MMO Reversing

Dave Kukfa

/who

- Dave Kukfa
- 3rd year
- MMO master
- Web
- Pentesting
- Reversing
- http://kukfa.co

Background

- Dungeon Runners
- Shut down in 2010
- Client still exists
- No servers to connect to

Server emulator

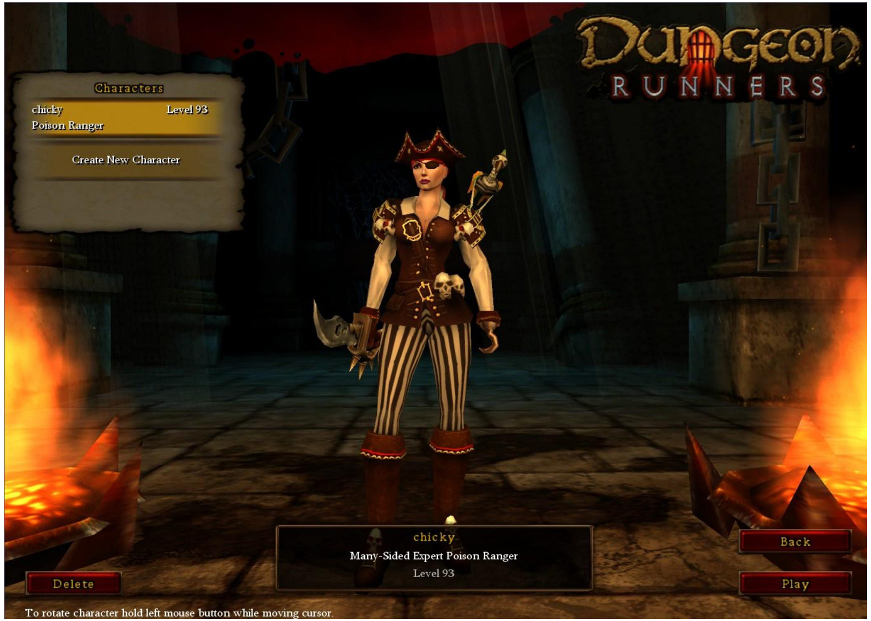
- Efforts to build a server emulator over the past year
  - AKA private server
- Goal: mimic the functionality of the original game’s server
- Server emulators exist for many online games
  - WoW
  - Everquest
  - Ultima Online
  - etc.

DR server components

- Authentication server
  - Logins
  - World selection
- Game server
  - Gameplay
  - Game environment (towns etc.)
  - Creating and saving characters
  - and more

Traffic flow

- Client initially connects to auth server
  - Sends back world list
- Player chooses a world to play on
- Passed to game server
- Select a character and start playing

