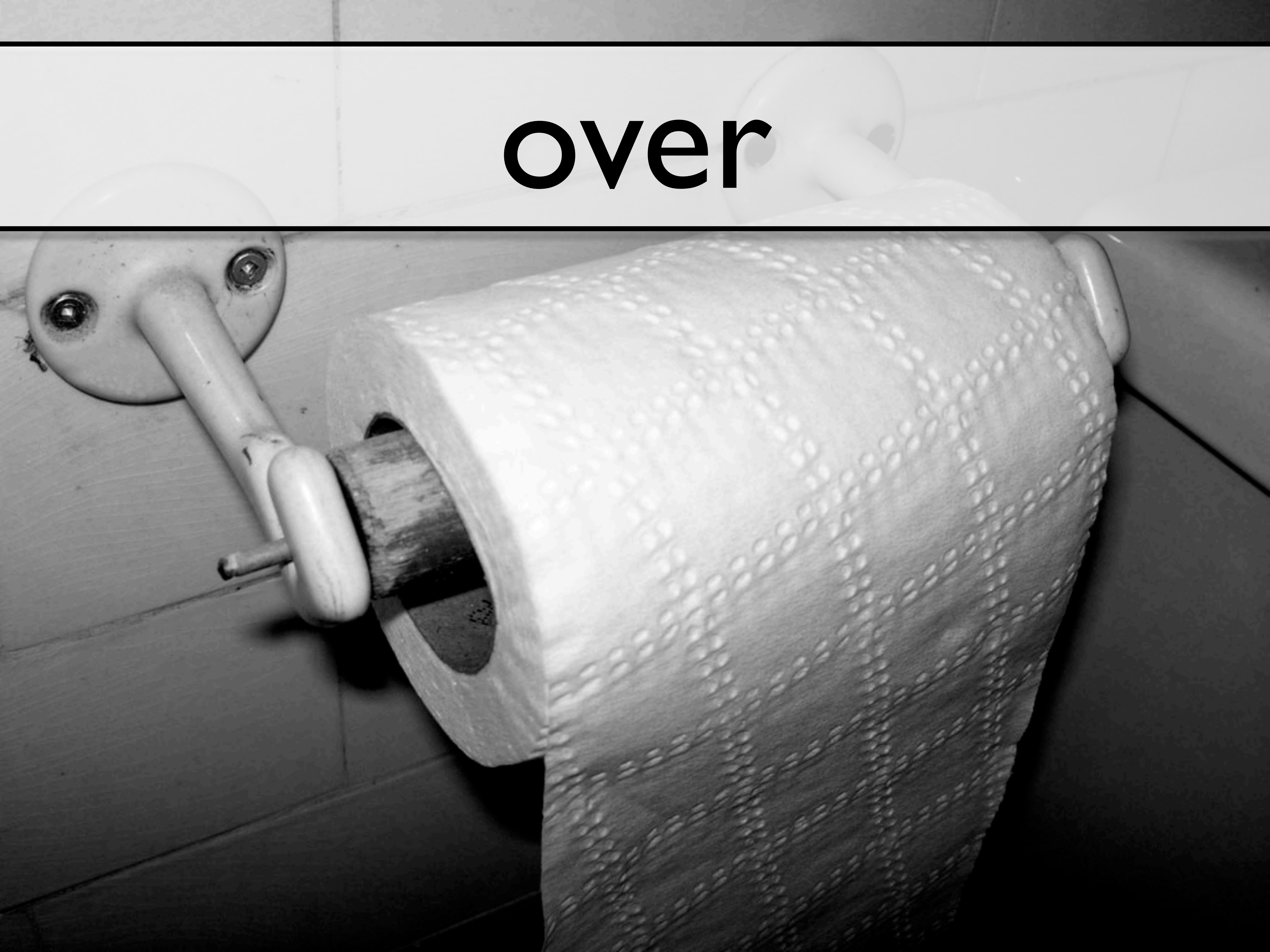
Maximum CTF

Get the most from capture the flag

place holder for warm-up quiz

psifertex

TM



over

Vim

Emacs

I’m old fashioned.__I use two spaces.

```
#!/bin/bash
```

PEPSI

Coca-Cola

DEFCON

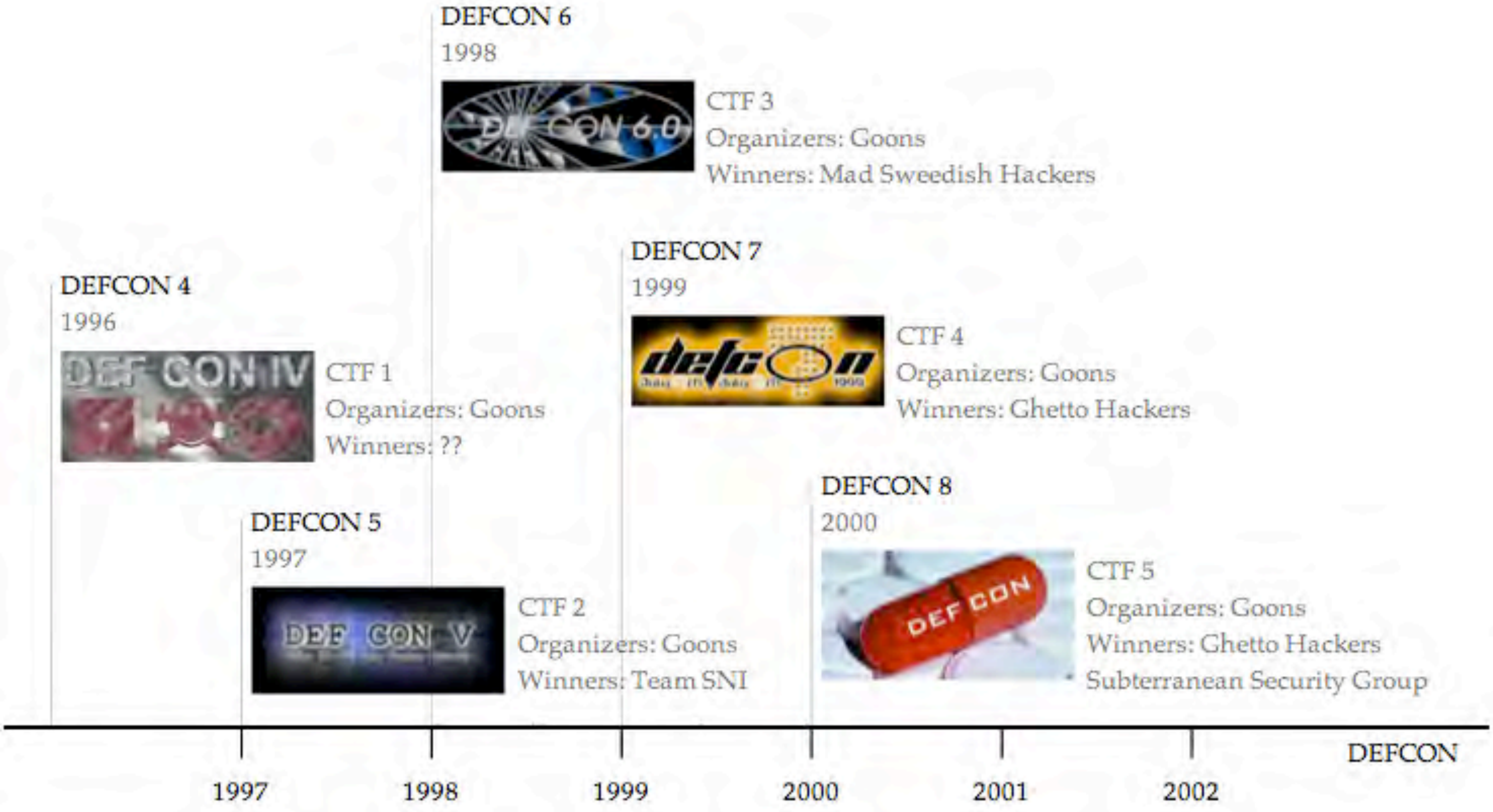
our team captain's
handle is "@tlas"

