



Hacking Mobile Games: Closing the Gap between "Ikan Bilis" and "Whales"

Nicholas Lim

- Associate Principal @ Vantage Point
- Hacks stuff for a living
- CREST CCT (App), OSCE and more.
- Most recent research -> mobile games

Disclaimer

- All information presented during this presentation are strictly for educational purposes only
- Vantage Point and the presenter will not be held responsible for any damages and/or losses due to misuse of information presented in this presentation.

Ikan Bilis.... what?



<https://www.delicious.com.au/recipes/ikan-bilis-peanuts/e5a92312-62fc-4a8e-9577-94ad4126a047>



Ikan Bilis

- “small fishes”
- F2P (free-to-play)
- Small spenders

Whales

- P2P (pay-to-play)
- P2W (pay-to-win)

Ikan Bilis vs Whales



<https://gfycat.com/gifs/detail/GlossyChillyBat>

Definition from Wiki -

"Game mechanics are constructs of rules or methods designed for interaction with the game state, thus providing **gameplay**."

A WEAPON IS A
GAME MECHANIC.

GAMEPLAY IS HOW IT
WORKS WITH OTHER
MECHANICS.

ARCADE RAGE

BY MART VIRKUS

COUNTER STRIKE

YOU HAVE A WEAPON.



WITH LIMITED HP, YOU EITHER
DIE FAST OR LIVE LONG ENOUGH
TO BECOME A СУКА БЛЯД.



<https://arcaderage.co/2016/07/10/gameplay-mechanics-explained/>

Mobile Game Mechanics – Clash Royale

Ranking in “Top Grossing Apps”



#14



#21



<https://www.youtube.com/watch?v=ipobTqtP-sw>

Mobile Game Mechanics – Clash Royale



Mobile Game Mechanics – Clash Royale



Mobile Game Mechanics – Clash Royale





Other Areas

- Online || Offline Components
- Social Elements (rankings/leaderboard)
- PvP?
- Shared || Instance Spaces

- Game Client
- Network Traffic
- Server
- ~~Business Logic~~ Game Mechanics
- and of course...

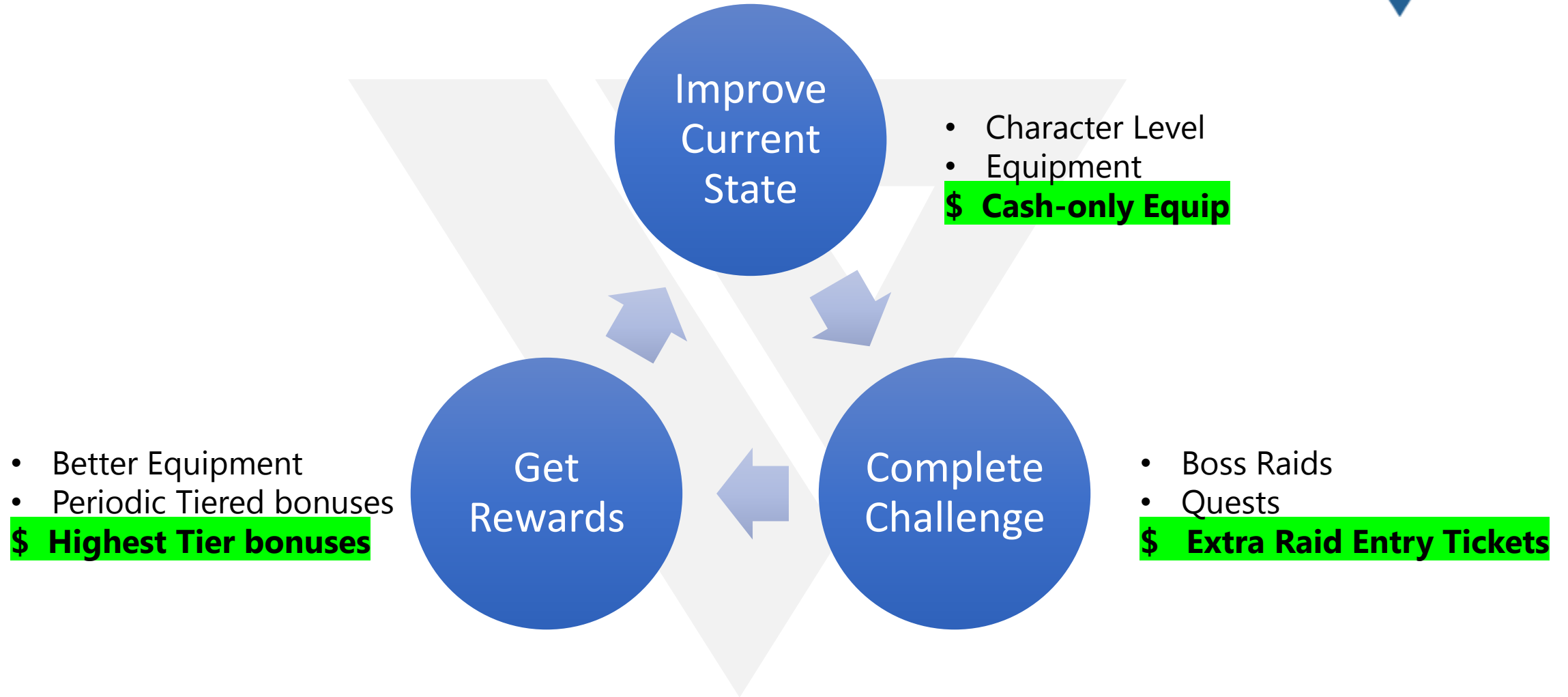


- Game Client
- Network Traffic
- Server
- ~~Business Logic~~ Game Mechanics



Identifying the Gap

The Gap – Game Progression





Closing the Gap?

maplestory **M**



Game #1 – MapleStory M

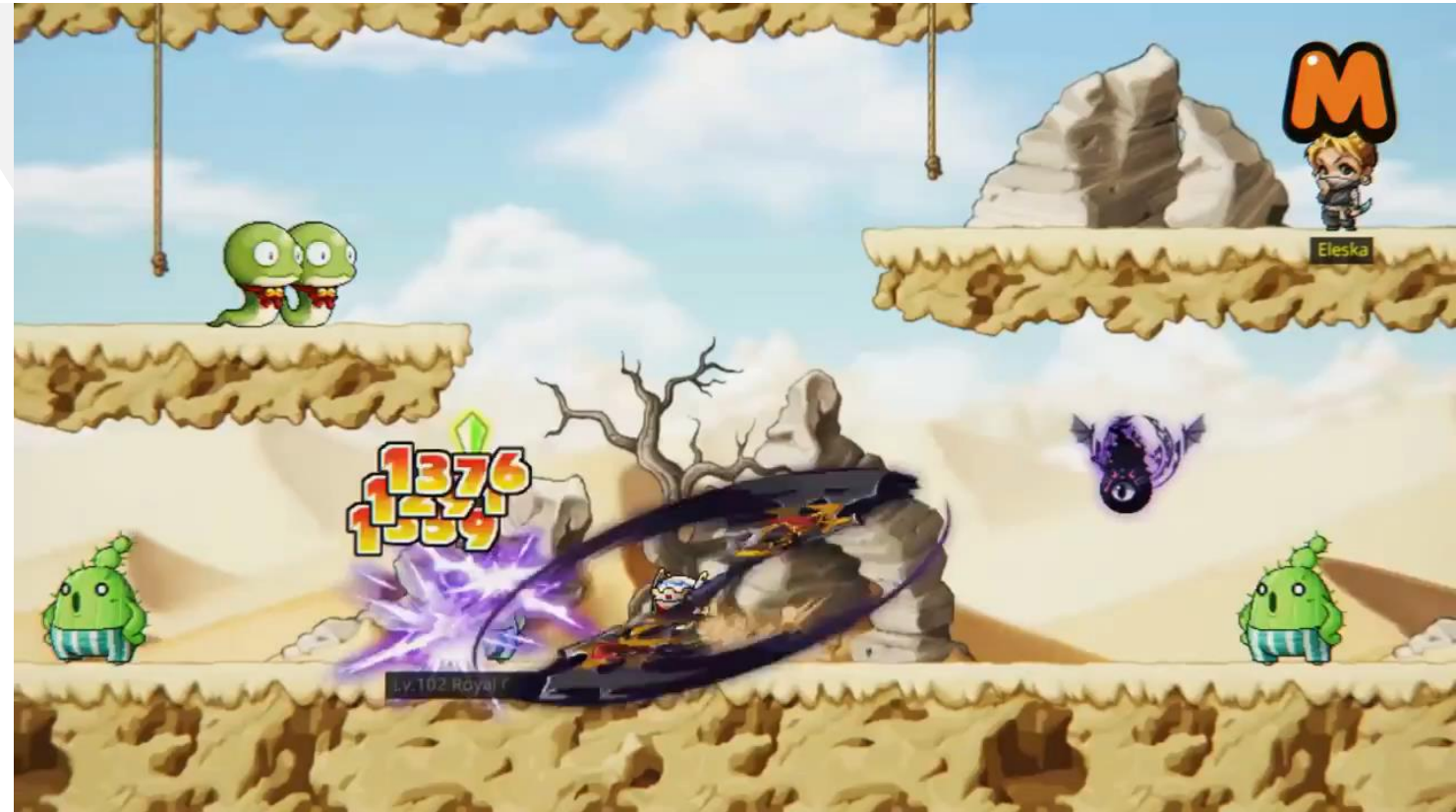
Ranking in “Top Grossing Apps”