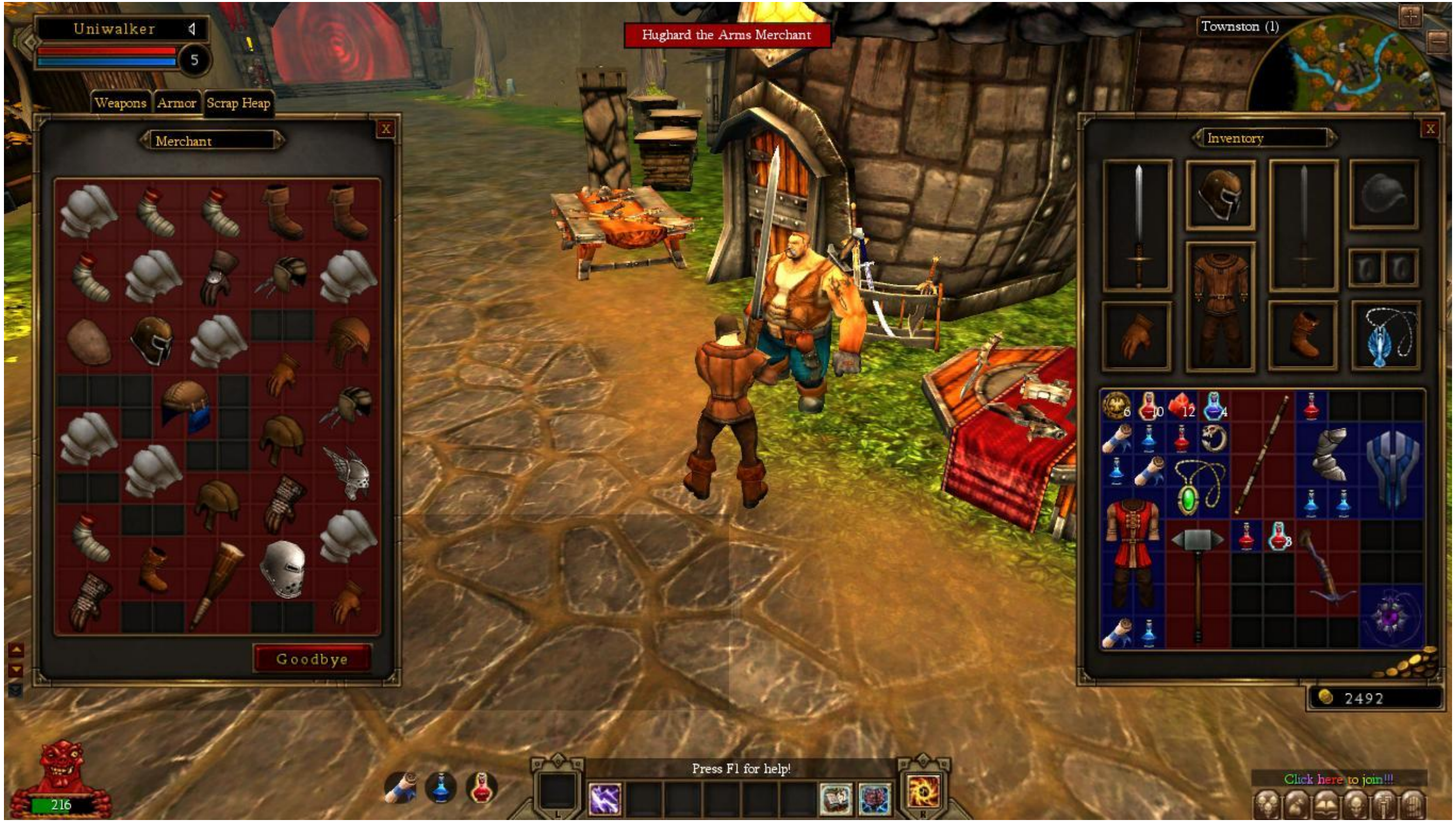


chicky Level 93
Poison Ranger

chicky
Many-Sided Expert Poison Ranger
Level 93

To rotate character hold left mouse button while moving cursor.

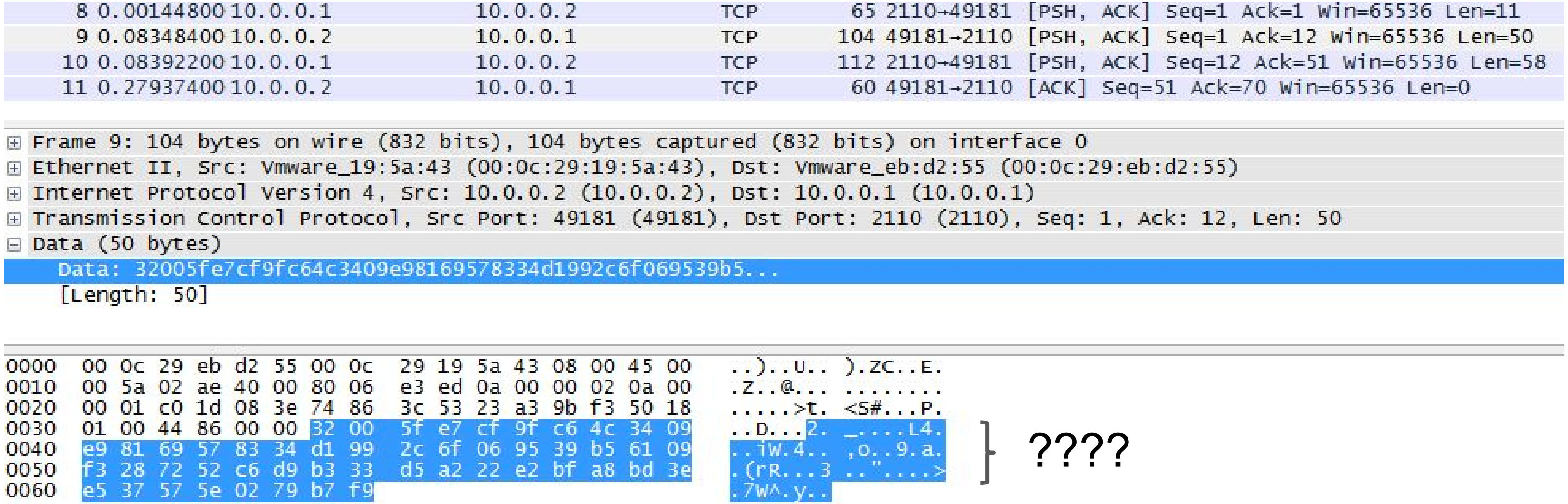
Lots of things to implement



Easier said than done

- Protocol analysis
    - Analyzing traffic between the client and the server
    - Identifying what the data in each packet is controlling
    - Detecting patterns and structure
    - Encryption and custom data formatting make this difficult
- Extremely difficult without an example
    - Server was shut down years ago
    - No one has a network capture of actual gameplay
    - Resort to reverse engineering and guess-and-check
    - Long and tedious

Protocol analysis



```
 8 0.00144800 10.0.0.1   10.0.0.2   TCP    65 2110→49181 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=11
 9 0.08348400 10.0.0.2   10.0.0.1   TCP   104 49181→2110 [PSH, ACK] Seq=1 Ack=12 Win=65536 Len=50
10 0.08392200 10.0.0.1   10.0.0.2   TCP   112 2110→49181 [PSH, ACK] Seq=12 Ack=51 Win=65536 Len=58
11 0.27937400 10.0.0.2   10.0.0.1   TCP    60 49181→2110 [ACK] Seq=51 Ack=70 Win=65536 Len=0
```

