
```



Jurassic Park - Escalation

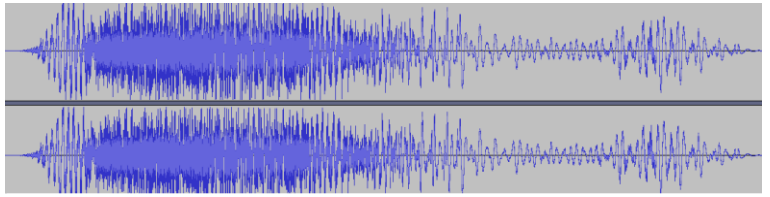
```
raw@raw-production:~$ sudo -l
sudo: unable to resolve host raw-production
[sudo] password for raw:
Matching Defaults entries for raw on raw-production:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User raw may run the following commands on raw-production:
    (ALL : ALL) ALL

raw@raw-production:~$ sudo -i
sudo: unable to resolve host raw-production
root@raw-production:~# id
uid=0(root) gid=0(root) groups=0(root),123(pulse-access)
```

Jurassic Park - Filesystem

```
root@raw-production:/# ls -lah
[TRUNCATED]
drwxr-xr-x 135 root root  12K Sep 20 22:10 etc
lrwxrwxrwx   1 root root    3 Jan 30  2018 g3 -> /pm
drwxr-xr-x   3 root root 4.0K Oct 30  2016 home
drw-rw-rw-   4 root root 4.0K Sep  6 00:08 pm
[TRUNCATED]
drwxr-xr-x  14 root root 4.0K Oct 31  2016 var
lrwxrwxrwx   1 root root   29 Oct 30  2016 vmlinuz -> boot/vmlinuz-4.4.0-31-
generic

root@raw-production:/pm# ls
dinocrc.txt  dinofiles.txt  g5  game  game_china  utils  version.txt
```

Jurassic Park - Filesystem

```
root@raw-production:/pm# cat dinofiles.txt
./dinofiles.txt
./g5/dino/data/adj/core/defs/coin/coin0Value.txt
./g5/dino/data/adj/core/defs/coin/coin1Value.txt
[TRUNCATED]
./g5/dino/data/snd/rumble/sounds/TrainCar_Switching_Rumble.wav
./g5/dino/data/snd/rumble/sounds/TreeLog_DinoImpactSloMo_Rumble.wav
./g5/dino/data/snd/rumble/sounds/TRex_Branch1_Rumble.wav
./g5/dino/data/snd/rumble/sounds/TRex_Chomp2_Rumble.wav
./g5/dino/data/snd/rumble/sounds/TRex_ChompRoar_Rumble.wav
[TRUNCATED]
```



Jurassic Park - Game Configuration

```
root@raw-production:/pm/g5/dino/data# ls -w 90
adj                 conf    GeneralPurposeStateMachine.txt  postfx              snd
AnisoSpecTex.ppm    cpmgui  glcgz                           programs_enc        SpecTex.ppm
attract             dialog  locales                         programs_enc_china  Thumbs.db
aud                 g5      pemitters                       scenes              translation

root@raw-production:/pm/g5/dino/data/conf# cat animals/trex/trex_travelanims.txt
########## runs
[TRUNCATED]
-- 7.816 ft (maya cm units) per second:
-- 5.74 mph
tanims[0].name = trex_run_v1
tanims[0].cycle_length = 150.0
tanims[0].units_traveled_per_cycle = 19.54
tanims[0].turn_radius = 0.0
```

Jurassic Park - Game Configuration

```
root@raw-production:/pm/g5/dino/data/conf# cat gameconf.txt
[TRUNCATED]
gun_shots_per_second = 10
gun_vol_start = 210.0
gun_vol_end = 70.0
gun_vol_time = 5.0
[TRUNCATED]
player_health = 15
[TRUNCATED]
raptor_health = 4
raptor_multiplayer_health_multiplier = 2.0
raptor_grapple_health_multiplier = 2.0
raptor_quick_attack_health_multiplier = 1.0
```

```
# these are overridden by the adjustments for now
dmg_cooldown_1player = 5
dmg_cooldown_2player = 5
dmg_cooldown_3player = 5
dmg_cooldown_4player = 5
```

Jurassic Park - Filesystem

```
root@raw-production:/pm# cat dinofiles.txt
./dinofiles.txt
./g5/dino/data/adj/core/defs/coin/coin0Value.txt
./g5/dino/data/adj/core/defs/coin/coin1Value.txt
[TRUNCATED]
./g5/dino/data/snd/rumble/sounds/TRex_Branch1_Rumble.wav
./g5/dino/data/snd/rumble/sounds/TRex_Chomp2_Rumble.wav
./g5/dino/data/snd/rumble/sounds/TRex_ChompRoar_Rumble.wav
[TRUNCATED]
root@raw-production:/pm# grep gameconf dinocrc.txt dinofiles.txt
dinocrc.txt:./g5/dino/data/conf/gameconf.txt, 3380, 1758768550
dinofiles.txt:./g5/dino/data/conf/gameconf.txt
```

Jurassic Park - Game Settings


```
root@raw-production:/pm/g5/dino/data/adj# ls */*
core/defs:
coin  datetime  main  sound

core/luts:
attractSoundFreqs.txt  language.txt  onOff.txt
currencyTypes.txt      months.txt

game/defs:
game  hardware  playerCost  sound

game/luts:
attractSoundFreqs.txt  friendlyFire.txt
cabType.txt            vibrateGuns.txt
difficulty.txt
```

https://www.youtube.com/watch?v=OU5FZwfvYSg

Jurassic Park - Game Settings

https://www.youtube.com/watch?v=OU5FZwfvYSg

/pm/g5/dino/data/adj/game/defs/playerCost/gamecost.txt

