# Hard Chatting - 400

## Category: Network Forensics

Problem Statement:
Hey, you're one of those computer people right? My boss Mike down at the garage said he got a letter from the internet company saying something about an attack? Could you take a look? I can't remember the password though…

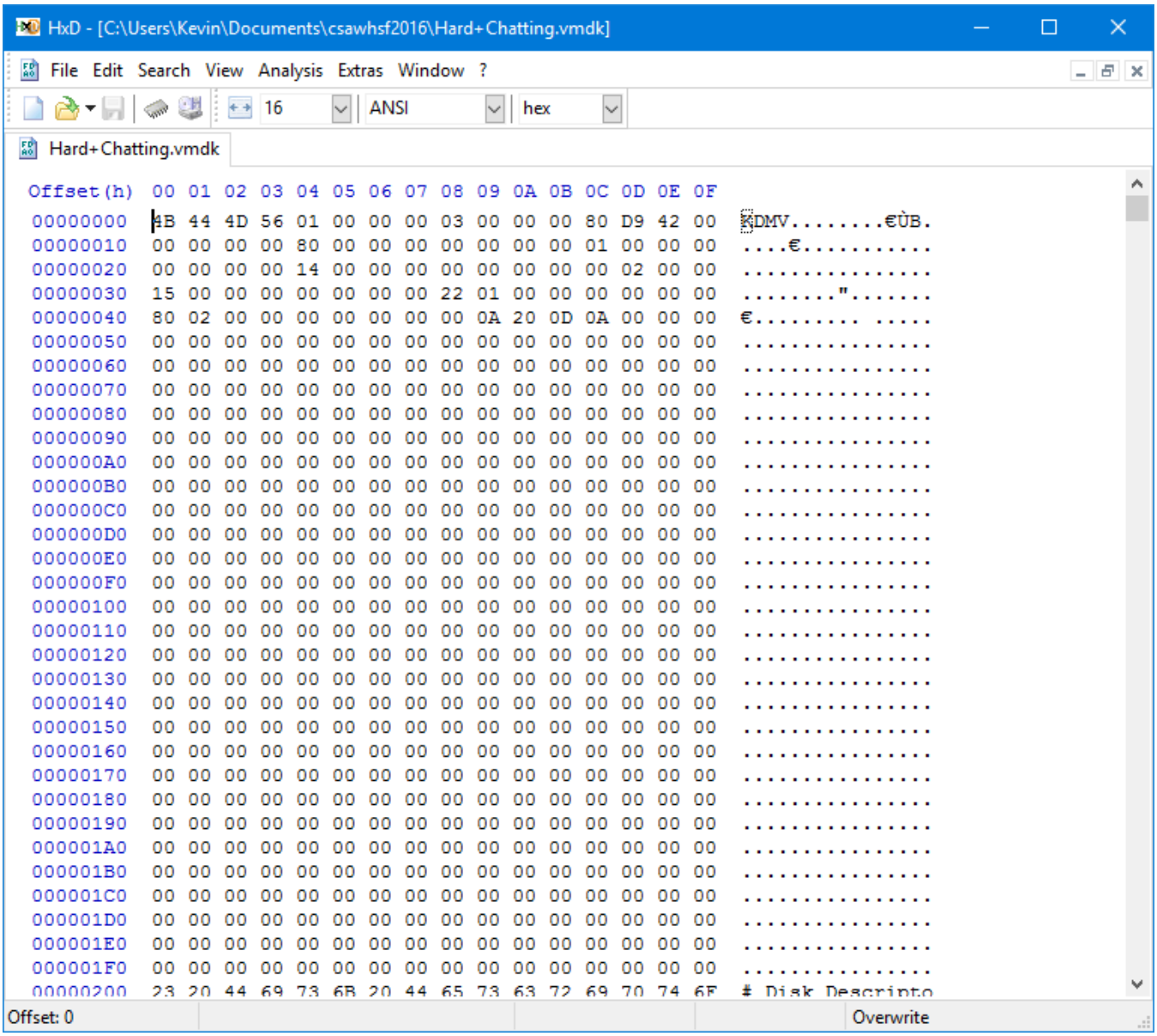
https://s3.amazonaws.com/hsf2016/Hard+Chatting.vmdk
Hash: `7a6346913d2f46cabf5120517fff94f6`