#1



#1



<https://www.youtube.com/watch?v=Awg8INN4Tdc>

Game Progression

- Kill mobs and do tasks to gain EXP
- The faster you kill, the more EXP you gain (per hour)
- To kill faster, you need to deal more damage (better equip / higher level)

Game Progression (Mathematical Estimates)

- Lv 1 – 100 => Takes around 30-50 game hours
- +1-2 weeks of farming => **"Epic"** weapon to **"Unique"**
- +120 days of farming => **"Unique"** to **"Legendary"**

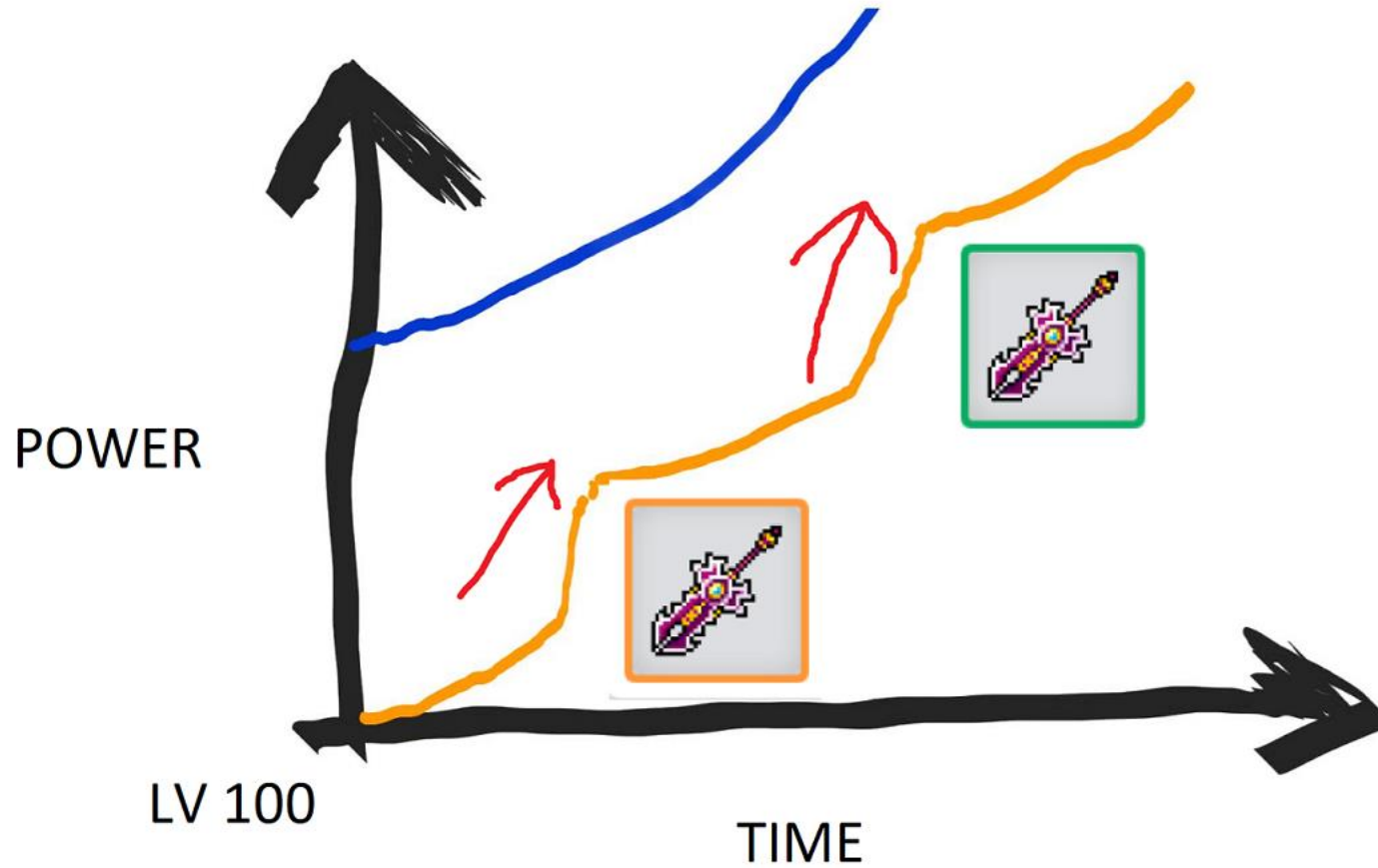
Game Progression (Mathematical Estimates)

- Lv 1 – 100 => Takes around 30-50 game hours
- \$\$ + 1-2 weeks of farming => “Epic” weapon to “Unique”
- \$\$ + 120 days of farming => “Unique” to “Legendary”