```
[TRUNCATED]
name                    = gamecost
version                 = 0
online_reconcile        = 1
default_value           = 100
min                     = 0
max                     = 2000000000
divisor                 = 100
step_value              = 25
displayAsTime           = 0
displayAsDate           = 0
displayAsCurrency       = 1
displayAsPercentage     = 0
displayPriority         = 2
```

Jurassic Park - Motion Settings

https://www.youtube.com/watch?v=l7fTwRMvam4

```
/pm/g5/dino/data/adj/game/defs# ls hardware/
cabinetMotion.txt    motionTilt.txt
cabType.txt          rumble.txt
lamps.txt            vehicleMotion.txt
motionHeight.txt     vibrateGunsEnable.txt
motionPitch.txt      vibrateGuns.txt
motionStrength.txt

hardware/motionStrength.txt
[TRUNCATED]
name                 = motionStrength
version              = 0
online_reconcile     = 1
default_value        = 50
min                  = 0
max                  = 100
divisor              = 0
step_value           = 10
displayPriority      = 30
```

Jurassic Park - Source?

```
root@raw-production:/pm/g5# grep -ri adj *
dino/src/src/gameflow_records.h:  float startDmgAdjustAfterDmg;
dino/src/src/gameflow_records.h:  float startDmgAdjustAfterTime;
dino/src/src/gameflow_records.h:  // difficulty value set in the adjustments menu
dino/src/src/gameflow_records.h:  float difficultyAdj;
dino/src/src/gameflow_records.h:float GameFlow_Get_DifficultyAdj();

root@raw-production:/pm/g5/dino/src/src# ls -w 100
[TRUNCATED]
crawlerbug_statemachine.h   game_proc.h                 ptrdon.h
credit_msg.h                game_qr.h                   ptrdon_sm.h
credits.h                   game_results.h              raptor_general.h
dino_agent.h                game_rtdt_datatypes.h       raptor_ggg_statemachine.h
dino_group.h                game_score_ggg.h            raptor_statemachine.h
dino_trigger_group.h        game_score.h                screenbug_statemachine.h
[TRUNCATED]
```

Jurassic Park - Source Code

raptor_general.h

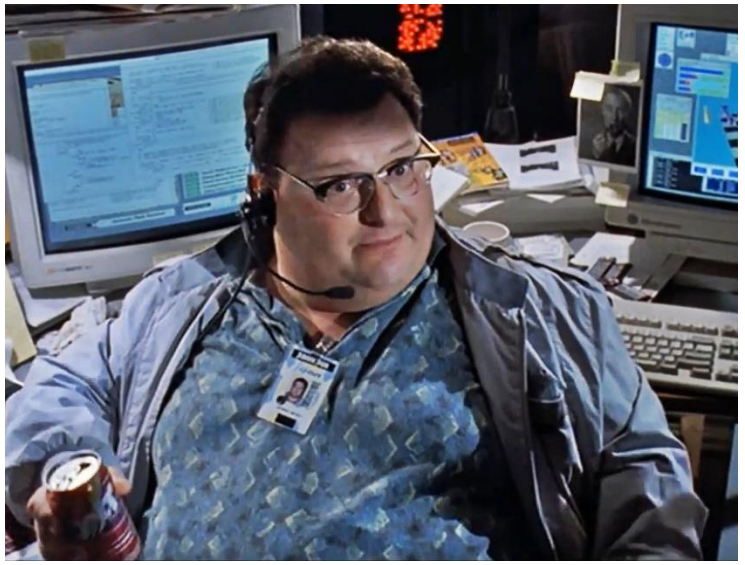
```
// primary data struct
typedef struct RaptorData
{
    RaptorModelData * rmd;    // model specific info
    int model;                // raptor or dilo
    int type;                 // type of raptor behavior
    int state;                // main raptor state
    float start_time;
    char start_trigger[SM_NAME_SIZE];
    char end_trigger[SM_NAME_SIZE];
    char killed_trigger[SM_NAME_SIZE]; // when raptor is killed, send this out
    float start_cam_time; // if we keep same camera while waiting to start - use this to start raptor
    uns32 start_cam_oid;      // this is the camera we are watching to decide to start
    float start_delay;        // If start camera changes, just use a normal timer to start the raptor
    float idle_delay;
    float end_delay; // delay before killing with end trigger
    int min_players; // how many players need to be in game for this guy to be allowed to spawn
    [TRUNCATED]
```

Jurassic Park - Source Code

```
root@raw-production:/pm/g5/dino/src/src# ls -w 100
attract.h                    gameflow_records.h           level_select3.h
aud_game.h                   game_gun_beam.h              level_select_ggg.h
autoplay.h                   game_gun_electro.h           level_select.h
boot.h                       game_gun_freeze.h            level_success.h
bullet_sm.h                  game_gun_grenade.h           location_diag.h
cera_group.h                 game_gun.h                   movie_text.h
cera_statemachine.h          game_gun_mg.h                mraptor_statemachine.h
circles_result.h             game_gun_minigun.h           obs_shoot_general.h
circles_tutorial.h           game_gun_rocket.h            obs_shoot_statemachine.h
compy_general.h              game_gun_shotgun.h           placeholder_statemachine.h
compyspline_statemachine.h   game_gun_tracker.h          progress_map.h
compy_statemachine.h         game.h                       ptrdon_global.h
copyright.h                  game.h.gch                   ptrdon_grp.h
crawlerbug_statemachine.h    game_hud.h                   ptrdon_grp_sm.h
credit_msg.h                 game_player.h                ptrdon.h
credits.h                    game_proc.h                  ptrdon_sm.h
dino_agent.h                 game_qr.h                    raptor_general.h
dino_group.h                 game_results.h               raptor_ggg_statemachine.h
dino_trigger_group.h         game_rtdt_datatypes.h        raptor_statemachine.h
emergency_stop.h             game_score_ggg.h             screenbug_statemachine.h
[TRUNCATED]
```

Jurassic Park - Source Code