1@stplace

the team name can be
read "last place" or
"first place",
ambiguously

we wanted to cover
our bases

if the replacement of
letters with numbers and
symbols doesn't make
sense to you, it's probably
best to just leave the
room now



DEFCON 4
1996

CTF 1
Organizers: Goons
Winners: ??

DEFCON 5
1997

CTF 2
Organizers: Goons
Winners: Team SNI

DEFCON 6
1998

CTF 3
Organizers: Goons
Winners: Mad Sweedish Hackers

DEFCON 7
1999

CTF 4
Organizers: Goons
Winners: Ghetto Hackers

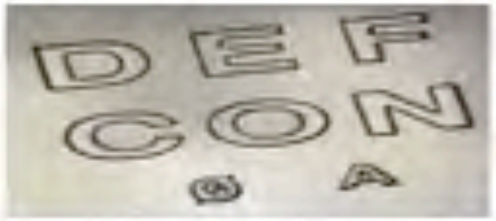
DEFCON 8
2000

CTF 5
Organizers: Goons
Winners: Ghetto Hackers
Subterranean Security Group

DEFCON 9
2001

CTF 6*
Organizers: Goons
Winners: Ghetto Hackers
Digital Revelation

DFECON 10
2002



CTF 7
Organizers: Ghetto Hackers
Winners: Digital Revelation

DEFCON 11
2003

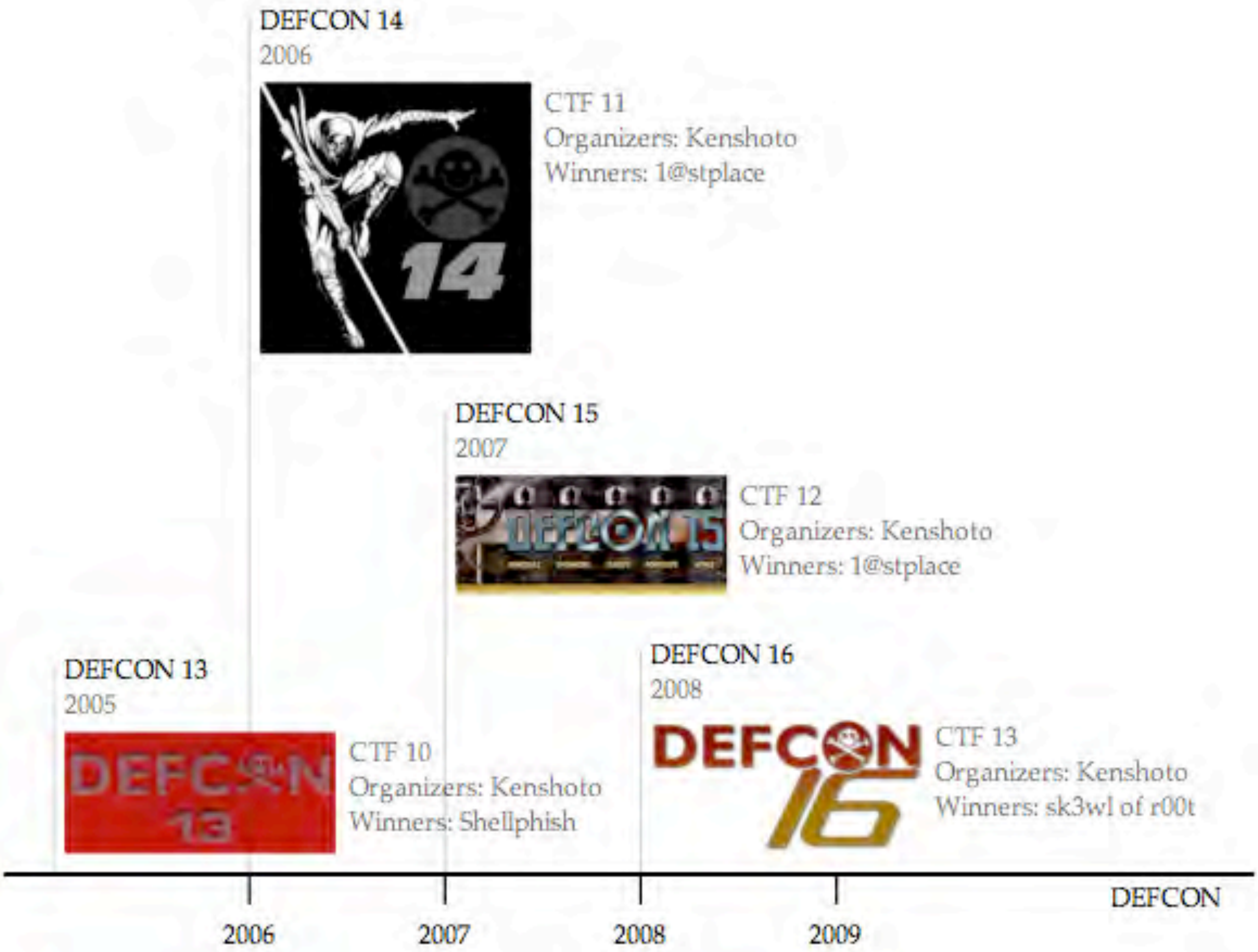
CTF 8
Organizers: Ghetto Hackers
Winners: Digital Revelation

DEFCON 12
2004

CTF 9
Organizers: Ghetto Hackers
Winners: Sk3wl of R00t

2002 2003 2004 2005 2006

DEFCON



DEFCON 13
2005
CTF 10
Organizers: Kenshoto
Winners: Shellphish

DEFCON 14
2006
CTF 11
Organizers: Kenshoto
Winners: 1@stplace

DEFCON 15
2007
CTF 12
Organizers: Kenshoto
Winners: 1@stplace

DEFCON 16
2008
CTF 13
Organizers: Kenshoto
Winners: sk3wl of r00t

DEFCON
17
I AM NINJA
BEER

Diutinus Defense Technologies Corp.

- Number of people in your organization (that will actively be participating in creating/planning/executing CTF):
20

- Experience team members have had in planning events (This could be a bake sale with 500 people, or a DoD briefings for 20 people, something that indicates some planning experience):

Coordination for training events for 40+ individuals.
Coordination semi-annual meeting of 20 corporation CEO's.
Coordination for activities of small groups of hackers to participating in ctf.
Experience with leadership of diverse hacking groups, attack forces and defensive forces
Experience with add-hoc generation of task teams to meet game or crisis needs
Access to a wide array of people which can be leveraged at and before con to problem solving and challenge meeting associated with the new CTF game.