Game #1 – MapleStory M

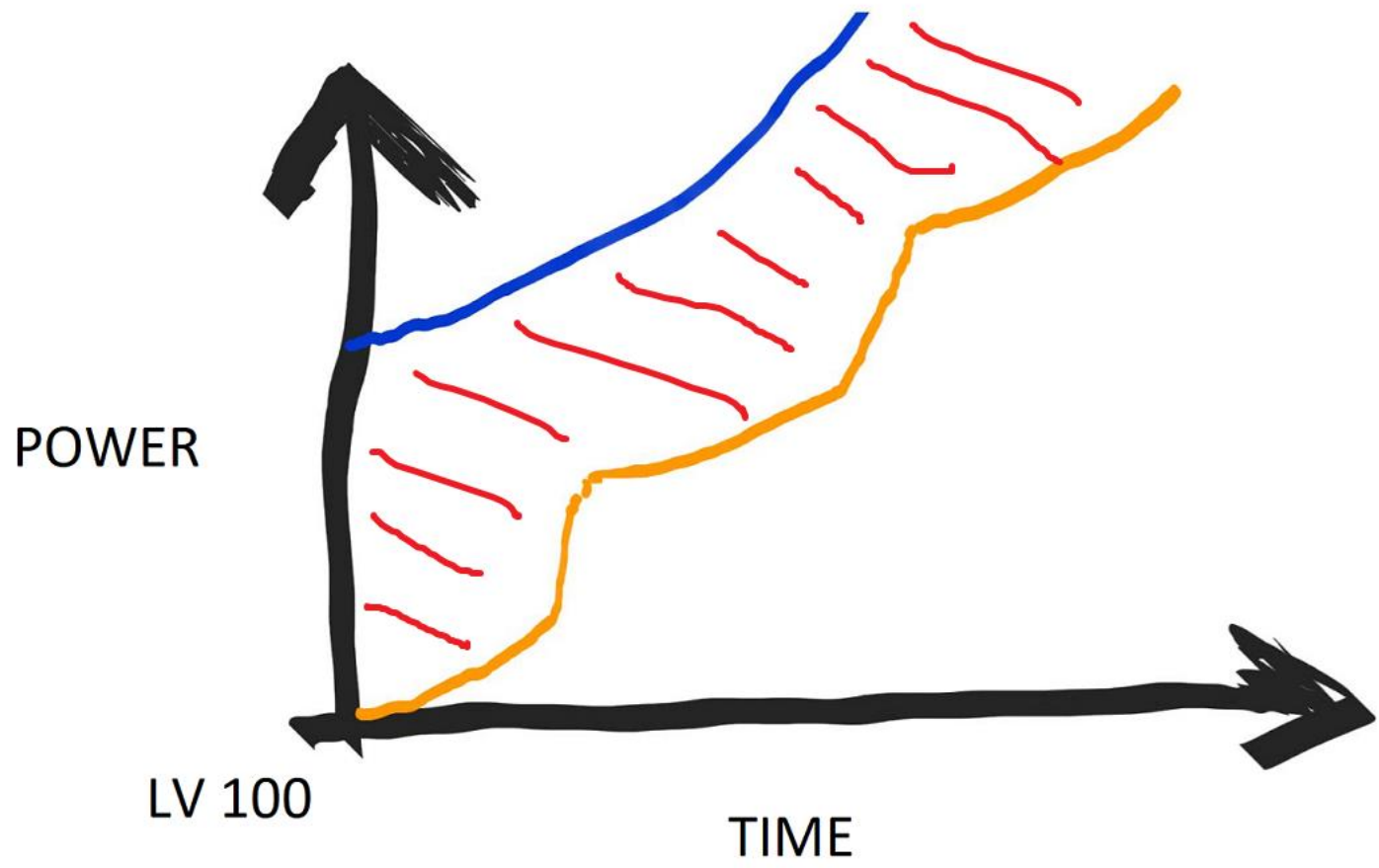
Blue -> whales
Orange -> ikan bilis



Game #1 – MapleStory M



Blue-> whales
Orange -> ikan bilis

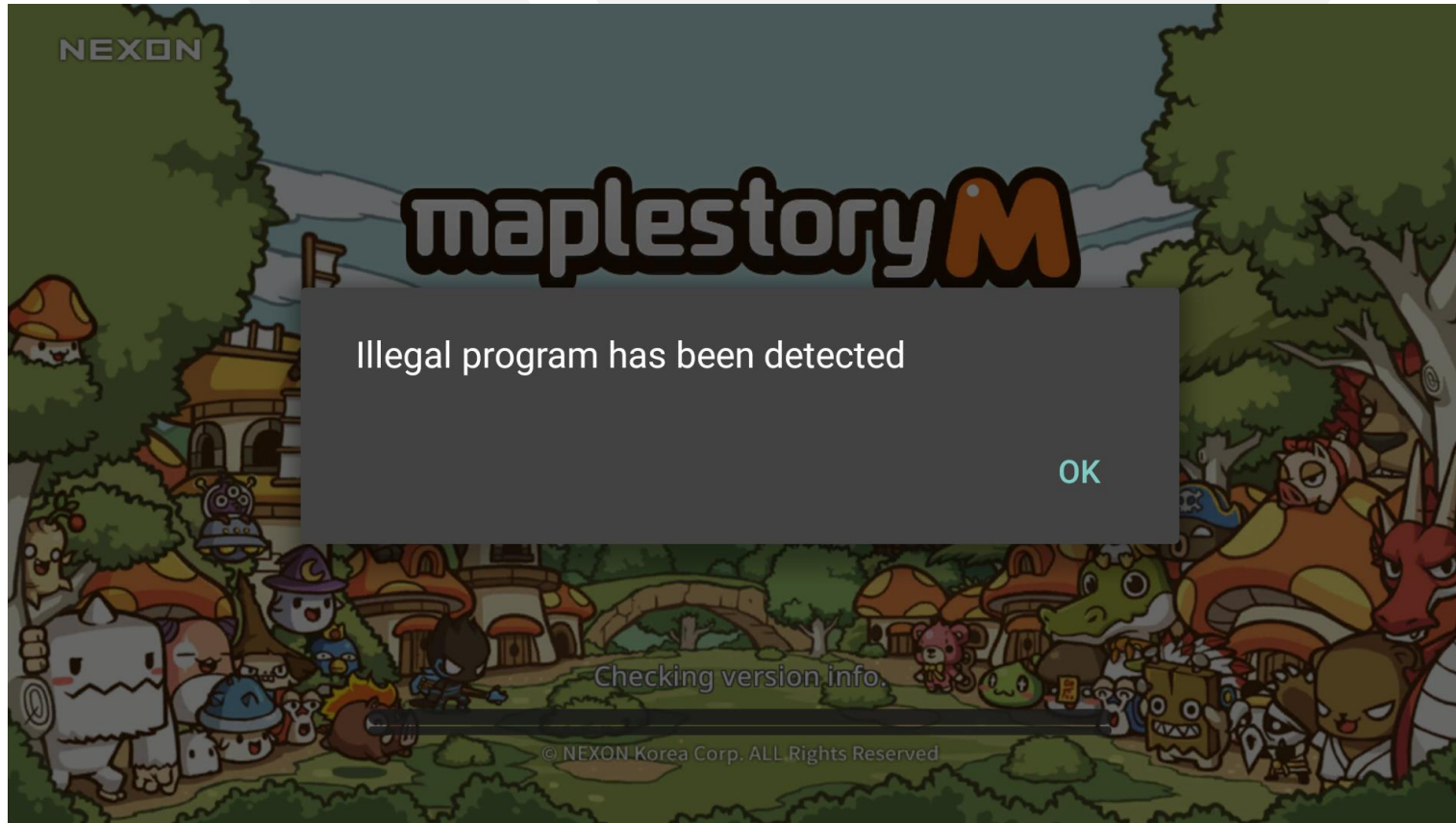


MapleStory M – Network Traffic

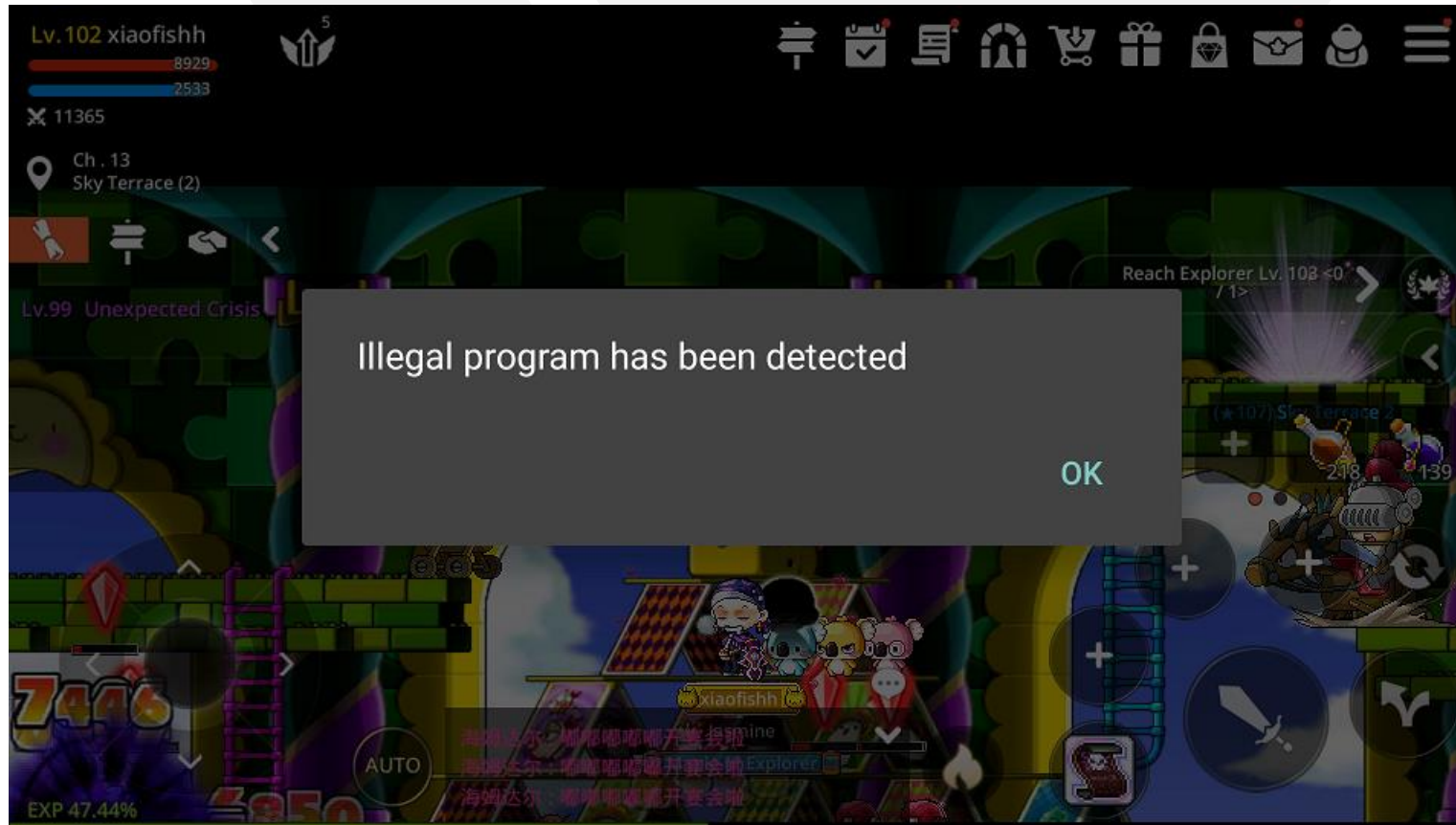
```
<Release AdjustProduction="true" ClientVersion="1.27.217" DevOption="false" EventURL="http://127.0.0.1:8080/maplem"
LoginServerIP="mm-gl-login-cd47a2c53d197a67.elb.ap-southeast-1.amazonaws.com" LoginServerPort="7500" MaxLoadPerSec="256" Memo="127_170"
NextVersionCheck="true" Report="false" ResourceURL="http://nxm-maplem.akamaized.net/Global/GooglePlay/127_170/" TapjoyDebug="false" />
<Release AdjustProduction="true" ClientVersion="1.27.218" DevOption="false" EventURL="http://127.0.0.1:8080/maplem"
LoginServerIP="mm-gl-login-cd47a2c53d197a67.elb.ap-southeast-1.amazonaws.com" LoginServerPort="7500" MaxLoadPerSec="256" Memo="127_170"
NextVersionCheck="true" Report="false" ResourceURL="http://nxm-maplem.akamaized.net/Global/GooglePlay/127_170/" TapjoyDebug="false" />
<Release AdjustProduction="true" ClientVersion="1.27.219" DevOption="false" EventURL="http://127.0.0.1:8080/maplem"
LoginServerIP="mm-gl-login-cd47a2c53d197a67.elb.ap-southeast-1.amazonaws.com" LoginServerPort="7500" MaxLoadPerSec="256" Memo="127_170"