```
root@raw-production:/pm/g5/g5engine/src/g5# find . -type f | xargs wc -l
    [TRUNCATED]
    73 ./game_core.h
 20518 total

root@raw-production:/pm/g5/dino/src# find . -type f | xargs wc -l
 [TRUNCATED]
    27 ./src/trex_sm.h
    25 ./src/wasp_swarm_statemachine.h
   138 ./src/mraptor_statemachine.h
7250 total
```



Jurassic Park (2015): 27,768 Lines of Code

...network & connection machines and debug 2 million lines of code...
-Dennis Nedry

“Game Disc”

Release Date:

2000-2010

Game:

Ticket Redemption

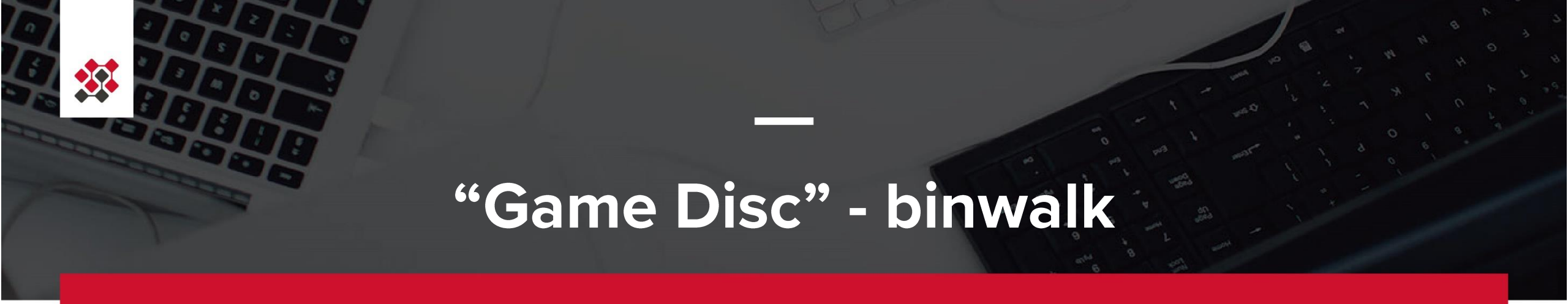
“Game Disc” - Disc Contents

```
/mnt/boot$ ls -lah
total 6.0M
drwxrwxrwt 6 400 401 2.0K Oct 27  2008 .
drwxrwxrwt 4 400 401 2.0K Oct 27  2008 ..
-rwxrwxrwx 1 400 401 1.7K Aug  7  2007 bootinst.bat
-rwxrwxrwx 1 400 401 2.1K Aug  7  2007 bootinst.sh
-rwxrwxrwx 1 400 401 2.4K Aug  7  2007 bootlilo.sh
-rwxrwxrwx 1 400 401 3.6K Aug  7  2007 chain.c32
drwxrwxrwt 2 400 401 2.0K Oct 27  2008 dos
-rwxrwxrwx 1 400 401 1.9M Aug  7  2007 initrd.gz
drwxrwxrwt 2 400 401 2.0K Oct 27  2008 isolinux
-rwxrwxrwx 1 400 401  93K Aug  7  2007 mt86p
drwxrwxrwt 2 400 401 2.0K Feb  2  2009 [REDACTED]
drwxrwxrwt 2 400 401 2.0K Oct 27  2008 syslinux
-rwxrwxrwx 1 400 401 112K Aug  7  2007 vesamenu.c32
-rwxrwxrwx 1 400 401 3.9M Aug  7  2007 vmlinuz
```

“Game Disc” - Partitions

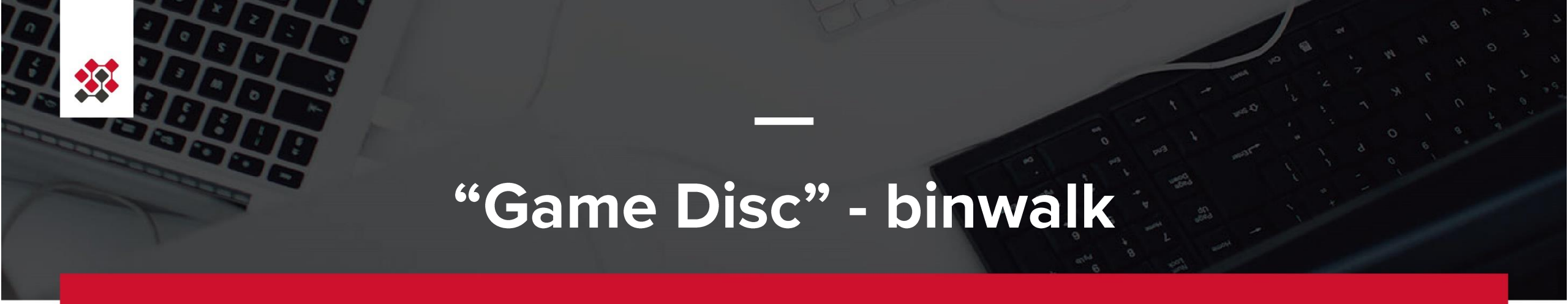
```
/mnt/boot/[REDACTED]$ ls -lah
total 2.5G
drwxrwxrwt 2 400 401 2.0K Feb  2  2009 .
drwxrwxrwt 6 400 401 2.0K Oct 27  2008 ..
-rwxrwxrwx 1 400 401 480K Dec 14  2004 dfsee
-rwxrwxrwx 1 400 401  148 Dec 22  2004 dfsee.key
-rwxrwxrwx 1 400 401 2.8K Feb  2  2009 lvm.pd1
-rwxrwxrwx 1 400 401 931M Feb  2  2009 part0.imz
-rwxrwxrwx 1 400 401 1.5G Feb  2  2009 part1.imz
-rwxrwxrwx 1 400 401 169M Feb  2  2009 part2.imz
-rwxrwxrwx 1 400 401  118 Aug 16  2007 restore2.dfs
-rwxrwxrwx 1 400 401   35 Aug 16  2007 restore.dfs
```