- Technical ability of team. This would include a general list of people's abilities * networking, hardware, etc and support the idea you can pull this off:

Several professional developers of networks wireless
Two sometimes professional engineers of networks
Several professional security researchers/forensics analysts
One amateur sheep luuuuuva
Other really smart people

- Physical resources (if any) that you will be bringing to help run CTF such as a disco ball, robots or enigma machines. This to help us plan to accommodate it with the hotel if you require extra power or special fire marshal approval for your Cray 1 cooling towers.:

~10 servers
~3 routers
~1.7 chemistry sets (GHB and Vitamin K synthesis for sheep luuuuuva)

- What experience have your team members had in playing CTF in the past. This is not a requirement, but shows real-world knowledge of the game as it has been played in the past.:

Occasional participants in defcon CTFs over the many years. Some participation in other (not-defcon) CTF type exercises

- Explain you vision for CTF -Explain, in a general manner, your vision of your CTF.

We view the CTF as the venue for real hackers to demonstrate/practice their skills at breaking into computers by remote. While we recognize that there are many skills to hacking such as social engineering, lock picking and more we think that some of these skills are already tested in other contests running at Defcon. While other contests may be combined in some capacity, they will not be a core focus of our flavour of CTF.

- Explain how you hope the attendees will experience it. For example, they sign up on-line, get a secret package in the mail, start blindfolded with an unusual laptop? Are their certain crises points you will introduce during the game to confuse or add to the pressure?

Attendees wishing to participate in the team portion of CTF will be required to register in advance in order to participate in the team qualifying round expected to take place approximately 2 months prior to Defcon. We anticipate accepting nine teams (plus returning champion) into the team competition to take place over the three days of Defcon. An individual competition organized similar to the qualifying round may be also offered during the con. Such an individual round could be entered by anyone choosing to register at Defcon. The individual competition would be accessed on the conference wireless with a scoreboard displaying the current individual leader board in the CTF arena. Teams may be required to overcome some initial challenge such as picking a lock to obtain access to their network feed into the game. A mob style element may be introduced by providing a game connection to the chill out area/amateur ctf tables. The mob would effectively be a non-scoring team capable of attacking all of the other teams and introducing general mayhem (other than DoS attacks which will not be acceptable. Too great bandwidth consumption by the mob will result in disconnection. We are not interested in seeing a bunch of nmap/nessus scans against the game network.

-Provide three reasons your group should host CTF.

1. We have enjoyed playing and observing CTF over the years and would like to give something back to the community.
2. We feel that the perspective we have gained as players will offer us the best opportunity to make a game that agrees to the spirit of CTF, incorporating the best of what we have experienced, with fresh ideas gained from an detailed knowledge of the game that only players could appreciate.
3. We have no commercial interest in the game and are doing this not for personal gain.
4. We don't really want to play a game not hosted by Kenshoto so we thought we might try to running the thing ourselves.

-How do players or teams qualify (if there are qualifications)?

As like the past, the qualification round will consist of a point oriented competition with wide variety of topics and exercising a wide variety of skills. The challenges will take the form of a Jeopardy style board. The nine top scoring teams will be offered spots to CTF. Ties will be broken by the first team to reach the score. Qualifying teams will have two weeks to confirm to CTF. After two weeks, any teams that have not confirmed their intention to participate at Defcon will lose their spot in the game and the next available team as determined by qualifying score will be offered a chance to participate in CTF.

-Is it multi player or single-player, or a combination?

We intend to maintain the team oriented aspect of the game while introducing an individual part to the game as a way to get more interest from Defcon attendees. A prize may be set aside for the winner of the individual competition.

-What innovations or new ideas are you bringing to CTF?

We intend to bring a new scoring system to the game with different visualization for the game activities. Additionally, there may be side challenges designed to mix things up a bit and test the diversity of each teams skills. Unlike recent years, we hope to make teams to defend multiple servers running different operating systems. In order to attract more attendees to the game we hope to make several opportunities for attendees to drop in and play in some way.

-How long will the contest take, will it be 24x7, 8 hour shifts, etc?

26 total hours. 10 hours Friday, 10 hours Saturday, and 6 hours Sunday.

-What technical work is required to execute your plan. This includes setting up environments beforehand, pre-qualification work if any, writing a scoring system, etc.?

Qualifications and the actual CTF competition will each require setup.

Quals will require making questions/challenges and answers as well as communications channels, web pages and score viewing methods.

CTF will require the setup of multiple environments including scoring, display and target services.

-Give an outline of the rules that will be presented to the participants:

Generally we're finding rules to be superficial, as such we don't intend to enforce many.

Rough outline:
No DoS. Windows is better!
No nmap/nessus scanning (they won't get you anything anyway)
Table limit of 8 enforced
No physical coercion (sheep excepted).

Quals:
We will conduct the qualifications in a similar manner as the previous Kenshoto CTF organizers to choose skilled teams for the purpose of supplying the eventual CTF competition with the most highly skilled players. The quals will include real time chat and multiple challenges with skill requirements similar to the skills required in CTF.

CTF:
All competing teams will be supplied with the same challenges at the same time or have equal opportunity to gain points or make progress. Simple game rules will be supplied in printed or digital form to ease potential language barrier issues.

-Why do you want to do this?

See section "Provide three reasons your group should host CTF."

-Explain what you believe is the best way to gauge a hacker's abilities, and how your vision of the contest could do this?