NextVersionCheck="true" Report="false" ResourceURL="http://nxm-maplem.akamaized.net/Global/GooglePlay/127_170/" TapjoyDebug="false" />
<Release AdjustProduction="true" ClientVersion="1.2701.240" DevOption="false" EventURL="http://127.0.0.1:8080/maplem"
LoginServerIP="mm-gl-login-cd47a2c53d197a67.elb.ap-southeast-1.amazonaws.com" LoginServerPort="7500" MaxLoadPerSec="256" Memo="12701_171"
NextVersionCheck="true" Report="false" ResourceURL="http://nxm-maplem.akamaized.net/Global/GooglePlay/12701_171/" TapjoyDebug="false" />
<Release AdjustProduction="true" ClientVersion="1.2701.241" DevOption="false" EventURL="http://127.0.0.1:8080/maplem"
LoginServerIP="mm-gl-login-cd47a2c53d197a67.elb.ap-southeast-1.amazonaws.com" LoginServerPort="7500" MaxLoadPerSec="256" Memo="12701_171"
NextVersionCheck="true" Report="false" ResourceURL="http://nxm-maplem.akamaized.net/Global/GooglePlay/12701_171/" TapjoyDebug="false" />
```

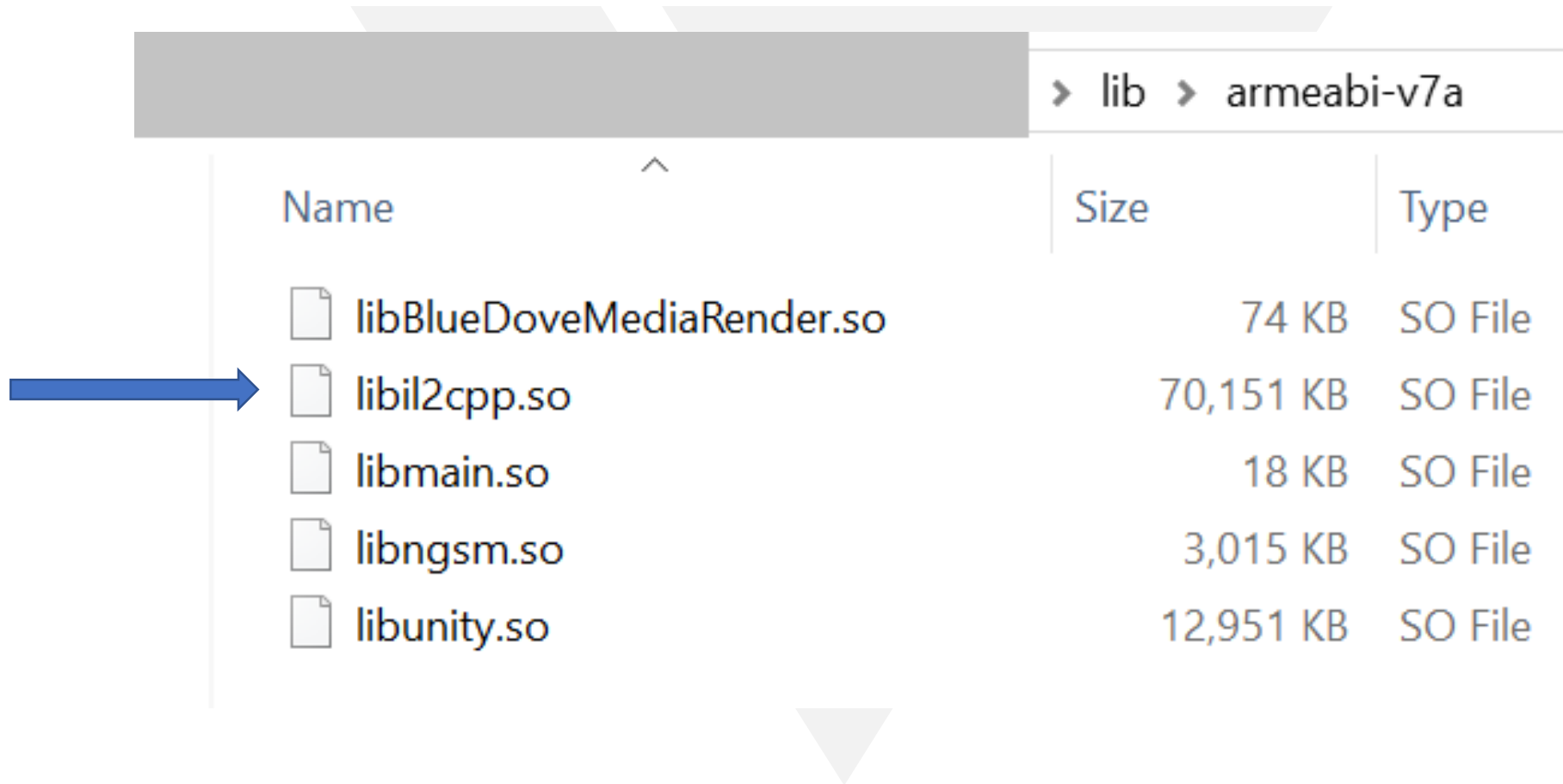
- Non-proxy aware, TCP
- Multiple EC2 instances with their default URLs
(ec2-x-x-x-x.ap-southeast-1.compute.amazonaws.com)
- Each login / “change channel” will change destination server
- Common port range (7201-7206)