```
/mnt/boot/[REDACTED]$ cat restore2.dfs
part 1
fs aux
base -p:1
wrim /boot/[REDACTED]/part0
part 2
wrim /boot/[REDACTED]/part1
part 3
wrim /boot/[REDACTED]/part2
```



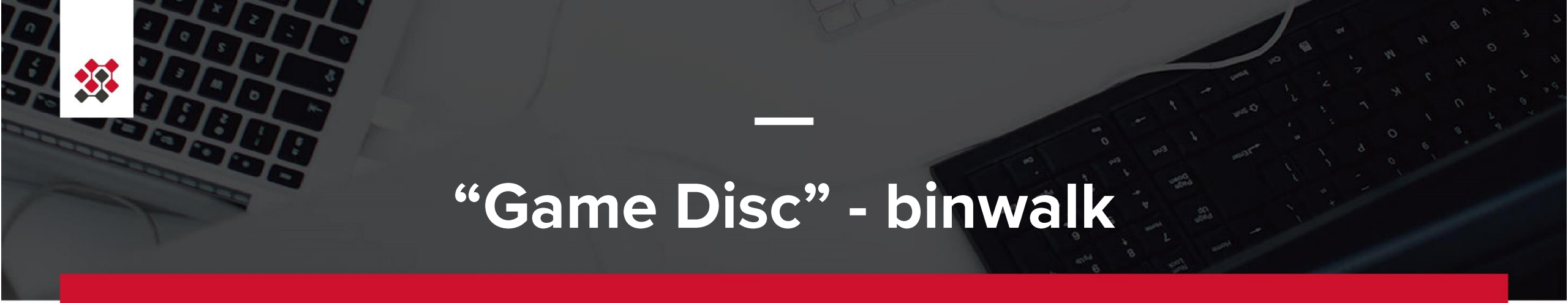
“Game Disc” - binwalk

```
/mnt/boot/[REDACTED]$ binwalk part0.imz

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
[TRUNCATED]
3925343       0x3BE55F        Unix path: /usr/local/bin:/bin:/usr/X11R6/bin:/usr/sbin:/sbin:/usr/bin;
3925787       0x3BE71B        Unix path: /lib/modules/2.6.24.2/kernel/drivers/usb/serial/pl2303.ko
3925912       0x3BE798        Unix path: /usr/src/rtinit/rtinit &> /dev/null
3926006       0x3BE7F6        Unix path: /usr/src/jamma/jamma w6
[TRUNCATED]
25170164      0x18010F4       bzip2 compressed data, block size = 900k
27025867      0x19C61CB       Zip archive data, at least v1.0 to extract, name:
www.example.com/httpdocs/data/example/invoices/
27025942      0x19C6216       Zip archive data, at least v2.0 to extract, compressed size: 915, uncompressed
size: 3436, name: www.example.com/httpdocs/data/example/invoices/invoice_1.html
27026946      0x19C6602       Zip archive data, at least v2.0 to extract, compressed size: 1478, uncompressed
size: 13567, name: www.example.com/httpdocs/data/example/invoices/invoice_10.html
27028514      0x19C6C22       Zip archive data, at least v2.0 to extract, compressed size: 2381, uncompressed
size: 28231, name: www.example.com/httpdocs/data/example/invoices/invoice_100.html
```



“Game Disc” - binwalk

```
$ binwalk --offset=0x19C61CB part0.imz
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
27025867      0x19C61CB       Zip archive data, at least v1.0 to extract, name:
www.example.com/httpdocs/data/example/invoices/
27025942      0x19C6216       Zip archive data, at least v2.0 to extract, compressed size: 915, uncompressed
size: 3436, name: www.example.com/httpdocs/data/example/invoices/invoice_1.html
[TRUNCATED]
uncompressed size: 28225, name: www.example.com/httpdocs/data/example/invoices/invoice_105.html
27043324      0x19CA5FC       Zip archive data, at least v2.0 to extract, compressed size: 1975, uncompressed
size: 21432, name: www.example.com/httpdocs/data/example/invoices/invoice_106.html
27080598      0x19D3796       gzip compressed data, maximum compression, has original file name: "fsck.8",
from Unix, last modified: 2003-08-12 18:46:12
27082250      0x19D3E0A       gzip compressed data, maximum compression, has original file name: "e2image.8",
from Unix, last modified: 2003-08-12 18:46:12
[TRUNCATED]
27101087      0x19D879F       Zip archive data, at least v2.0 to extract, compressed size: 1189, uncompressed
size: 8054, name: www.example.com/httpdocs/data/example/invoices/invoice_112.html
```



“Game Disc” - binwalk

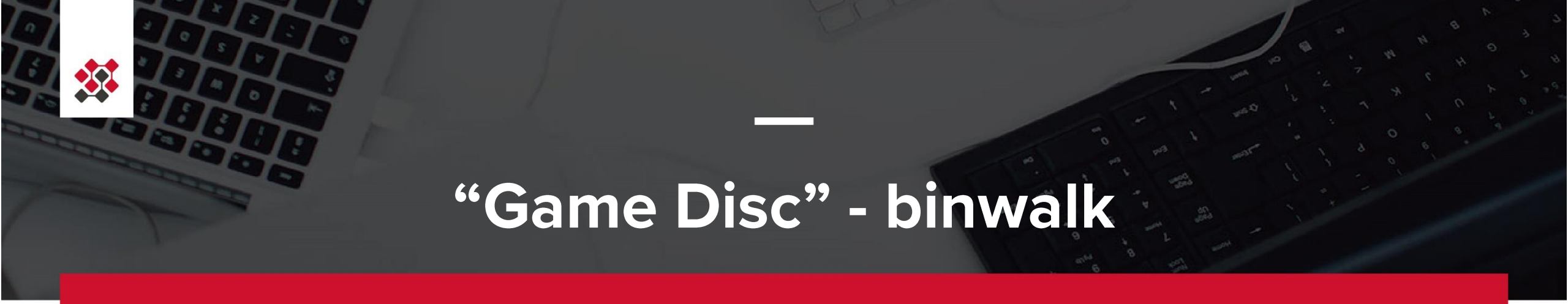
```
$ binwalk --offset=0x19C61CB part0.imz | grep example| wc -l
632
```