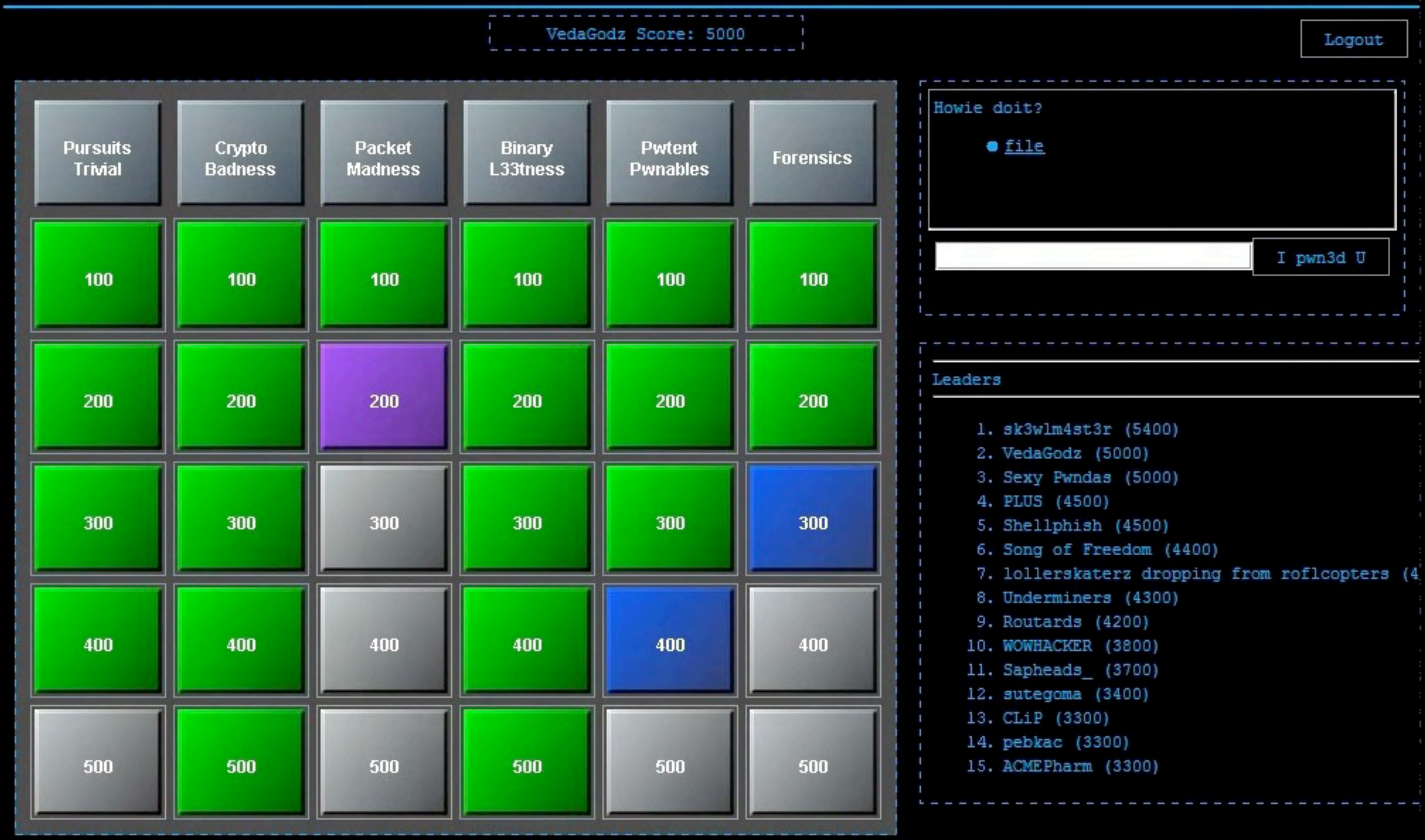
Cross between depth of skill and breadth of skill.
Team flexibility
Team diversity
Parallels with either business or national capability
Ability to pick up sheep

CTF has traditionally been oriented around computer network attack and defense. While we recognize that there are many other areas of interest within the hacking community, we feel that many of these areas are well tested by other Defcon contests, and we would like to continue the tradition of Defcon hosting the premiere CTF event. The primary focus of the game will be software exploiting. Some side challenges may use other areas of hacking such as lock picking. Our type of the game would present approximately 15 network based services for each team to attack. Vulnerabilities made into the services would range in difficulty from simple stack overflows to more complex heap overflows and cryptographic challenges.

-Tell us anything else that you think may be important or that we might consider in choosing your group to host CTF.

You know us and our intentions/culture Our priorities lie with the reputation and progress of the game and the conference rather than in the furtherance of commercial interests.

Te amo en la noche,
Te amo en la mañana.
Me largo para que cuando fuera,
Oh ovejas de hacer lo de banana.



VedaGodz Score: 5000

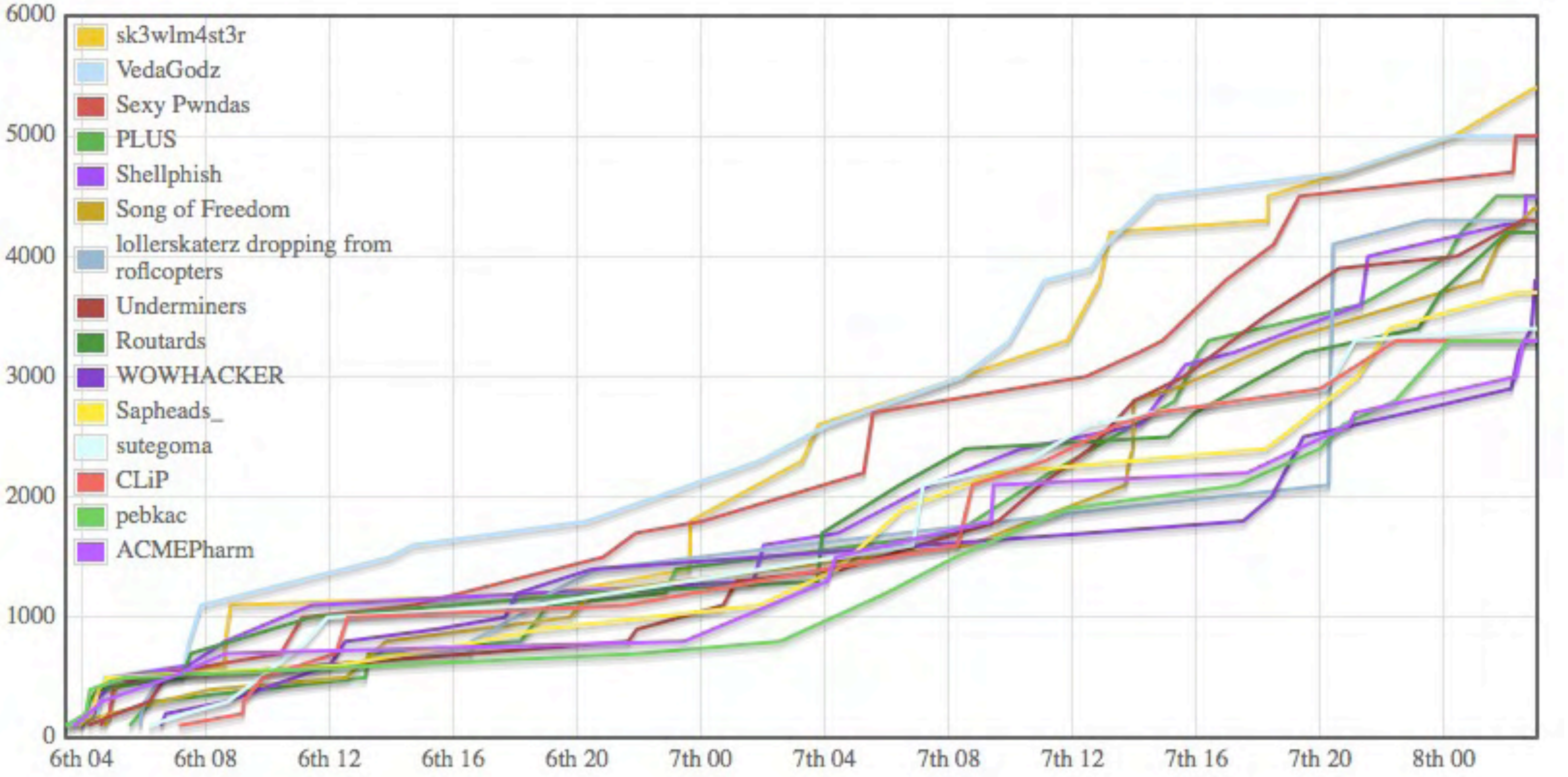
Pursuits Trivial	Crypto Badness	Packet Madness	Binary L33tness	Pwtent Pwnables	Forensics
100	100	100	100	100	100
200	200	200	200	200	200
300	300	300	300	300	300
400	400	400	400	400	400
500	500	500	500	500	500

Howie doit?