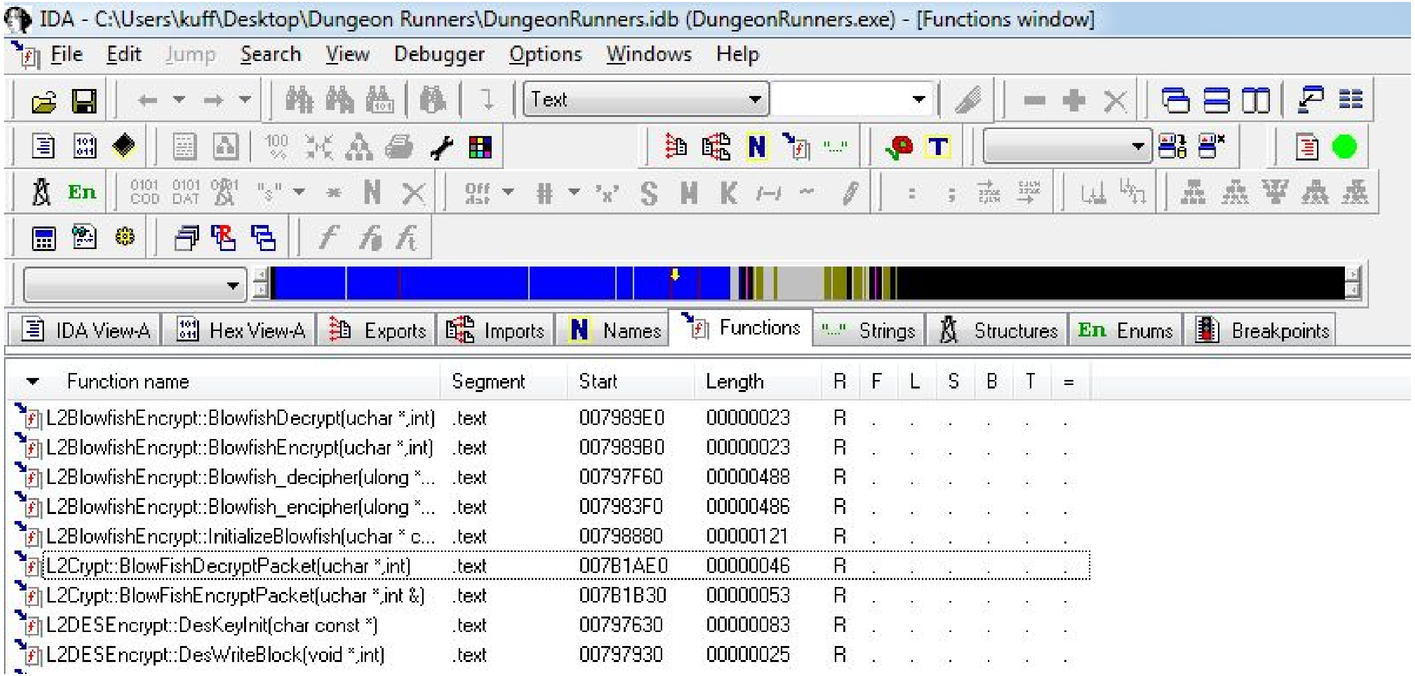
```
⊞ Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
⊞ Ethernet II, Src: Vmware_19:5a:43 (00:0c:29:19:5a:43), Dst: Vmware_eb:d2:55 (00:0c:29:eb:d2:55)
⊞ Internet Protocol Version 4, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.1 (10.0.0.1)
⊞ Transmission Control Protocol, Src Port: 49181 (49181), Dst Port: 2110 (2110), Seq: 1, Ack: 12, Len: 50
⊟ Data (50 bytes)
    Data: 32005fe7cf9fc64c3409e98169578334d1992c6f069539b5...
    [Length: 50]
```

```
0000  00 0c 29 eb d2 55 00 0c  29 19 5a 43 08 00 45 00   ..)..U.. ).ZC..E.
0010  00 5a 02 ae 40 00 80 06  e3 ed 0a 00 00 02 0a 00   .Z..@... ........
0020  00 01 c0 1d 08 3e 74 86  3c 53 23 a3 9b f3 50 18   .....>t. <S#...P.
0030  01 00 44 86 00 00 32 00  5f e7 cf 9f c6 4c 34 09   ..D...2. _....L4.
0040  e9 81 69 57 83 34 d1 99  2c 6f 06 95 39 b5 61 09   ..iW.4.. ,o..9.a.
0050  f3 28 72 52 c6 d9 b3 33  d5 a2 22 e2 bf a8 bd 3e   .(rR...3 ..".....>
0060  e5 37 57 5e 02 79 b7 f9                             .7W^.y..
```

????