Challenge by Gus Naughton

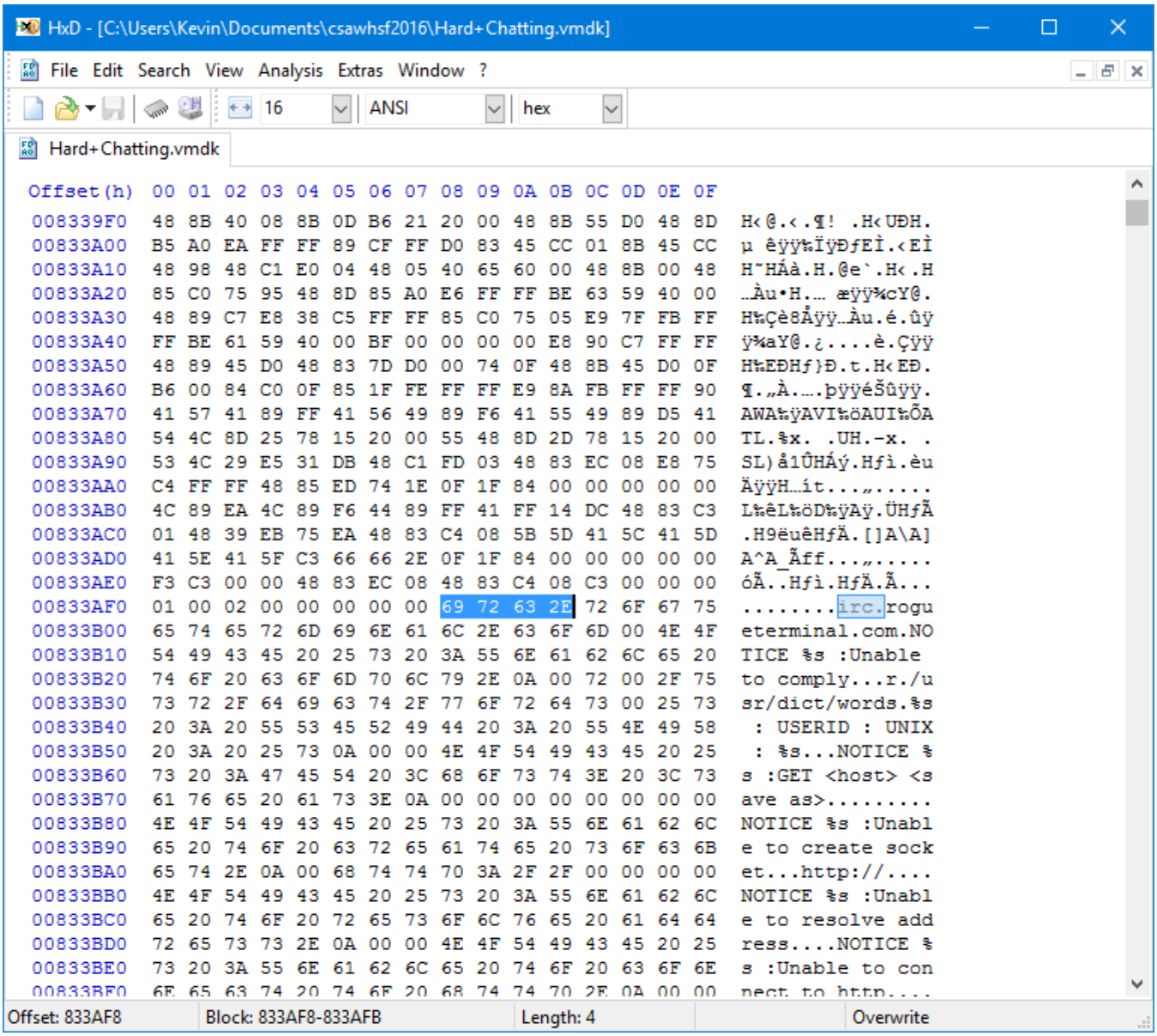
---

## Writeup

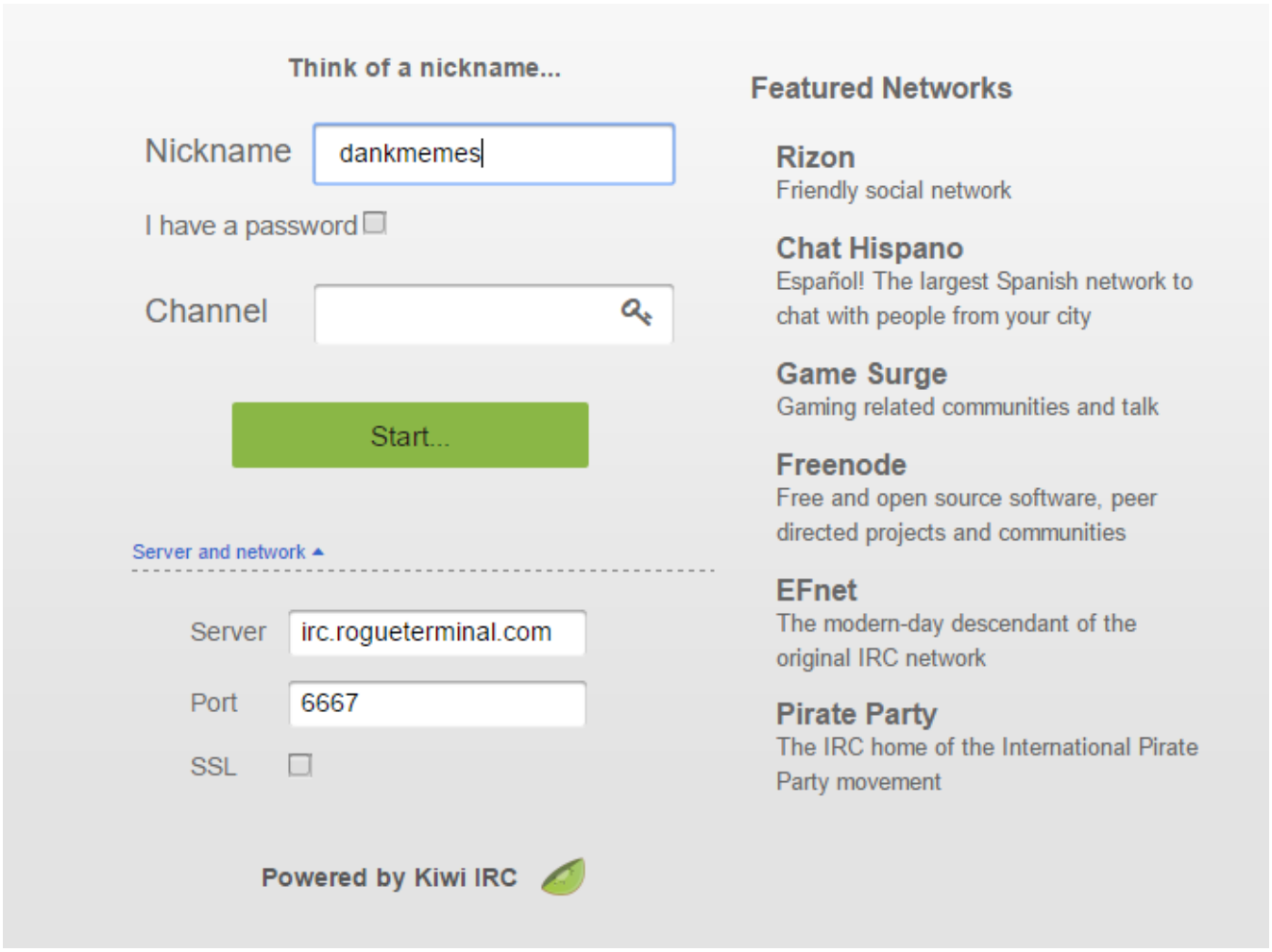
1. First, we download the VMDK. A VMDK is a virtual machine file, and is normally loaded by a virtualization software like VMWare or Virtualbox. However, this file format often stores user files uncompressed, so any data we want could be found within a hex editor, or even in plaintext. As such, we open it with our hex editor of choice (I used HxD).