```
$ binwalk --offset=0x19C61CB part0.imz | egrep “compressed.*example”
27025867      0x19C61CB       Zip archive data, at least v1.0 to extract, name:
www.example.com/httpdocs/data/example/invoices/
27025942      0x19C6216       Zip archive data, at least v2.0 to extract, compressed size: 915, uncompressed
size: 3436, name: www.example.com/httpdocs/data/example/invoices/invoice_1.html
27026946      0x19C6602       Zip archive data, at least v2.0 to extract, compressed size: 1478, uncompressed
size: 13567, name: www.example.com/httpdocs/data/example/invoices/invoice_10.html
```

```
$ …egrep "compressed.*example" | awk -F'[ \t,]+' '{print "--offset=" $2 " --length=" $13}'
--offset=0x19C6216 --length=915
--offset=0x19C6602 --length=1478

$ … | xargs -n5 binwalk -e part0.imz --directory "/tmp/" --rm
```

“Game Disc” - binwalk

```
$ binwalk --offset=0x19C61CB part0.imz | grep example| wc -l
632

$ binwalk --offset=0x19C61CB part0.imz | egrep “compressed.*example”
27025867      0x19C61CB       Zip archive data, at least v1.0 to extract, name:
www.example.com/httpdocs/data/example/invoices/
27025942      0x19C6216       Zip archive data, at least v2.0 to extract, compressed size: 915, uncompressed
size: 3436, name: www.example.com/httpdocs/data/example/invoices/invoice_1.html
27026946      0x19C6602       Zip archive data, at least v2.0 to extract, compressed size: 1478, uncompressed
size: 13567, name: www.example.com/httpdocs/data/example/invoices/invoice_10.html

$ … egrep "compressed.*example" | awk -F'[ \t,]+' '{print "--offset=" $2 " --length=" $13}'
--offset=0x19C6216 --length=915
--offset=0x19C6602 --length=1478

$ … | xargs -n5 binwalk -e part0.imz --directory "/tmp/" --rm
```



“Game Disc” - binwalk

```
$ binwalk --offset=0x19C61CB part0.imz | grep example| wc -l
632

$ binwalk --offset=0x19C61CB part0.imz | egrep “compressed.*example”
27025867      0x19C61CB       Zip archive data, at least v1.0 to extract, name:
www.example.com/httpdocs/data/example/invoices/
27025942      0x19C6216       Zip archive data, at least v2.0 to extract, compressed size: 915, uncompressed
size: 3436, name: www.example.com/httpdocs/data/example/invoices/invoice_1.html
27026946      0x19C6602       Zip archive data, at least v2.0 to extract, compressed size: 1478, uncompressed
size: 13567, name: www.example.com/httpdocs/data/example/invoices/invoice_10.html

$ … egrep "compressed.*example" | awk -F'[ \t,]+' '{print "--offset=" $2 " --length=" $13}'
--offset=0x19C6216 --length=915
--offset=0x19C6602 --length=1478

$ … xargs -n5 binwalk -e part0.imz --directory "/tmp/" --rm
```

“Game Disc” - binwalk

COMMAND:

```
$ binwalk --offset=0x19C61CB part0.imz | egrep "compressed.*example" |
    awk -F'[ \t,]+' '{print "--offset=" $2 " --length=" $13}' |
    xargs -n5 binwalk -e part0.imz --directory "/tmp/" -rm
```

TRANSLATION:

```
$ binwalk -e part0.imz --directory "/tmp" --rm --offset=0x19C6216 --length=915
$ binwalk -e part0.imz --directory "/tmp" --rm --offset=0x19C6602 --length=1478
$ binwalk -e part0.imz --directory "/tmp" --rm --offset=0x19C6C22 --length=2381
```

“Game Disc” - Web Directory

```
example/httpdocs/includes$ ls -w 100
advertisements_search.php           google_map.php                  report_tournaments.php
auth.php                            help.php                        state_options.html
bill_account_summary.php            js                              steps.php
bill_report.php                     locations_delete.php            tabs.php
bill_send.php                       locations_import.php            templates
bill_send_print.php                 locations_tabs.php              tournament_details.php
bill_transaction_history_print.php  login.php                       tournaments_button.php
[TRUNCATED]
games_my.php                        player_form.php                 tournaments_form_simple6.php
games_patch.php                     player_profile.php              tournaments_join2.php
games_settings_dropdown.php         report_locations.php            tournaments_join_confirm.php
games_tabs.php                      report_machine_diag.php         tournaments_join.php
games_tournaments_list.php          report_player_adv.php           tournaments_prizes.php
global_footer.html                  report_player_bests.php         tournaments_summary.php
global_header.html                  report_player_bonus.php         updates_[REDACTED]
global_nav_dummy.html               report_play_location.php        uploads
global_nav.html                     report_play_machine.php
global_vars.php                     report_purchases_location.php
```

“Game Disc” - Extracted Content