- file

Leaders

1. sk3wlm4st3r (5400)
2. VedaGodz (5000)
3. Sexy Pwndas (5000)
4. PLUS (4500)
5. Shellphish (4500)
6. Song of Freedom (4400)
7. lollerskaterz dropping from roflcopters (4
8. Underminers (4300)
9. Routards (4200)
10. WOWHACKER (3800)
11. Sapheads_ (3700)
12. sutegoma (3400)
13. CLiP (3300)
14. pebkac (3300)
15. ACMEPharm (3300)

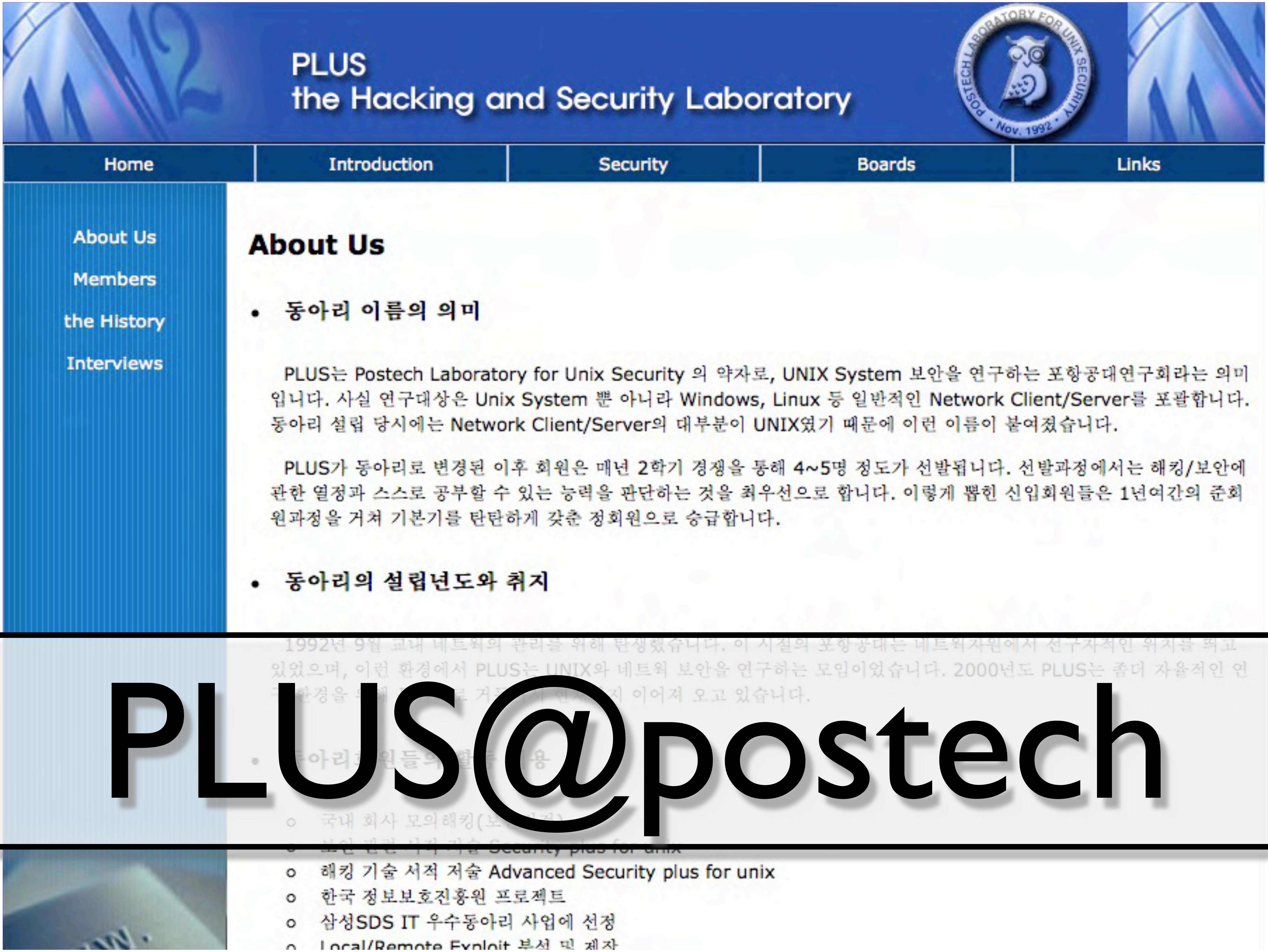

6000
5000
4000
3000
2000
1000
0
sk3wlm4st3r
VedaGodz
Sexy Pwndas
PLUS
Shellphish
Song of Freedom
lollerskaterz dropping from roflcopters
Underminers
Routards
WOWHACKER
Sapheads_
sutegoma
CLiP
pebkac
ACMEPharm
6th 04
6th 08
6th 12
6th 16
6th 20
7th 00
7th 04
7th 08
7th 12
7th 16
7th 20
8th 00

sk3wl of r00t

team awesome

sexy pandas

PLUS@postech


PLUS
the Hacking and Security Laboratory
POSTECH LABORATORY FOR UNIX SECURITY · Nov. 1992 ·
Home
Introduction
Security
Boards
Links
About Us
Members
the History
Interviews