Spring break

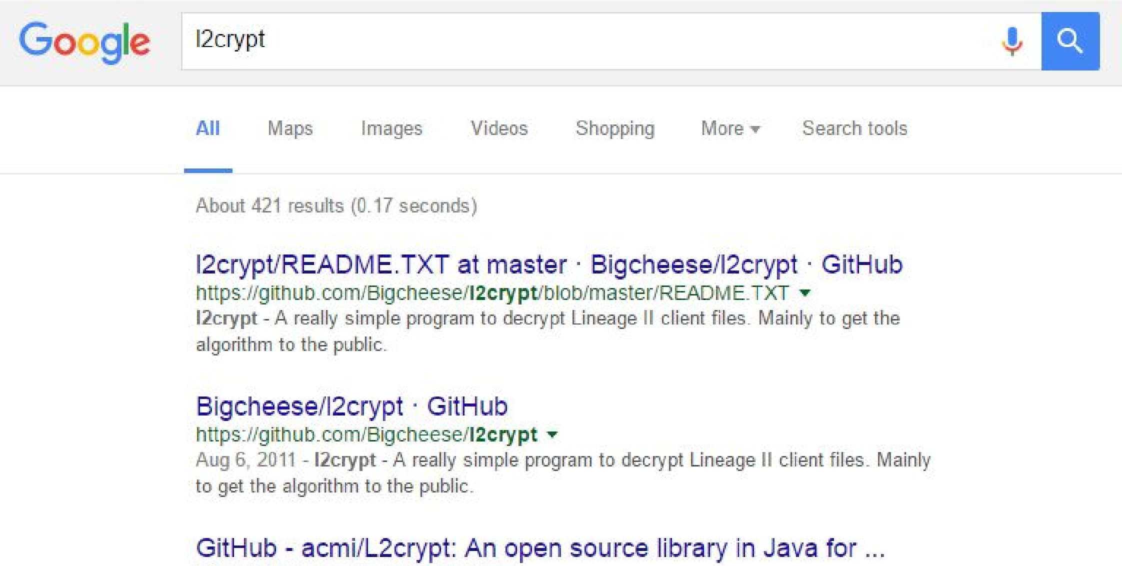
- Took another look at the client



Function name	Segment	Start	Length	R	F	L	S	B	T	=
L2BlowfishEncrypt::BlowfishDecrypt(uchar *,int)	.text	007989E0	00000023	R	.	.	.	.	.	.
L2BlowfishEncrypt::BlowfishEncrypt(uchar *,int)	.text	007989B0	00000023	R	.	.	.	.	.	.
L2BlowfishEncrypt::Blowfish_decipher(ulong *...	.text	00797F60	00000488	R	.	.	.	.	.	.
L2BlowfishEncrypt::Blowfish_encipher(ulong *...	.text	007983F0	00000486	R	.	.	.	.	.	.
L2BlowfishEncrypt::InitializeBlowfish(uchar * c...	.text	00798880	00000121	R	.	.	.	.	.	.
L2Crypt::BlowFishDecryptPacket(uchar *,int)	.text	007B1AE0	00000046	R	.	.	.	.	.	.
L2Crypt::BlowFishEncryptPacket(uchar *,int &)	.text	007B1B30	00000053	R	.	.	.	.	.	.
L2DESEncrypt::DesKeyInit(char const *)	.text	00797630	00000083	R	.	.	.	.	.	.
L2DESEncrypt::DesWriteBlock(void *,int)	.text	00797930	00000025	R	.	.	.	.	.	.

“L2”

- Dungeon Runners published by NCsoft
  - As are Lineage and Lineage II (other MMOs)
- Googling reveals..



About 421 results (0.17 seconds)

l2crypt/README.TXT at master · Bigcheese/l2crypt · GitHub
https://github.com/Bigcheese/**l2crypt**/blob/master/README.TXT ▾
l2crypt - A really simple program to decrypt Lineage II client files. Mainly to get the algorithm to the public.

Bigcheese/l2crypt · GitHub
https://github.com/Bigcheese/**l2crypt** ▾
Aug 6, 2011 - **l2crypt** - A really simple program to decrypt Lineage II client files. Mainly to get the algorithm to the public.

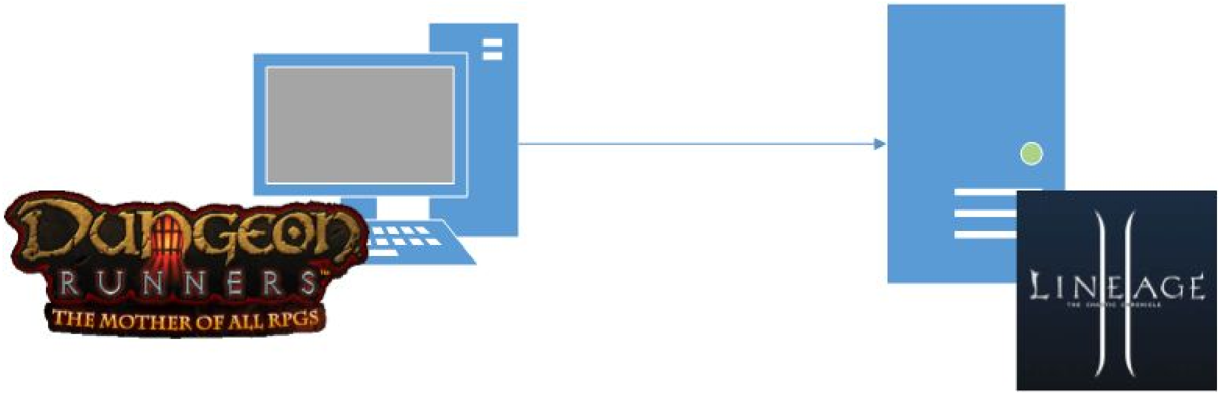
GitHub - acmi/L2crypt: An open source library in Java for ...