MapleStory M – Game Client / Modification



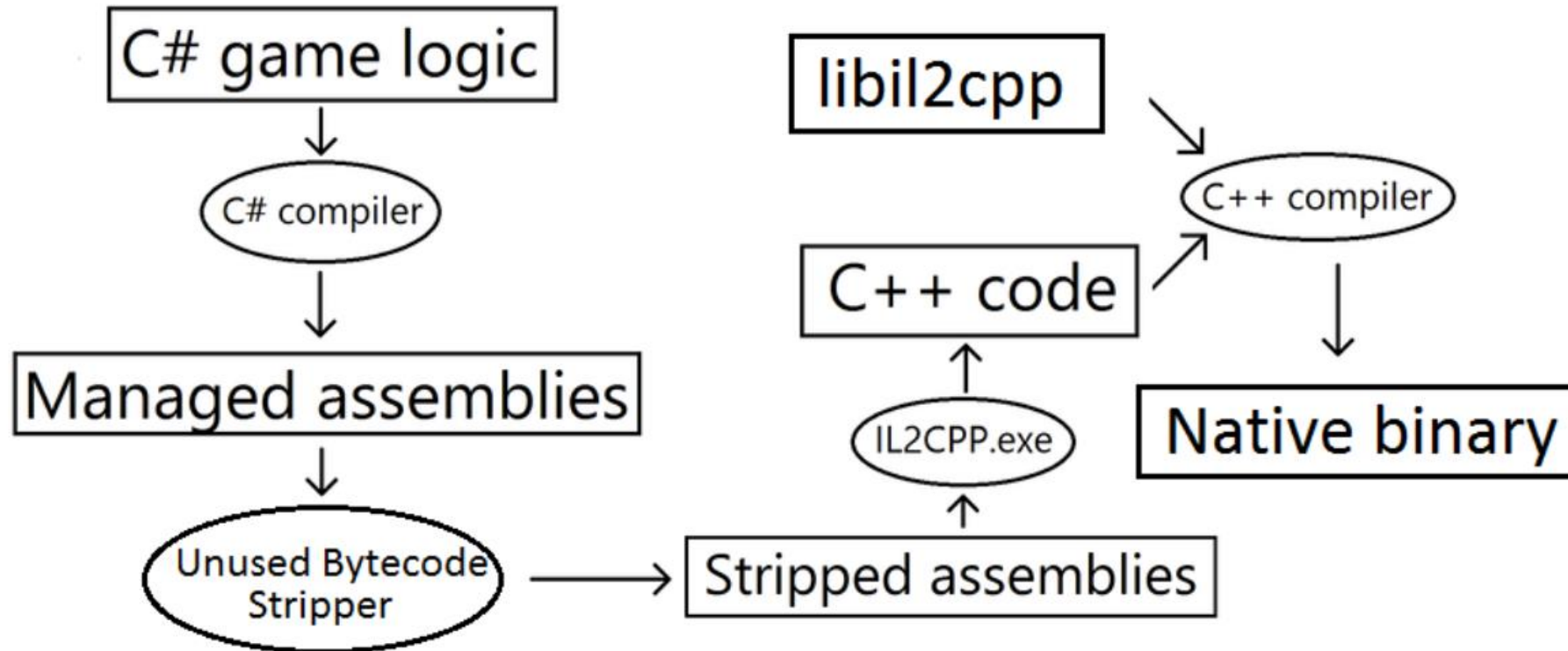
MapleStory M – Game Client





Name	Size	Type
 libBlueDoveMediaRender.so	74 KB	SO File
 libil2cpp.so	70,151 KB	SO File
 libmain.so	18 KB	SO File
 libngsm.so	3,015 KB	SO File
 libunity.so	12,951 KB	SO File

IL2CPP



<https://docs.unity3d.com/Manual/IL2CPP-HowItWorks.html>





- <https://github.com/Perfare/Il2CppDumper>
 - needs libil2cpp.so and global-metadata.dat
 - needs two parameters in libil2cpp.so
- Throw libil2cpp.so into IDA -> fetch 2 addresses
 - `il2cpp::vm::MetadataCache::Register()`

MapleStory M – Game Client

The screenshot displays the IDA Pro interface with several windows open. The main window shows assembly code for a function named `s_I12CppCodegenRegistration`. The code includes instructions for loading registers and performing an addition. A red box highlights the symbols `g_CodeRegistration` and `g_MetadataRegistration` used in the assembly. Below the assembly view, a terminal window titled `il2cppDumper.exe` shows the execution of a utility program. The terminal output includes instructions for selecting a mode, initializing the il2cpp file, applying relocations, and dumping the code. The program prompts for input code and metadata registrations, which are redacted with grey boxes. The terminal concludes with a 'Done!' message and a prompt to press any key to exit.

```
EXPORT _Z27s_I12CppCodegenRegistration
_Z27s_I12CppCodegenRegistration ; DATA XREF: sub_1B6312C+10↑o
; .got: _Z27s_I12CppCodegenRegistration_ptr↓o
LDR R0, =(g_CodeRegistration_ptr - 0x3C70C0C)
LDR R1, =(g_MetadataRegistration_ptr - 0x3C70C10)
LDR R2, =(unk_3F4A688 - 0x3C70C14)
; End of function s_I12CppCodegenRegistration(void)
LDR R0, [PC,R0] ; g_CodeRegistration
LDR R1, [PC,R1] ; g_MetadataRegistration
ADD R2, PC, R2 ; unk_3F4A688
B j_j__ZN6il2cpp2vm13MetadataCache8RegisterEPK22I12CppCodeRegistrationP
```

```
il2cppDumper.exe
Select Mode: 1.Manual 2.Auto 3.Auto(Advanced) 4.Auto(Plus) 5.Auto(Symbol)
Initializing il2cpp file...
Applying relocations...
Input CodeRegistration: ██████████
Input MetadataRegistration: ██████████
Dumping...
Done !
Create DummyDll...
Done !
Press any key to exit...
```

Name 	Size
 DummyDll	
 dump.cs	8,547 KB
 script.py	9,488 KB



MapleStory M – Game Client

```
public abstract void OnAttackDamage(User attacker, IAgent defender, ulong tick, byte status, long health64, int mana,
    int damage, uint markerHandle, int effect, byte hitOffset, int splitOffset, bool fromSkill, bool damageFontShow,
    bool showEffectForce); // 0

public abstract void OnAttackDamage(IAgent attacker, User defender, ulong tick, byte status, long health64, int mana,
    int damage, uint markerHandle, int effect, int splitOffset, bool fromSkill, bool damageFontShow, bool
    showEffectForce); // 0

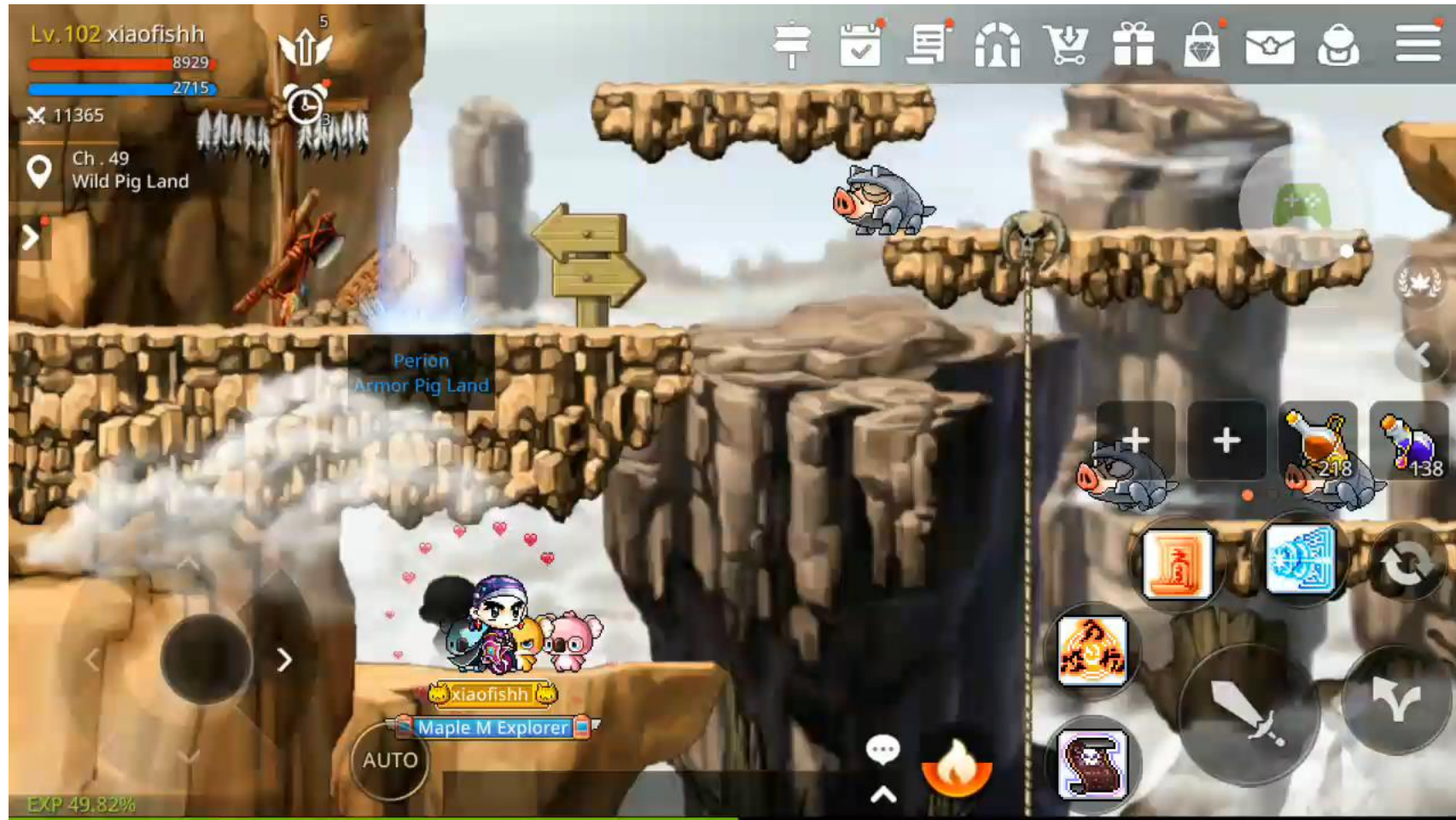
public abstract void OnAttackDamage(IAgent attacker, IAgent defender, ulong tick, byte status, long health64, int
    mana, int damage, uint markerHandle, int effect, byte hitOffset, int splitOffset, bool fromSkill, bool
    damageFontShow, bool showEffectForce); // 0
```