```
smenu4">View/Edit Game Machines</a></div>
&menu=smenu4">My Game Defaults</a></div>
enu4">Add Game Machines</a></div>
nu=smenu4">Change Settings</a></div>


u=smenu4">List Factory Defaults</a></div>
smenu4">Add Factory Defaults</a></div>

smenu4">Upload Patch</a></div>



script:void(null)'>Tournaments</a></div>


enu=smenu5">Create Tournament</a></div>
enu=smenu5&R1=V1">Join Tournament</a></div>

enu=smenu5">Copy Tournament</a></div>

&menu=smenu5">View/Edit Tournaments</a></div>
```

```
$settings['Violence']['1'] = 'Normal';
$settings['Violence']['2'] = 'No Blood';
```

Invoice

[redacted]

DATE	INVOICE #	DUE DATE
03-14-08	90	03-29-08

BILL TO
[redacted] PA 15330

BILLING CYCLE
02-01-08 — 02-29-08

DATE	DESCRIPTION	QTY	RATE	AMOUNT
02-01-08	Custom Contest Play	7	$0.50	$3.50
02-01-08	Trophy Club Play	2	$0.50	$1.00
02-02-08	Custom Contest Play	7	$0.50	$3.50
02-02-08	Trophy Club Play	2	$0.50	$1.00
02-05-08	Custom Contest Play	1	$0.50	$0.50

Wheel of Fortune

Raw Thrills

Release Date:

2010

Game:

Ticket Redemption

Wheel of Fortune

Wheel of Fortune - Filesystem

```
root@mrjackpots:/mnt/wof# ls -w 100
bin   dev  g3   lib         media  opt  proc   root  selinux sys  usr
boot  etc  home  lost+found  mnt    pm   rawsrc  sbin  srv tmp  var

root@mrjackpots:/mnt/wof# ls -lah pm/
total 8.0K
drwxr-xr-x  2 root root 4.0K Sep 21  2011 .
dr-xr-xr-x 24 root root 4.0K Mar 11  2014 ..
root@mrjackpots:/mnt/wof# ls -lah rawsrc/
total 12K
drwxr-xr-x  3 root root 4.0K Mar 10  2014 .
dr-xr-xr-x 24 root root 4.0K Mar 11  2014 ..
drwxr-xr-x  2 root root 4.0K Mar 10  2014 dipsw
```

Wheel of Fortune - Filesystem

```
root@mrjackpots:/mnt/wof/rawsrc/dipsw# ls -w 110
check_warm_boot.sh  gun_flash_serial.sh      run_game           wifi_detect.sh
device_open         open_modem_ctrtl_port.sh sierralink.sh      wifi_setup.sh
eth.sh              ppp.sh                   therm_detect.sh    wmdbi_detect.sh
go                  reset_usb_bus.sh         volup.sh           wof_hw_check.sh

root@mrjackpots:/mnt/wof/rawsrc/dipsw# cat wof_hw_check.sh
#!/bin/sh
# check for the touch monitor

while [ 1 ]; do

    num_monitors=0
    need_monitors=1
```

Wheel of Fortune - Filesystem

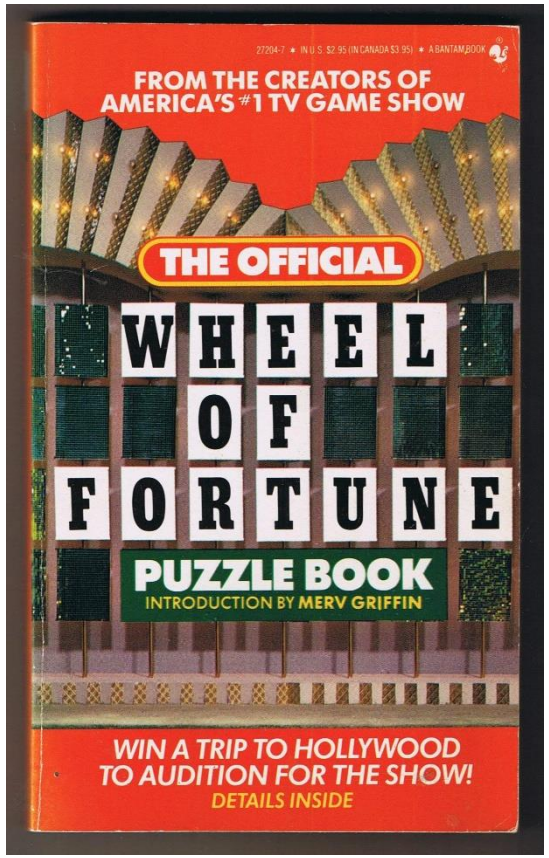
```
root@mrjackpots:/mnt/wof/root# cat .bash_history
tar -zxvf snx_V2.0.1.0.tar.gz
cd snx
make clean
make
make install
vi /rawsrc/dipsw/go
cd /pm
./strip-DEV.sh
dmesg
[TRUNCATED]

make
make clean
make 2> [OOPS]
vi [OOPS]
make clean; make 2>
[OOPS]
vi [OOPS]
make clean
make
make clean; make 2>
[OOPS]
vi [OOPS]
make clean; make 2>

cp rc.local [OOPS].sh
vi [OOPS].sh
./[OOPS].sh
cd /root
vi .bashrc
reboot
vi /root/.bashrc
rm -rf /wofvuser/
killall xscrensaver
killall xscreensaver
make clean; make -j
rm -rf /wofvuser/
./game

./game
gdb game
```

Wheel of Fortune - Filesystem

```
root@mrjackpots:/mnt/wof/var/log# grep "/pm" *
anaconda.log:06:18:53,932 DEBUG    : isys.py:mount()- going to mount /dev/sda2 on
/mnt/sysimage/pm as ext4 with options defaults
anaconda.program.log:Running... /bin/mount -n -t ext4 -o defaults /dev/sda2
/mnt/sysimage/pm
anaconda.storage.log:  mountpoint = /pm  mountopts = None

root@mrjackpots:/mnt/wof/var/log# mount /dev/sdb2 /mnt/wof/pm/^C
root@mrjackpots:/mnt/wof# cd pm/
root@mrjackpots:/mnt/wof/pm# ls
game  version.txt  wofvdata
```

Wheel of Fortune - Filesystem