Timeline

- Dungeon Runners
    - Developed in 2005
    - Entered closed beta in May 2006
- Lineage II
    - Several different versions
    - First (Prelude) launched April 2004
    - Followed by C1 (June 2004) and C2 (December 2004)

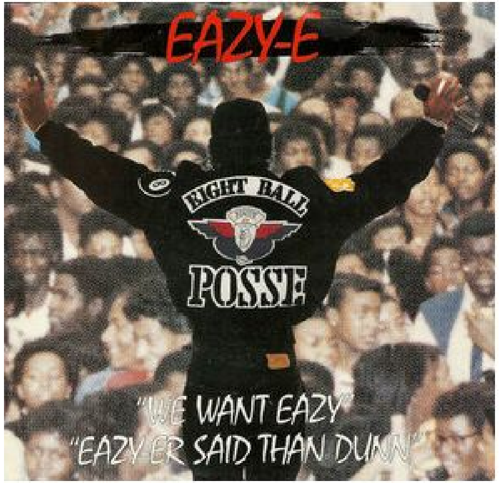
Shot in the dark

- Set up a L2 server emulator
- Point the DR client at it
- See what happens



Again, easier said than done

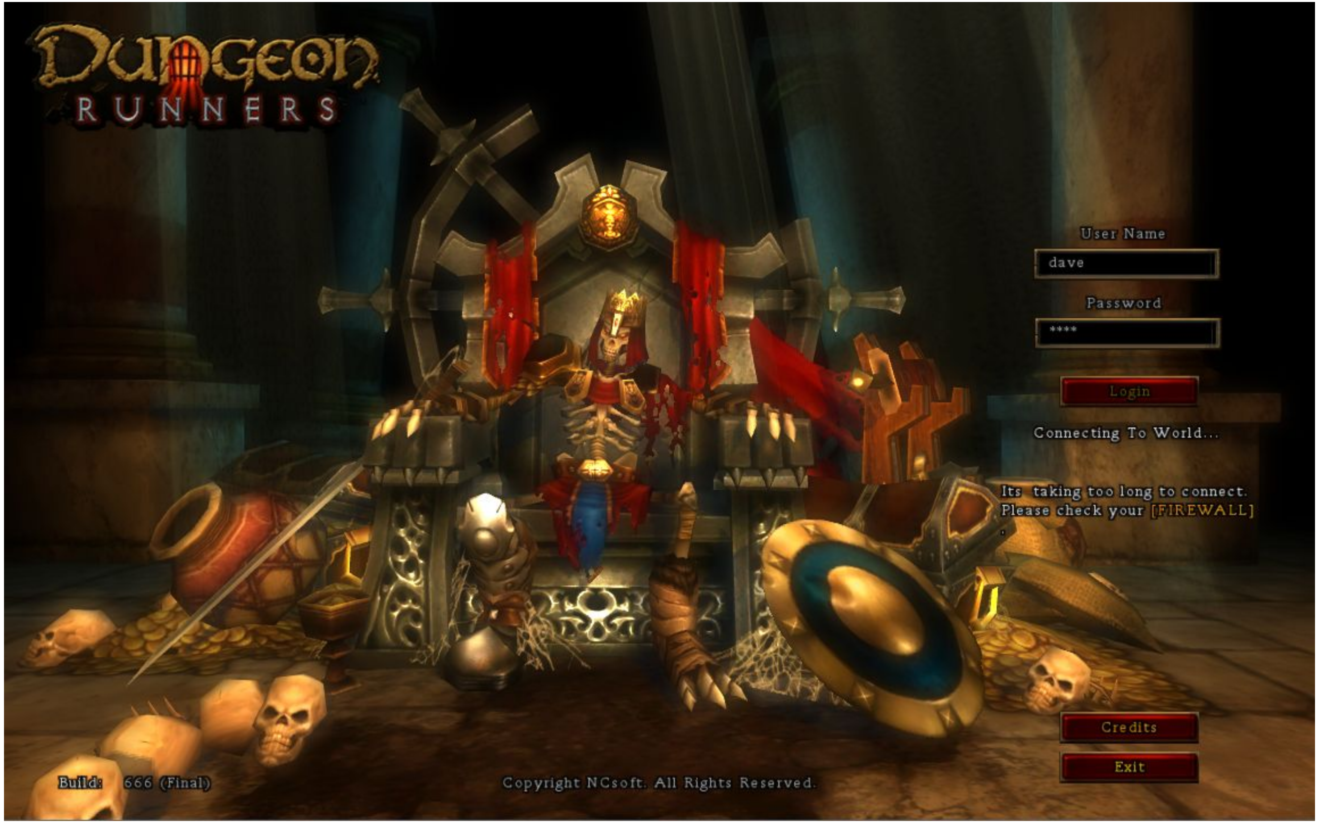
- Trying to find Prelude/C1/C2 servers
- Not fun trying to download obscure programs made 12 years ago
  - Surfing old forums
  - Many dead links
  - Searching for mirrors
- web.archive.org is a life saver



L2J

- One of the popular L2 server emulators
  - Comes with auth server and game server
- Ended up using a legacy version
  - C1/C2 compatible
  - November 2004
- Thankfully archived on Sourceforge

Used to seeing this...