About Us

- 동아리 이름의 의미

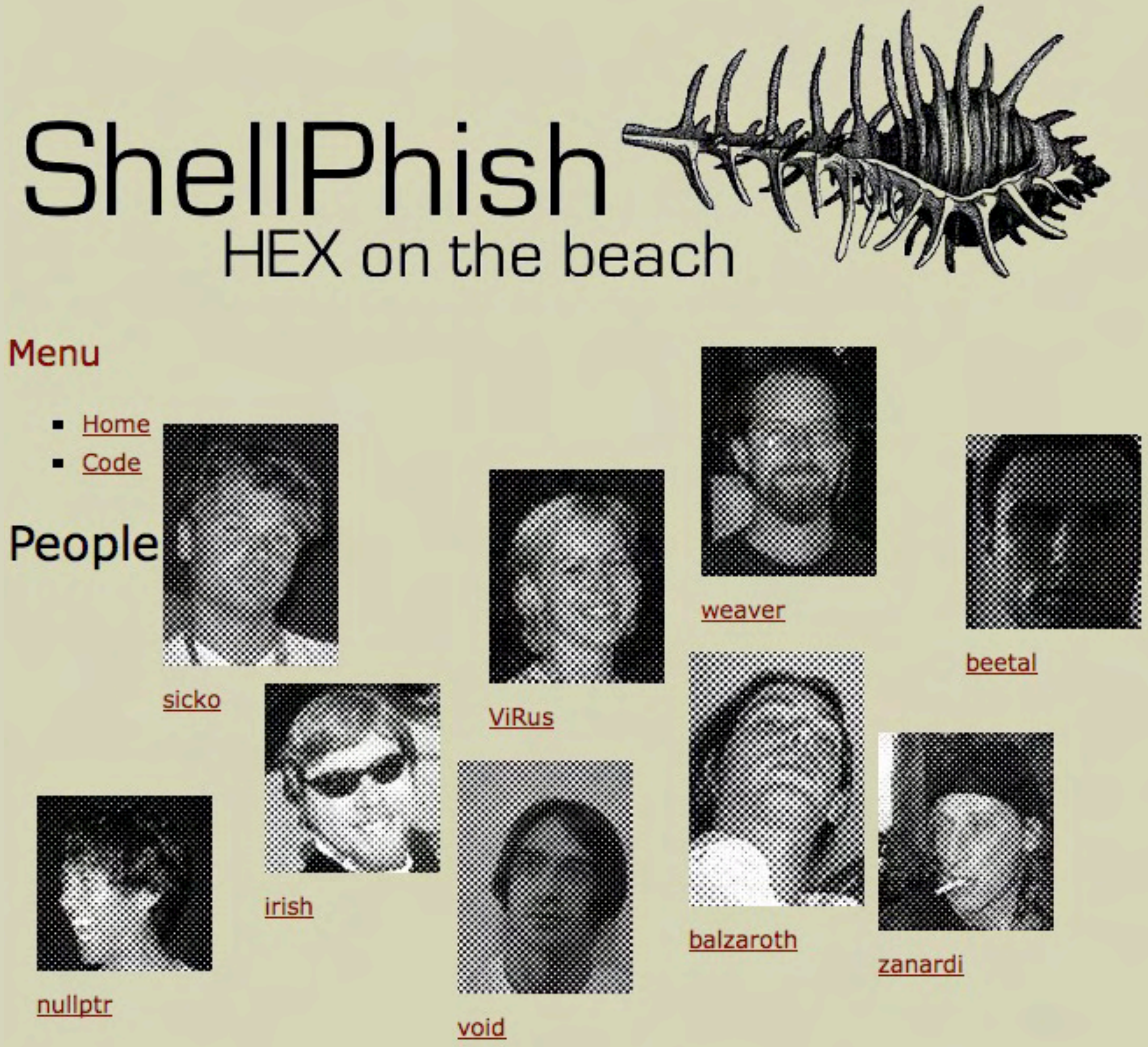
PLUS는 Postech Laboratory for Unix Security 의 약자로, UNIX System 보안을 연구하는 포항공대연구회라는 의미입니다. 사실 연구대상은 Unix System 뿐 아니라 Windows, Linux 등 일반적인 Network Client/Server를 포괄합니다. 동아리 설립 당시에는 Network Client/Server의 대부분이 UNIX였기 때문에 이런 이름이 붙여졌습니다.

PLUS가 동아리로 변경된 이후 회원은 매년 2학기 경쟁을 통해 4~5명 정도가 선발됩니다. 선발과정에서는 해킹/보안에 관한 열정과 스스로 공부할 수 있는 능력을 판단하는 것을 최우선으로 합니다. 이렇게 뽑힌 신입회원들은 1년여간의 준회원과정을 거쳐 기본기를 탄탄하게 갖춘 정회원으로 승급합니다.

- 동아리의 설립년도와 취지

1992년 9월 교내 네트워크의 관리를 위해 탄생했습니다. 이 시절의 포항공대는 네트워자원에서 선구자적인 위치를 띄고 있었으며, 이런 환경에서 PLUS는 UNIX와 네트워 보안을 연구하는 모임이었습니다. 2000년도 PLUS는 좀더 자율적인 연구환경을 [illegible] 거듭[illegible] 현재[illegible]지 이어져 오고 있습니다.

- [illegible]아리 [illegible]원들의 활동 [illegible]용
  - 국내 회사 모의해킹(보[illegible])
  - 보안 관련 서적 저술 Security plus for unix
  - 해킹 기술 서적 저술 Advanced Security plus for unix
  - 한국 정보보호진흥원 프로젝트
  - 삼성SDS IT 우수동아리 사업에 선정
  - Local/Remote Exploit 분석 및 제작