```
root@mrjackpots:/mnt/wof/pm/wofvdata# ls -l
total 24
drwxr-xr-x 2 root root 4096 May  2  2012 cf
drwxr-xr-x 2 root root 4096 Nov 25  2013 docs
drwxr-xr-x 2 root root 4096 Nov 12  2012 hd_pc
drwxr-xr-x 3 root root 4096 May  2  2012 snd
drwxr-xr-x 2 root root 4096 May  2  2012 ssl
drwxr-xr-x 2 root root 4096 May  2  2012 xml

root@mrjackpots:/mnt/wof/pm/wofvdata# ls docs/
puzzles_eur.txt  puzzles.txt
```

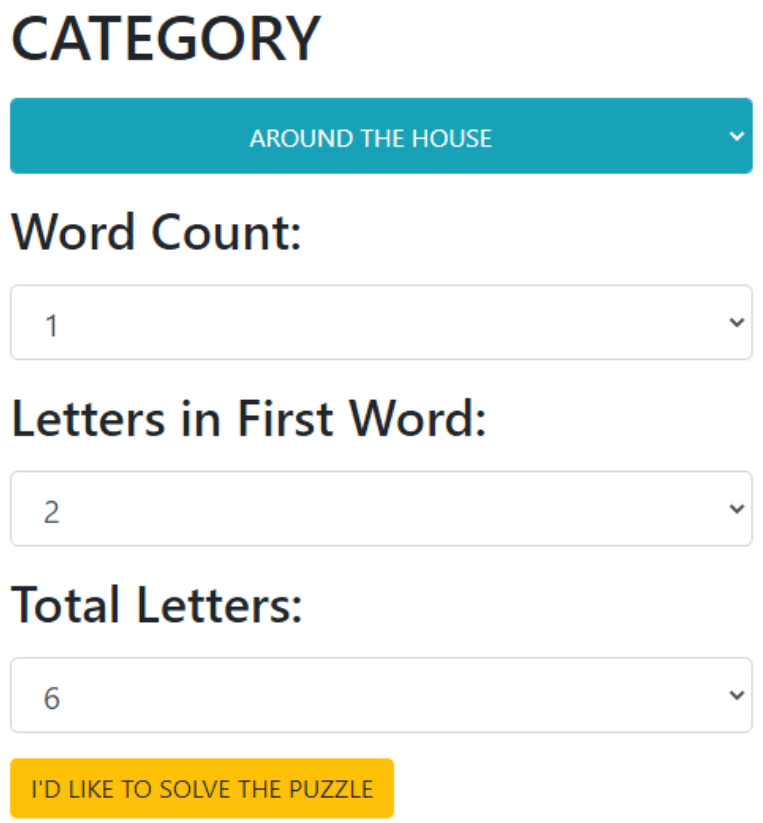


Wheel of Fortune - Puzzles

```
root@mrjackpots:/mnt/wof/pm/wofvdata# head docs/puzzles.txt
AROUND THE HOUSE,ADDRESS LABELS
AROUND THE HOUSE,AFGHAN RUG
AROUND THE HOUSE,AIR FRESHENER
AROUND THE HOUSE,ALARM CLOCK
AROUND THE HOUSE,APPOINTMENT BOOK
AROUND THE HOUSE,AREA RUG
AROUND THE HOUSE,AUTOMATIC GARAGE DOOR OPENER
AROUND THE HOUSE,BARBECUE GRILL
AROUND THE HOUSE,BARBECUE TONGS

root@mrjackpots:/mnt/wof/pm/wofvdata# wc -l docs/puzzles.txt
3931 docs/puzzles.txt
root@mrjackpots:/mnt/wof/pm/wofvdata# wc -l docs/puzzles_eur.txt
3947 docs/puzzles_eur.txt
```

Wheel of Fortune - PoC

```
filename = "puzzles.txt"

def openpuzzle(question_cat, word_count,
firstword_count, question_count):

    with open(filename, 'r', newline='') as data:
            answerkey = csv.DictReader(data,
("CATEGORY", "ANSWER"))

            results = []