User Name

dave

Password

****

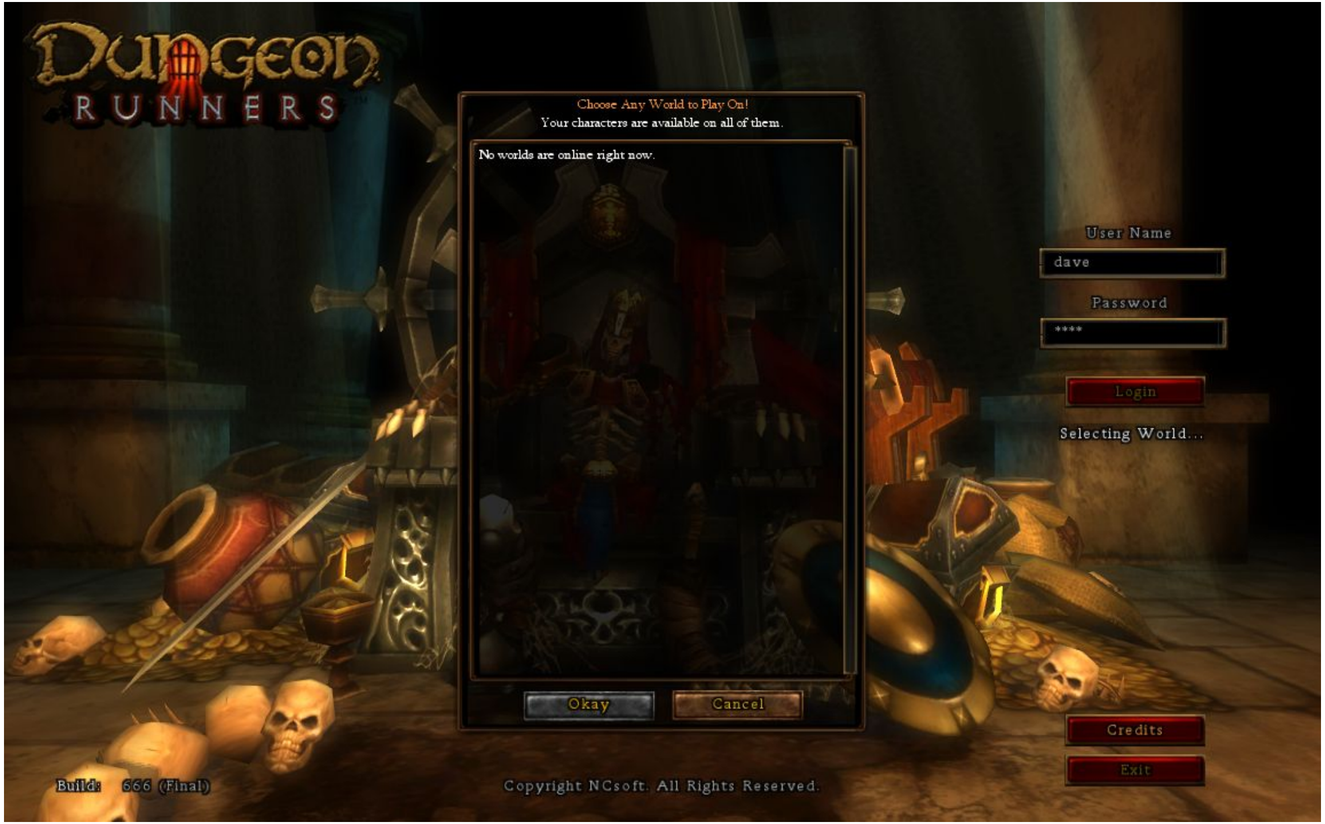
Connecting To World...

Its taking too long to connect.
Please check your [FIREWALL]

Build: 666 (Final)

Copyright NCsoft. All Rights Reserved.

With L2J...



Choose Any World to Play On!

Your characters are available on all of them.

No worlds are online right now.