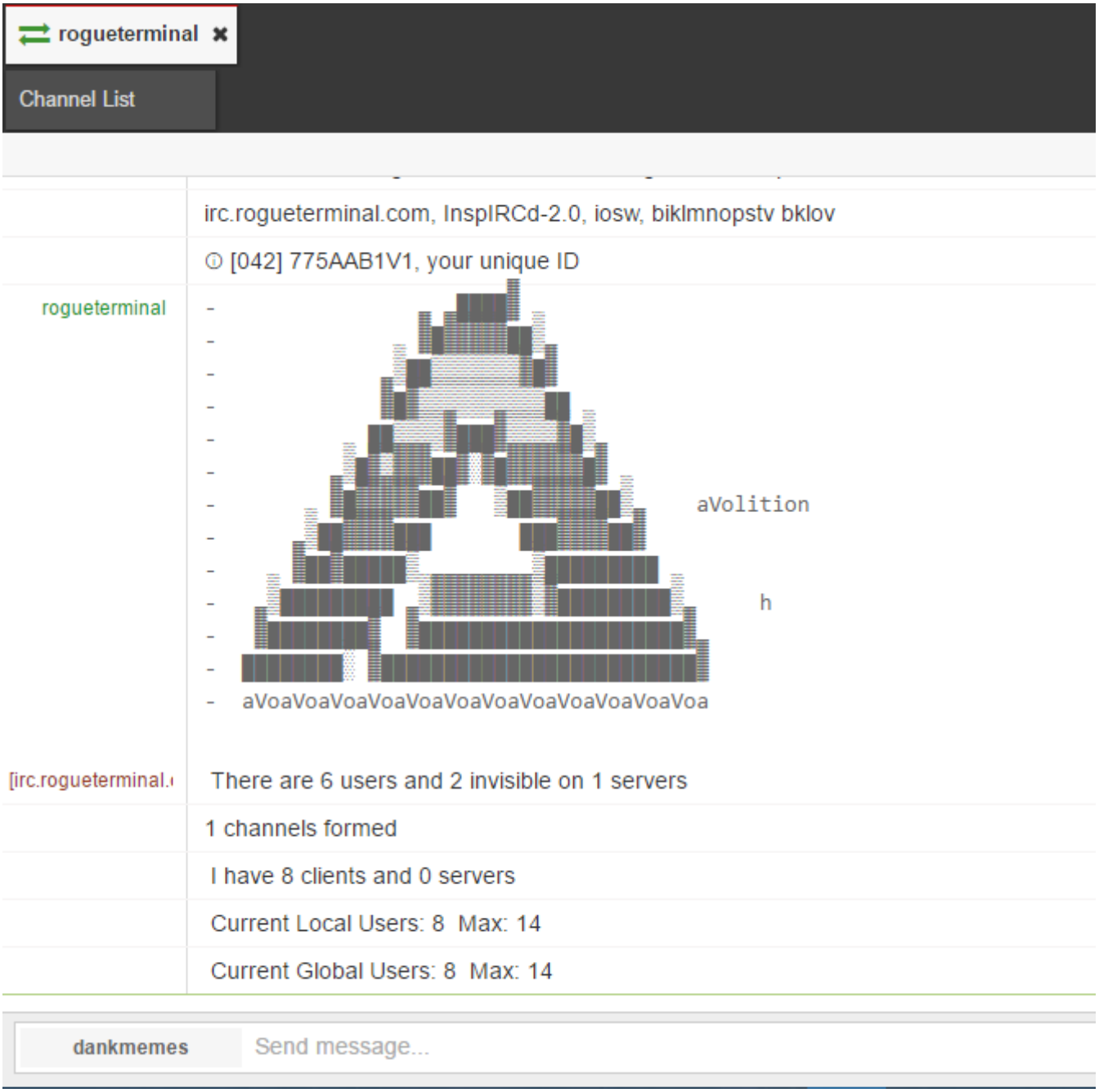



2. Based on the problem description and title, we can infer that the problem has something to do with chatting, or IRC (internet relay chat). We CTRL+F `irc.` to find irc related things (the reason the . is there is to eliminate all words that just have the substring “irc” in them, and because most IRC servers use irc.servername.net format. As such, we can possibly find some sort of IRC server that might have been used).

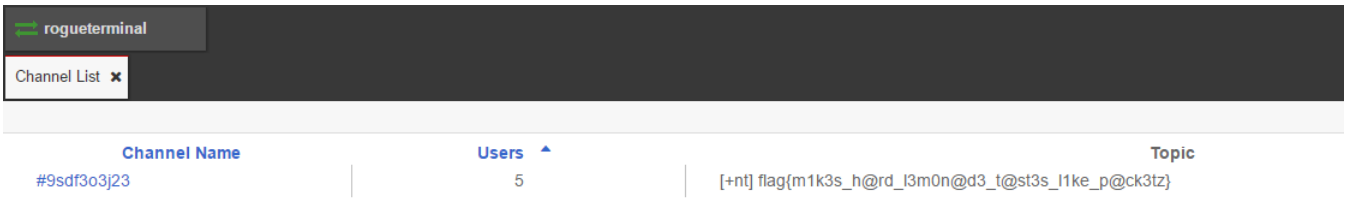



3. Luckily for us, it seems like our hunch was correct that something was going on with IRC, as we quickly find `irc.rogueterminal.net`. We can connect to this IRC server on port `6667` (the default for non-SSL IRC).


Think of a nickname...
Nickname
dankmemes
I have a password
Channel
Start...
Server and network
Server
irc.rogueterminal.com
Port
6667
SSL
Powered by Kiwi IRC
Featured Networks
Rizon
Friendly social network
Chat Hispano
Español! The largest Spanish network to chat with people from your city
Game Surge
Gaming related communities and talk
Freenode
Free and open source software, peer directed projects and communities
EFnet
The modern-day descendant of the original IRC network
Pirate Party
The IRC home of the International Pirate Party movement




4. Once we're in, we can run `/list` to get a list of channels. The only channel has the flag as its channel topic.




Flag: `flag{m1k3s_h@rd_l3m0n@d3_t@st3s_l1ke_p@ck3tz}`