ShellPhish

HEX on the beach

Menu

- Home
- Code

People

sicko

ViRus

weaver

beetal

irish

nullptr

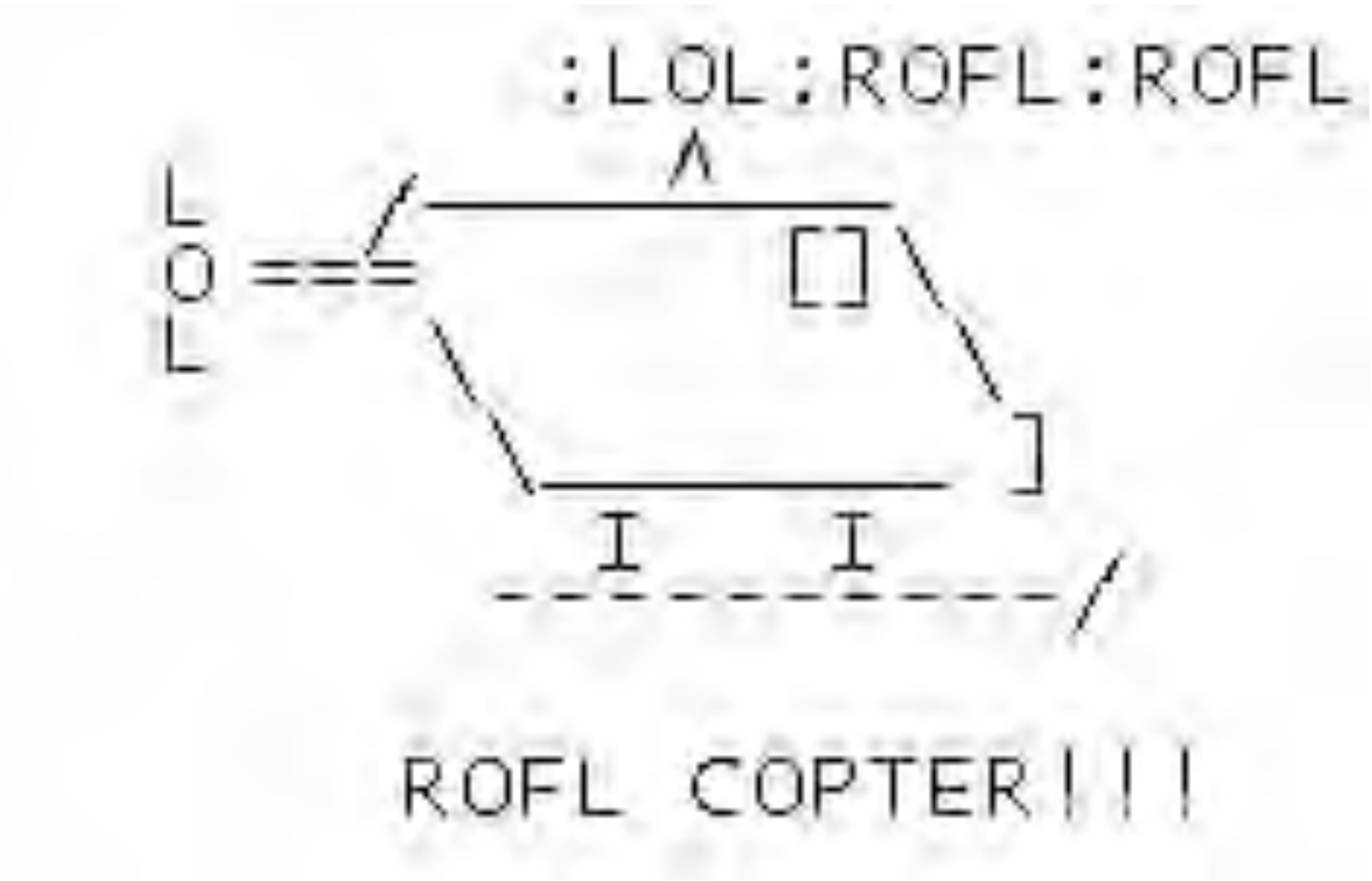
void

balzaroth

zanardi

song of
freedom
송오브프리덤

lollerskaterz dropping from roflcopters

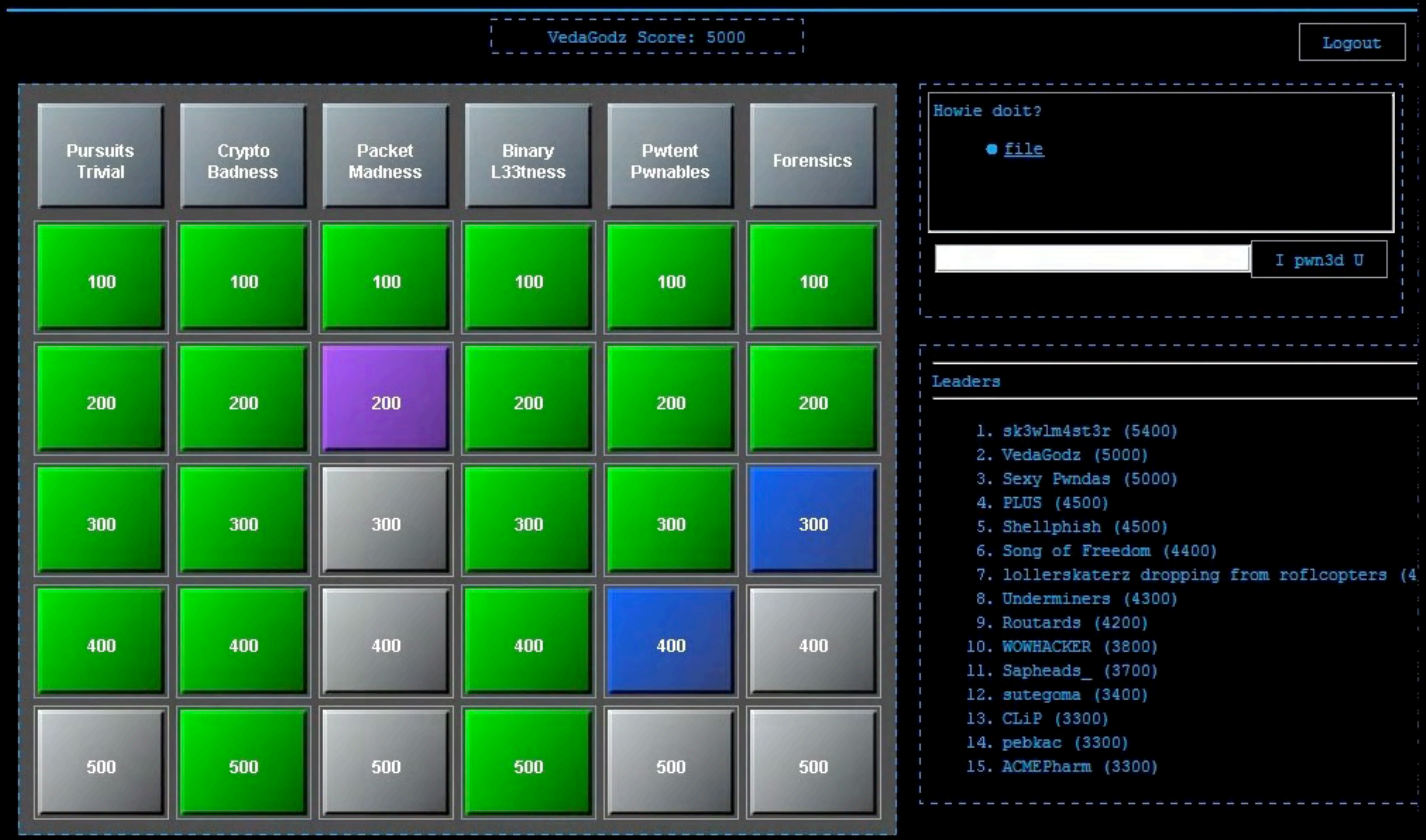


routards

WOWHACKER

sapheads

mechanics



VedaGodz Score: 5000

Pursuits Trivial	Crypto Badness	Packet Madness	Binary L33tness	Pwtent Pwnables	Forensics
100	100	100	100	100	100
200	200	200	200	200	200
300	300	300	300	300	300
400	400	400	400	400	400
500	500	500	500	500	500

Howie doit?

- file

Leaders

```
 1. sk3wlm4st3r (5400)
 2. VedaGodz (5000)
 3. Sexy Pwndas (5000)
 4. PLUS (4500)
 5. Shellphish (4500)
 6. Song of Freedom (4400)
 7. lollerskaterz dropping from roflcopters (4
 8. Underminers (4300)
 9. Routards (4200)
10. WOWHACKER (3800)
11. Sapheads_ (3700)
12. sutegoma (3400)
13. CLiP (3300)
14. pebkac (3300)
15. ACMEPharm (3300)
```