Top exploit for MSM in the wild (patched recently)

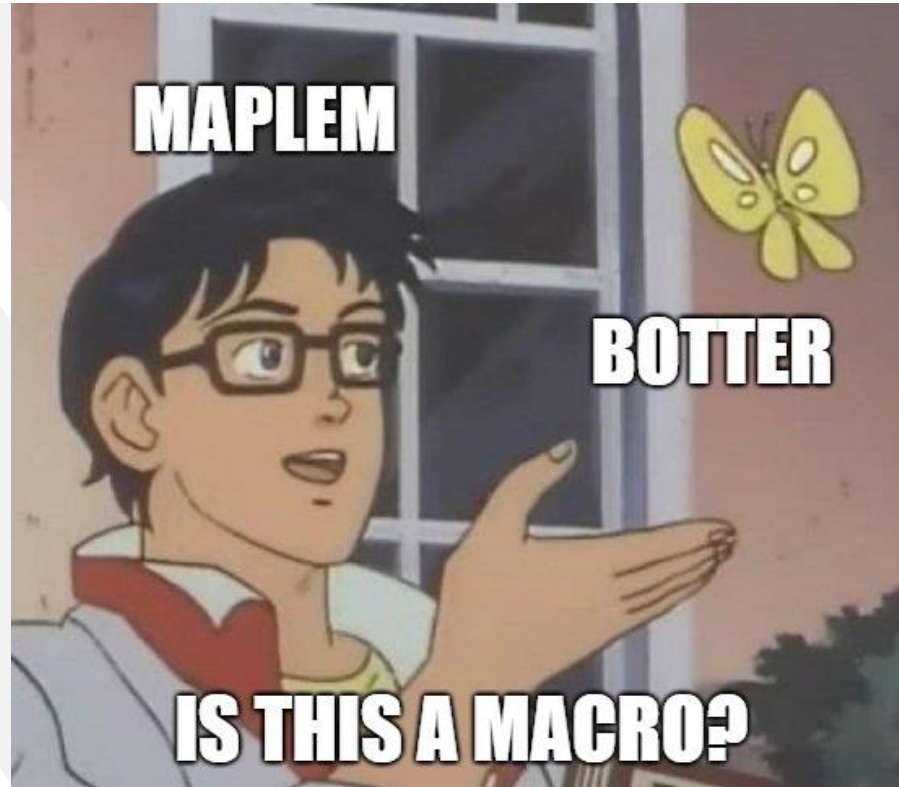
- “Cast Skill” Packet Replay
- Concept of Balance
 - “Ultimate” skills deal high damage but comes with long cooldown time
- Exploit effectively closes the attack power gap (the whales don’t need them as much)