User Name: dave

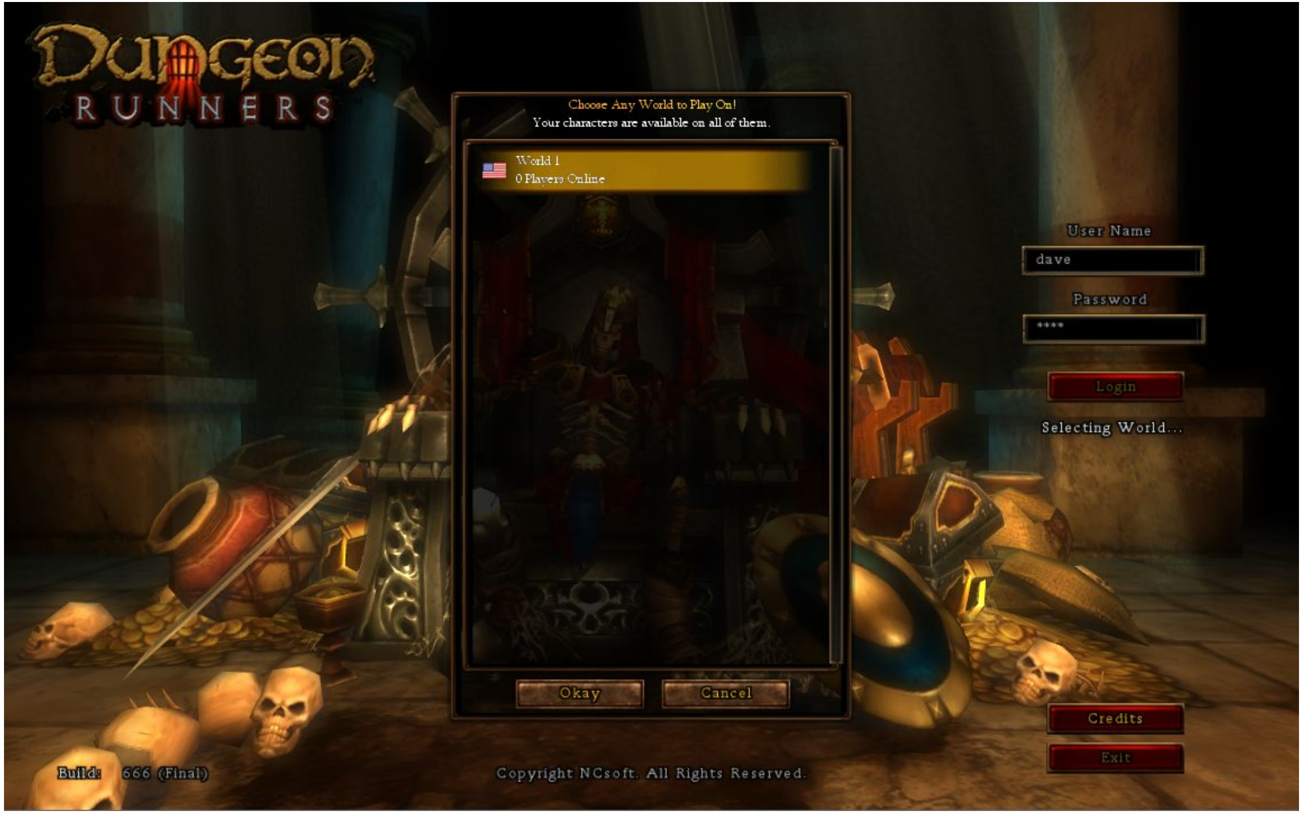
Password: ****

Selecting World...

Build: 666 (Final)

Copyright NCsoft. All Rights Reserved.

After some tweaks...



Choose Any World to Play On!
Your characters are available on all of them.

World 1
0 Players Online

User Name: dave

Password: ****

Selecting World...

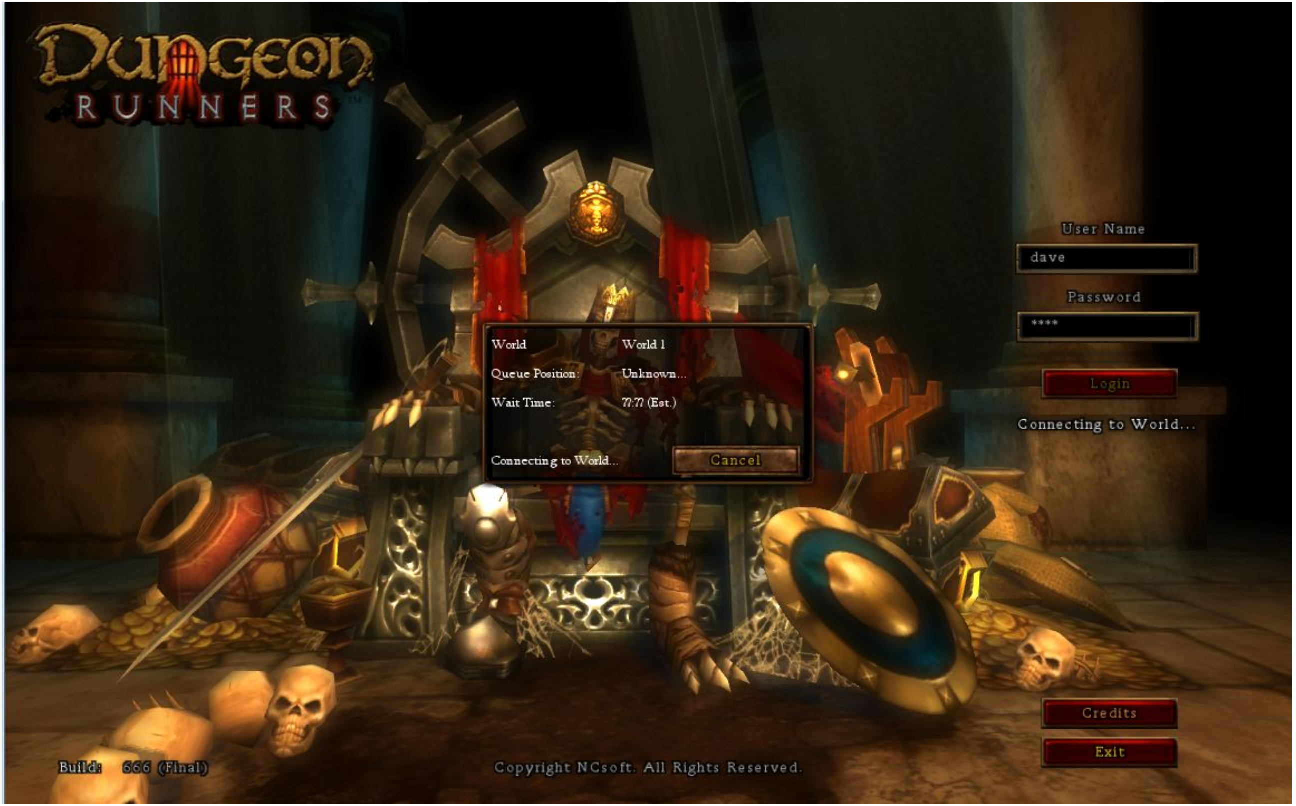
Build: 666 (Final)