            for row in answerkey:
                answers = answer(results, answerkey,
row, question_cat, word_count, firstword_count,
[TRUNCATED]
```



WHEEL OF FORTUNE

CATEGORY

ON THE MAP

Word Count:

2

Letters in First Word:

12

Total Letters:

18

I'D LIKE TO SOLVE THE PUZZLE

WHEEL OF FORTUN

Answers	Letters				
SOUTHWESTERN STATES	S *(4)*	T *(4)*	H *(1)*	W *(1)*	R *(1)*

Wheel of Fortune - Maximum Ticket Payout

NA

Average: 2001.347915 Count: 3932 Sum: 7869300

	A	B	C
1	CATEGORY	ANSWER	PAYOUT
2	PHRASE	YOU TOOK THE WORDS RIGHT OUT OF MY MOUTH	4500
3	SONG/ARTIST	BLUE SUEDE SHOES BY ELVIS PRESLEY	4500
4	PHRASE	IT'S THE LITTLE THINGS THAT MATTER	4500
5	HUSBAND AND WIFE	WARREN BEATTY AND ANNETTE BENING	4500
6	SONG LYRICS	TOGETHER FOREVER AND NEVER TO PART	4500
7	PERSON	FORMER PRESIDENT OF THE UNITED STATES	4200
8	PHRASE	LET'S GET TO THE BOTTOM OF THIS	4200
9	PHRASE	THE BEST OFFENSE IS A GOOD DEFENSE	4200
10	PHRASE	YOU LOOK LIKE SOMEONE I USED TO KNOW	4200
11	MOVIE TITLE	NATIONAL LAMPOONS CHRISTMAS VACATION	4200
12	PHRASE	GETTING BETTER ALL THE TIME	3900
13	PHRASE	PICK A NUMBER BETWEEN ONE AND TEN	3900
14	PHRASE	MAKE SURE WE'RE ALL ON THE SAME PAGE	3900
15	FOOD AND DRINK	STEAMED ASPARAGUS SPEARS	3900
16	HUSBAND AND WIFE	BEN AFFLECK AND JENNIFER GARNER	3900
17	LANDMARK	GRACELAND IN MEMPHIS TENNESSEE	3900
18	PHRASE	I THINK WE GOT OFF ON THE WRONG FOOT	3900
19	PHRASE	YOU'RE NOT OUT OF THE WOODS YET	3900
20	CLASSIC TV	LAVERNE DEFAZIO AND SHIRLEY FEENEY	3900

EU

	A	B	C
1	CATEGORY	ANSWER	PAYOUT
2	PHRASE	IT'S THE LITTLE THINGS THAT MATTER	4500
3	PHRASE	YOU TOOK THE WORDS RIGHT OUT OF MY MOUTH	4500
4	SONG LYRICS	TOGETHER FOREVER AND NEVER TO PART	4500
5	SONG/ARTIST	BLUE SUEDE SHOES BY ELVIS PRESLEY	4500
6	MOVIE TITLE	NATIONAL LAMPOONS CHRISTMAS VACATION	4200
7	PHRASE	LET'S GET TO THE BOTTOM OF THIS	4200
8	PHRASE	YOU LOOK LIKE SOMEONE I USED TO KNOW	4200
9	FOOD AND DRINK	STEAMED ASPARAGUS SPEARS	3900
10	LANDMARK	GRACELAND IN MEMPHIS TENNESSEE	3900
11	PHRASE	GETTING BETTER ALL THE TIME	3900
12	PHRASE	HAVE YOUR PEOPLE CALL MY PEOPLE	3900
13	PHRASE	I THINK WE GOT OFF ON THE WRONG FOOT	3900
14	PHRASE	IF MY MEMORY SERVES ME CORRECTLY	3900
15	PHRASE	LEAVE YOUR MESSAGE AFTER THE TONE	3900
16	PHRASE	MAKE SURE WE'RE ALL ON THE SAME PAGE	3900
17	PHRASE	PICK A NUMBER BETWEEN ONE AND TEN	3900
18	PHRASE	THE BEST OFFENCE IS A GOOD DEFENCE	3900
19	PHRASE	YOU'RE NOT OUT OF THE WOODS YET	3900
20	SONG LYRICS	I WANT TO FLY LIKE AN EAGLE TO THE SEA	3900

Remediation

Remediation

Arcade Owners

Black Box

- Network connectivity?
- Weak credentials?
- Unnecessary services?
- Ask for more information

Network Isolation

- Keep off the network (not always possible)
- Restrict inbound/outbound traffic to only the necessary hosts
  - Game patches
  - Online services (leaderboards, profiles)

Remediation

Developers

Vendors

Lockdown

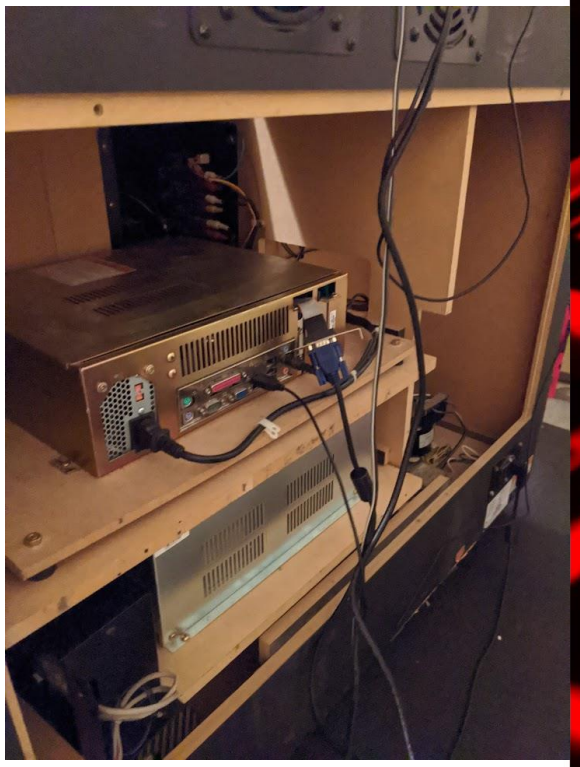
- Disable management interfaces
- Remove unused services

Development

- Dedicated development systems
- Isolate “production” builds
- Purge sensitive or custom data

Transparency

- Arcade Owners
  - Document requirements
- Players
  - The Cutting Room Floor (https://tcrf.net/)



References

Further Reading

- Don’t Give Credit: Hacking Arcade Machines
  - https://downloads.immunityinc.com/infiltrate-archives/Arcade_Attacks.pdf
- Unraveling Konami’s Arcade DRM
  - https://mon.im/2017/12/konami-arcade-drm.html
- pwning a SafeNET Microdog
  - https://mercaldim.gitbook.io/writeups/20131223
- The Cutting Room Floor
  - https://tcrf.net/The_Cutting_Room_Floor
  - https://tcrf.net/Jurassic_Park_Arcade

Buy Your Own

- eBay
  - https://www.ebay.com/usr/bruce1arcade
  - https://www.ebay.com/usr/migs2007/
- Stores
  - https://www.arcadespareparts.com
  - https://www.betson.com/
- Buyee - Japanese Proxy Delivery
  - https://buyee.jp/yahoo/auction?lang=en

Jackpot!

Attacking Arcade Machines

Patrick Sayler

www.netspi.com

twitter.com/psayler