MapleStory M – Game Mechanics

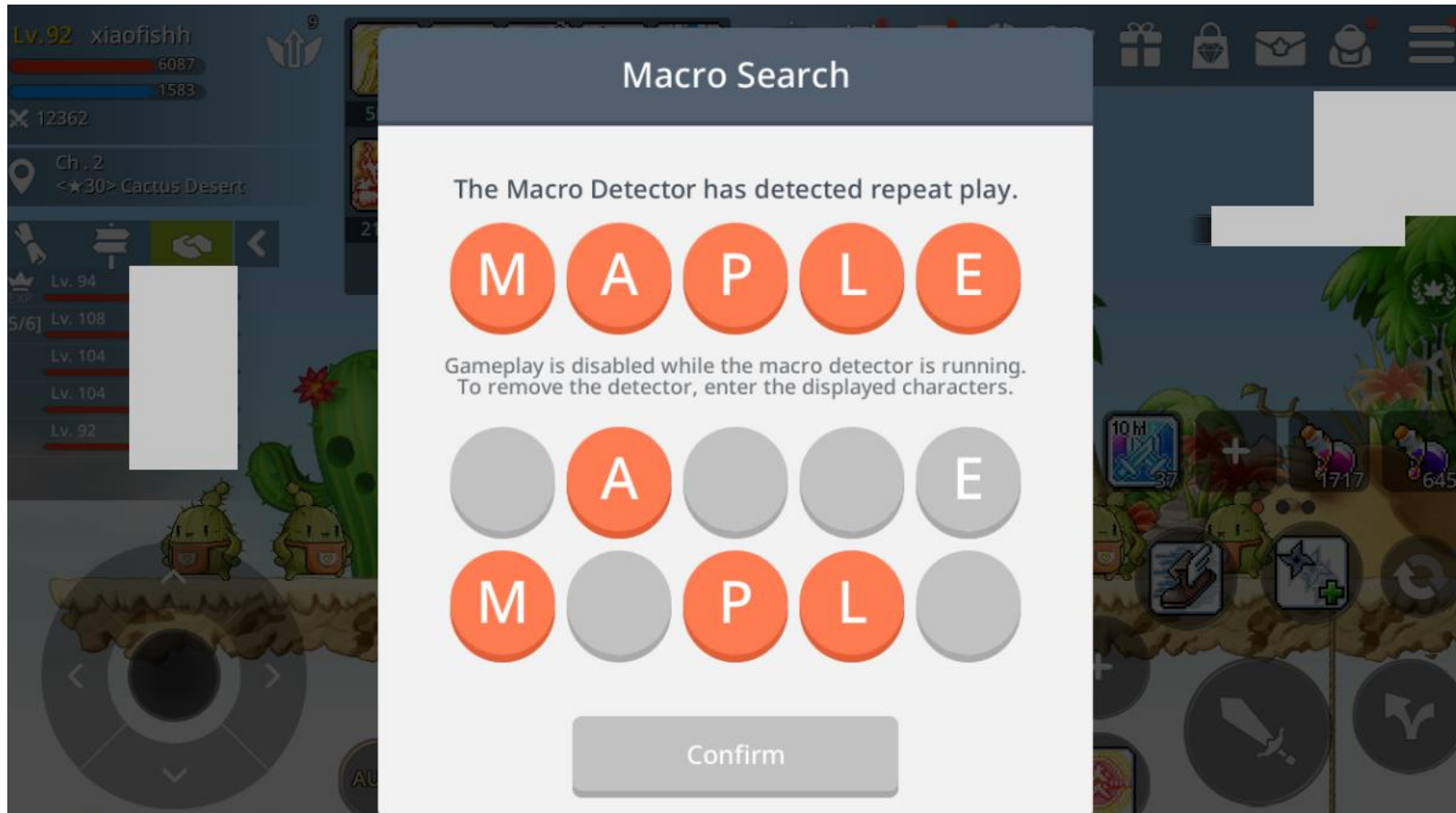


Top Abuse by Players

- Macros / Bots

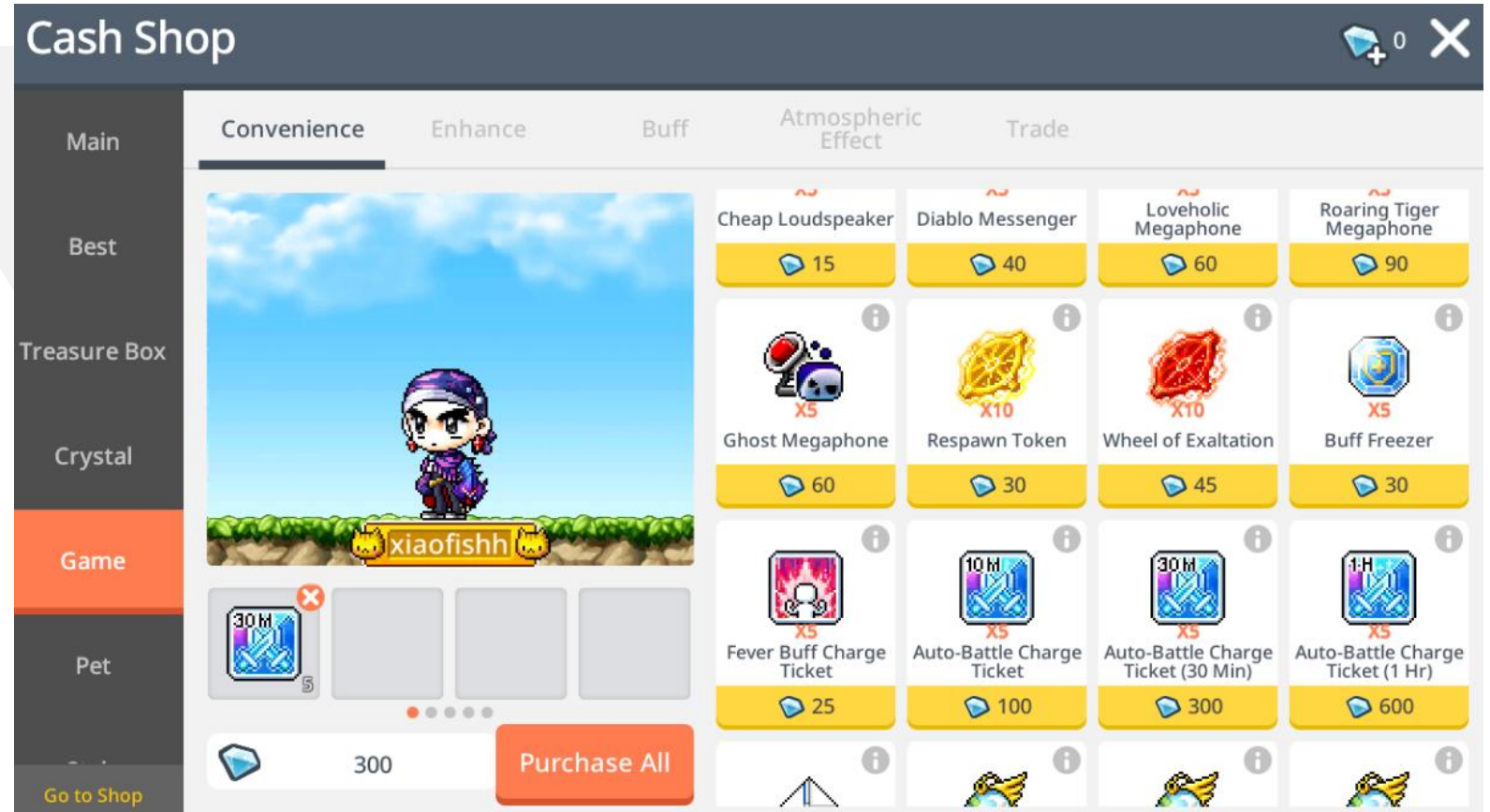


MapleStory M – Game Mechanics

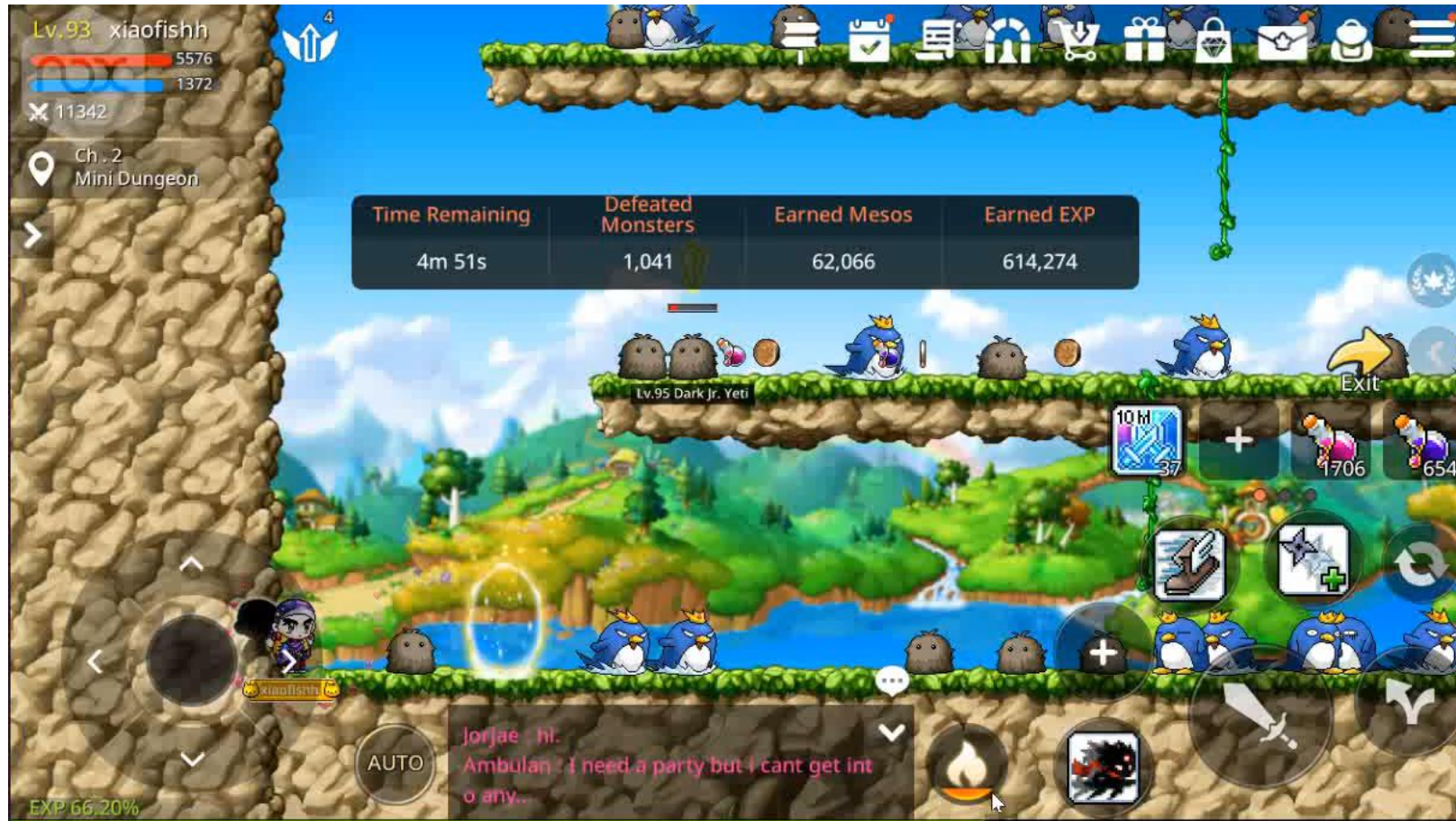


Auto-Battle

- 5 hrs for 600c
- Crystal Rates -
107.6c per SGD
- ~\$6 per 5hrs of
Auto-Battle



MapleStory M – Game Mechanics



Game #2 – King's Raid

Ranking in "Top Grossing Apps"