Copyright NCsoft. All Rights Reserved.

Aftermath

- Concluded that DR used L2 auth server protocols
- Clients could successfully connect to auth server
  - Passed to game server after selecting a world
- Ran into problems with the game server
  - Not responding to client packets
- Spring break ended

Current point



User Name: dave

Password: ****

Connecting to World...

World: World 1

Queue Position: Unknown...

Wait Time: 77:77 (Est.)

Connecting to World...

Build: 666 (Final)

Copyright NCsoft. All Rights Reserved.

Positives

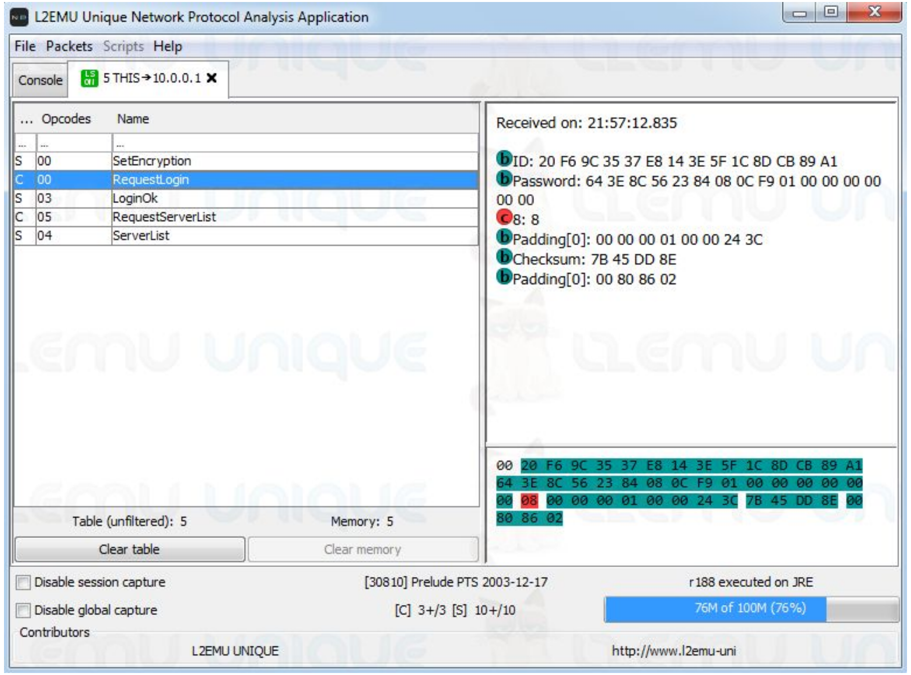
- Now have a working authentication server
- Huge lead for determining the rest of the game protocols
- Met a ton of devs in L2 emulator community

Tools

- IDA
- Wireshark
- Hex editor
- Lots of work by hand
    - Roll your sleeves up

Netpro

- L2 packet visualizer
  - Intercepts L2 traffic and analyzes it for you



L2EMU Unique Network Protocol Analysis Application
File Packets Scripts Help
Console
5 THIS→10.0.0.1

...	Opcodes	Name
...	...	...
S	00	SetEncryption
C	00	RequestLogin
S	03	LoginOk
C	05	RequestServerList
S	04	ServerList

Table (unfiltered): 5 Memory: 5

Received on: 21:57:12.835

```
ID: 20 F6 9C 35 37 E8 14 3E 5F 1C 8D CB 89 A1
Password: 64 3E 8C 56 23 84 08 0C F9 01 00 00 00 00
00 00
8: 8
Padding[0]: 00 00 00 01 00 00 24 3C
Checksum: 7B 45 DD 8E
Padding[0]: 00 80 86 02
```

```
00 20 F6 9C 35 37 E8 14 3E 5F 1C 8D CB 89 A1
64 3E 8C 56 23 84 08 0C F9 01 00 00 00 00 00
00 08 00 00 00 01 00 00 24 3C 7B 45 DD 8E 00
80 86 02
```

□ Disable session capture [30810] Prelude PTS 2003-12-17 r188 executed on JRE

□ Disable global capture [C] 3+/3 [S] 10+/10 76M of 100M (76%)

Contributors

L2EMU UNIQUE http://www.l2emu-uni

Future work

- Revisit the game server
    - Hammer out bugs
- Determine how often game server uses L2 protocols
- Eventually recreate the game world
    - NPCs
    - Monsters
    - Quests
    - etc.

Questions?

- dxk2652@rit.edu