#61



#18



<https://www.youtube.com/watch?v=jRsMDI5bF0w>

Game Progression

- Clear game chapters to unlock more "side-quests"
- More unlocked chapters gives more daily/weekly rewards.
- To clear more chapters, you need to deal more damage (better equip / higher level)

Game Progression (Mathematical Estimates)

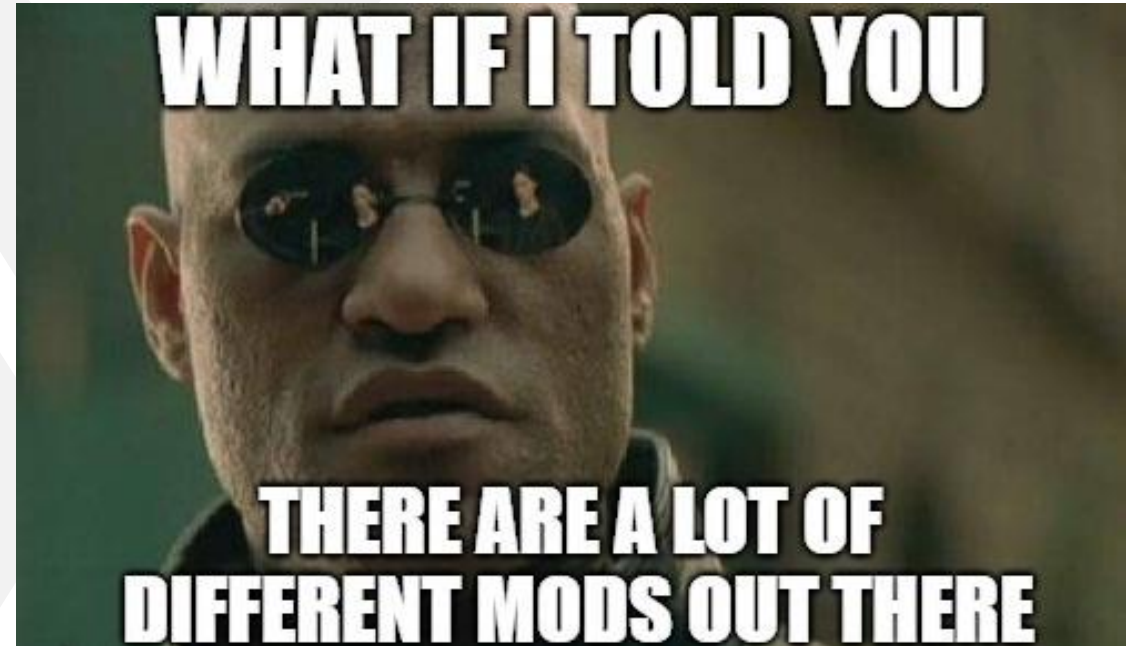
- Chapter 1 – 6 => Takes around 2-4 calendar weeks
- + 1-2 months => Chapter 7
- + xx months => Chapter 8

Game Progression (Mathematical Estimates)

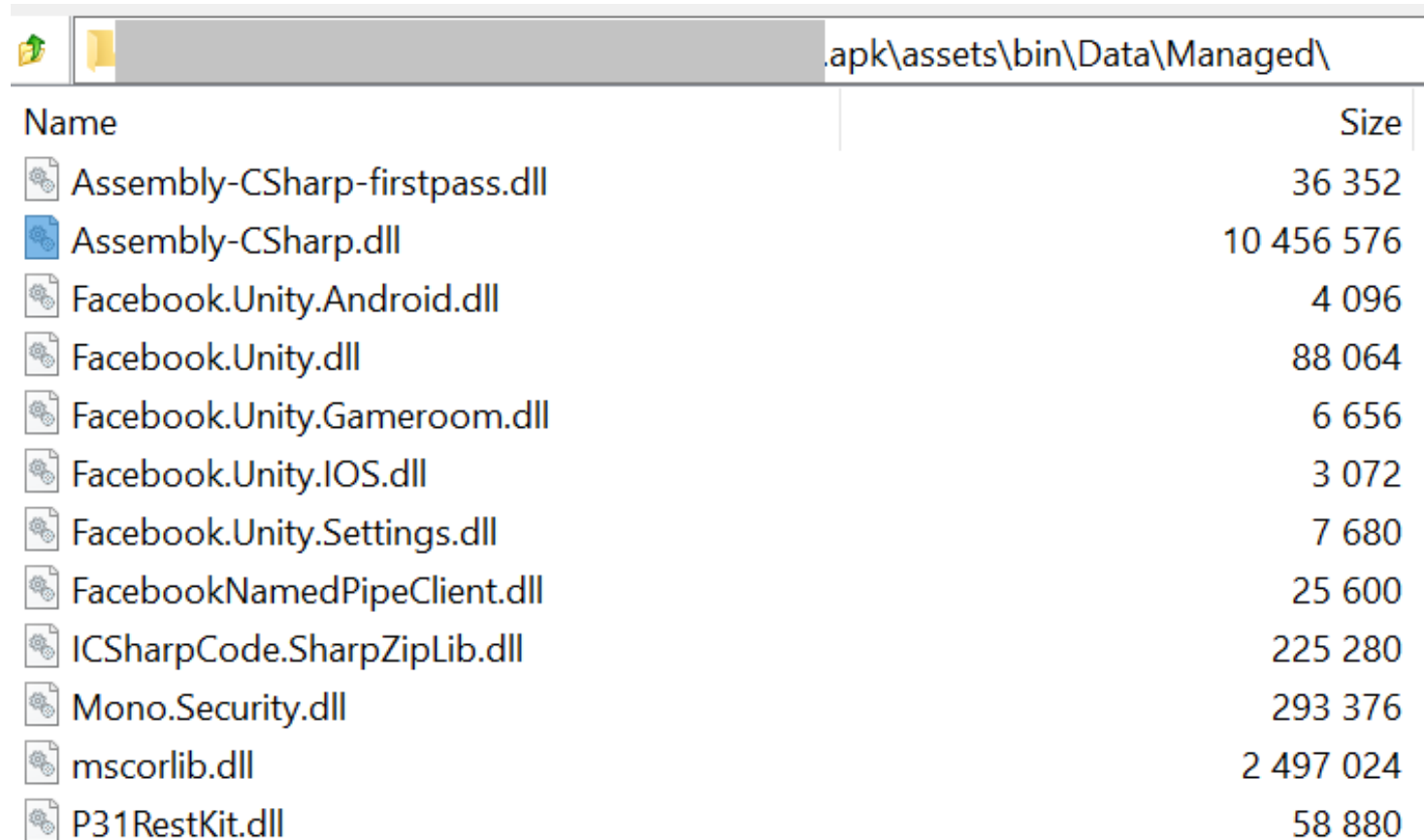
- Chapter 1 – 6 => Takes around 2-4 calendar weeks
- + 1-2 months => Chapter 7
- \$\$\$ within 1st month => Chapter 8













Known Exploits for KR in the wild

- In the form of publicly distributed mods
 - God Mode
 - 2x / 5x / 10x ATK, DEF and HP
 - 1-hit kill




King's Raid – Game Client



Name	Size
 Assembly-CSharp-firstpass.dll	36 352
 Assembly-CSharp.dll	10 456 576
 Facebook.Unity.Android.dll	4 096
 Facebook.Unity.dll	88 064
 Facebook.Unity.Gameroom.dll	6 656
 Facebook.Unity.IOS.dll	3 072
 Facebook.Unity.Settings.dll	7 680
 FacebookNamedPipeClient.dll	25 600
 ICSharpCode.SharpZipLib.dll	225 280
 Mono.Security.dll	293 376
 mscorlib.dll	2 497 024
 P31RestKit.dll	58 880

King's Raid – Game Client



 Assembly-CSharp.dll

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00€...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..'.'!.,.Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
00000080	50	45	00	00	4C	01	04	00	00	00	00	00	00	00	00	00	PE..L.....

Known Exploits for KR in the wild

- Tried to learn from existing mods

King's Raid – Game Mechanics / Normal



King's Raid – Game Mechanics / Modded



King's Raid – Game Mechanics





Questions?

nicholas.lim@vantagepoint.sg

@kactros_n