flags

Roles

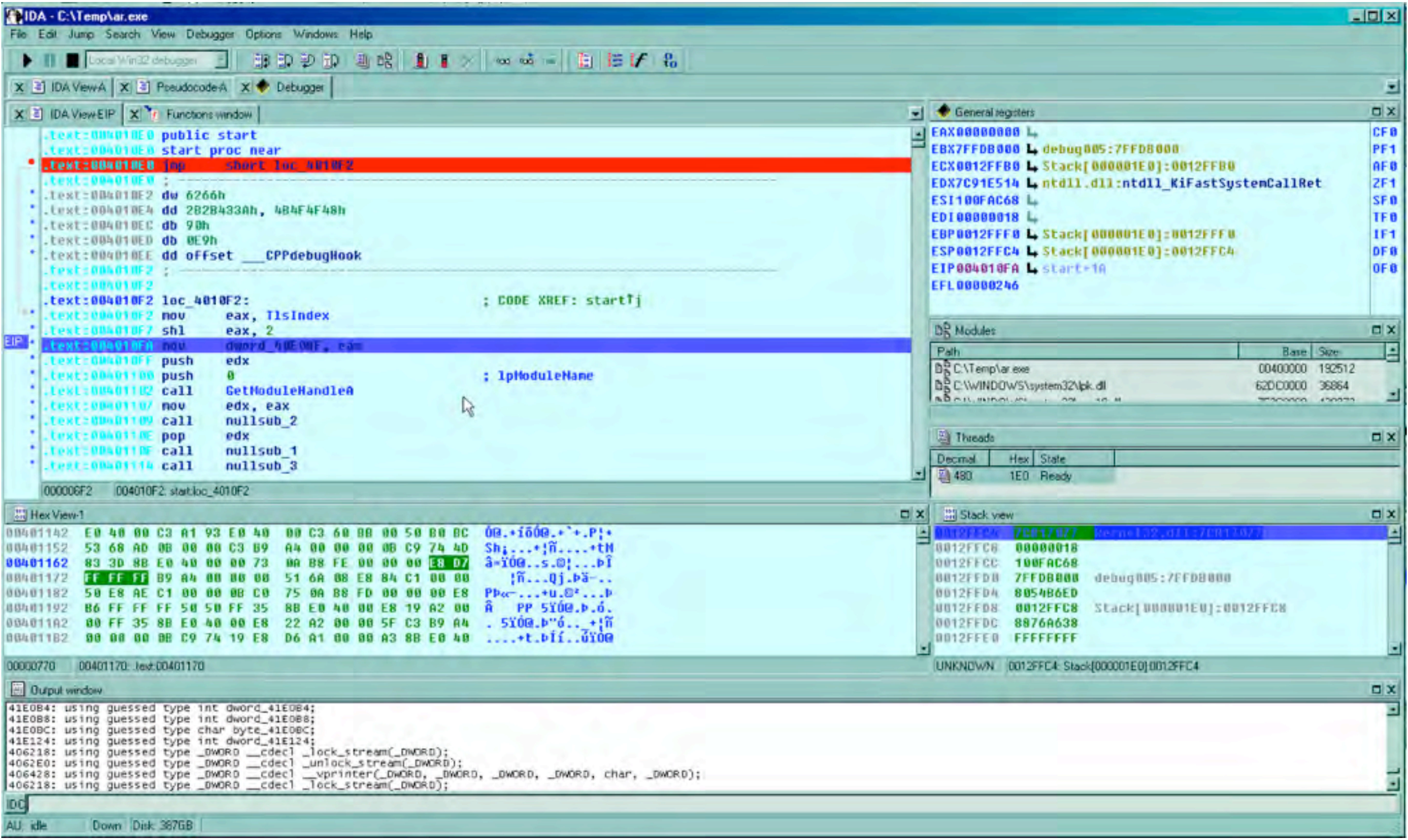
“Coordinator”
“Nose”
“Reverser”
“Exploiter”
“Sysadmin”
“Defender”
“Scripter”

teamwork

Team Size

Skillz

HackerTrivia
PackerDefeats
Phreaking
PHP
octal
Off-by-one
Trickiness
fileformats
Vulnerabilities
networkprotocols
BufferOveflows
PowerPC
Pwnage
OperatingSystemFundamentals
Exploitation
ByteCodeDecompilation
C++
x86
hex
binary
Encryption
BinaryProtection
Decompilation
Python
reverseengineering
Debuggers
ARM
Cryptography
PPC
assembly
EncodingMethods
GoogleFOO
hacking
VirtualMachines
Disassemblers
Shellcode
L33tness
ArcaneArchitectures
RFCReadingComprehension



```
.text:004010E0 public start
.text:004010E0 start proc near
.text:004010E0 jmp     short loc_4010F2
.text:004010E0 ; ---------------------------------------------------------------------------
.text:004010E2 dw 6266h
.text:004010E4 dd 2B2B433Ah, 484F4F48h
.text:004010EC db 90h
.text:004010ED db 0E9h
.text:004010EE dd offset ___CPPdebugHook
.text:004010F2 ; ---------------------------------------------------------------------------
.text:004010F2
.text:004010F2 loc_4010F2:                              ; CODE XREF: start↑j
.text:004010F2 mov     eax, TlsIndex
.text:004010F7 shl     eax, 2
.text:004010FA mov     dword_40E00F, eax
.text:004010FF push    edx
.text:00401100 push    0                                ; lpModuleName
.text:00401102 call    GetModuleHandleA
.text:00401107 mov     edx, eax
.text:00401109 call    nullsub_2
.text:0040110E pop     edx
.text:0040110F call    nullsub_1
.text:00401114 call    nullsub_3
```

000006F2 004010F2: start:loc_4010F2

```
EAX00000000 ↳                                        CF0
EBX7FFDB000 ↳ debug005:7FFDB000                      PF1
ECX0012FFB0 ↳ Stack[000001E0]:0012FFB0               AF0
EDX7C91E514 ↳ ntdll.dll:ntdll_KiFastSystemCallRet    ZF1
ESI100FAC68 ↳                                        SF0
EDI00000018 ↳                                        TF0
EBP0012FFF0 ↳ Stack[000001E0]:0012FFF0               IF1
ESP0012FFC4 ↳ Stack[000001E0]:0012FFC4               DF0
EIP004010FA ↳ start+1A                               OF0
EFL00000246
```

Path	Base	Size
C:\Temp\ar.exe	00400000	192512
C:\WINDOWS\system32\lpk.dll	62DC0000	36864

Decimal	Hex	State
480	1E0	Ready

```
00401142  E0 40 00 C3 A1 93 E0 40  00 C3 60 B8 00 50 B0 BC  Ó@.+íôÓ@.+`+.P¦+
00401152  53 68 AD 0B 00 00 C3 B9  A4 00 00 00 0B C9 74 4D  Sh¡...+¦ñ....+tM
00401162  83 3D 8B E0 40 00 00 73  0A B8 FE 00 00 00 E8 D7  â=ïÓ@..s.©¦...ÞÎ
00401172  FF FF FF B9 A4 00 00 00  51 6A 08 E8 84 C1 00 00     ¦ñ...Qj.Þä-..
00401182  50 E8 AE C1 00 00 0B C0  75 0A B8 FD 00 00 00 E8  PÞ«-...+u.©²...Þ
00401192  B6 FF FF FF 50 50 FF 35  8B E0 40 00 E8 19 A2 00  Â   PP 5ïÓ@.Þ.ó.
004011A2  00 FF 35 8B E0 40 00 E8  22 A2 00 00 5F C3 B9 A4  . 5ïÓ@.Þ"ó.._+¦ñ
004011B2  00 00 00 0B C9 74 19 E8  D6 A1 00 00 A3 8B E0 40  ....+t.ÞÍí..úïÓ@
```

00000770 00401170: .text:00401170

```
0012FFC4  7C817077  kernel32.dll:7C817077
0012FFC8  00000018
0012FFCC  100FAC68
0012FFD0  7FFDB000  debug005:7FFDB000
0012FFD4  8054B6ED
0012FFD8  0012FFC8  Stack[000001E0]:0012FFC8
0012FFDC  8876A638
0012FFE0  FFFFFFFF
```

UNKNOWN 0012FFC4: Stack[000001E0]:0012FFC4

```
41E0B4: using guessed type int dword_41E0B4;
41E0B8: using guessed type int dword_41E0B8;
41E0BC: using guessed type char byte_41E0BC;
41E124: using guessed type int dword_41E124;
406218: using guessed type _DWORD __cdecl _lock_stream(_DWORD);
4062E0: using guessed type _DWORD __cdecl _unlock_stream(_DWORD);
406428: using guessed type _DWORD __cdecl __vprinter(_DWORD, _DWORD, _DWORD, _DWORD, char, _DWORD);
406218: using guessed type _DWORD __cdecl _lock_stream(_DWORD);
```

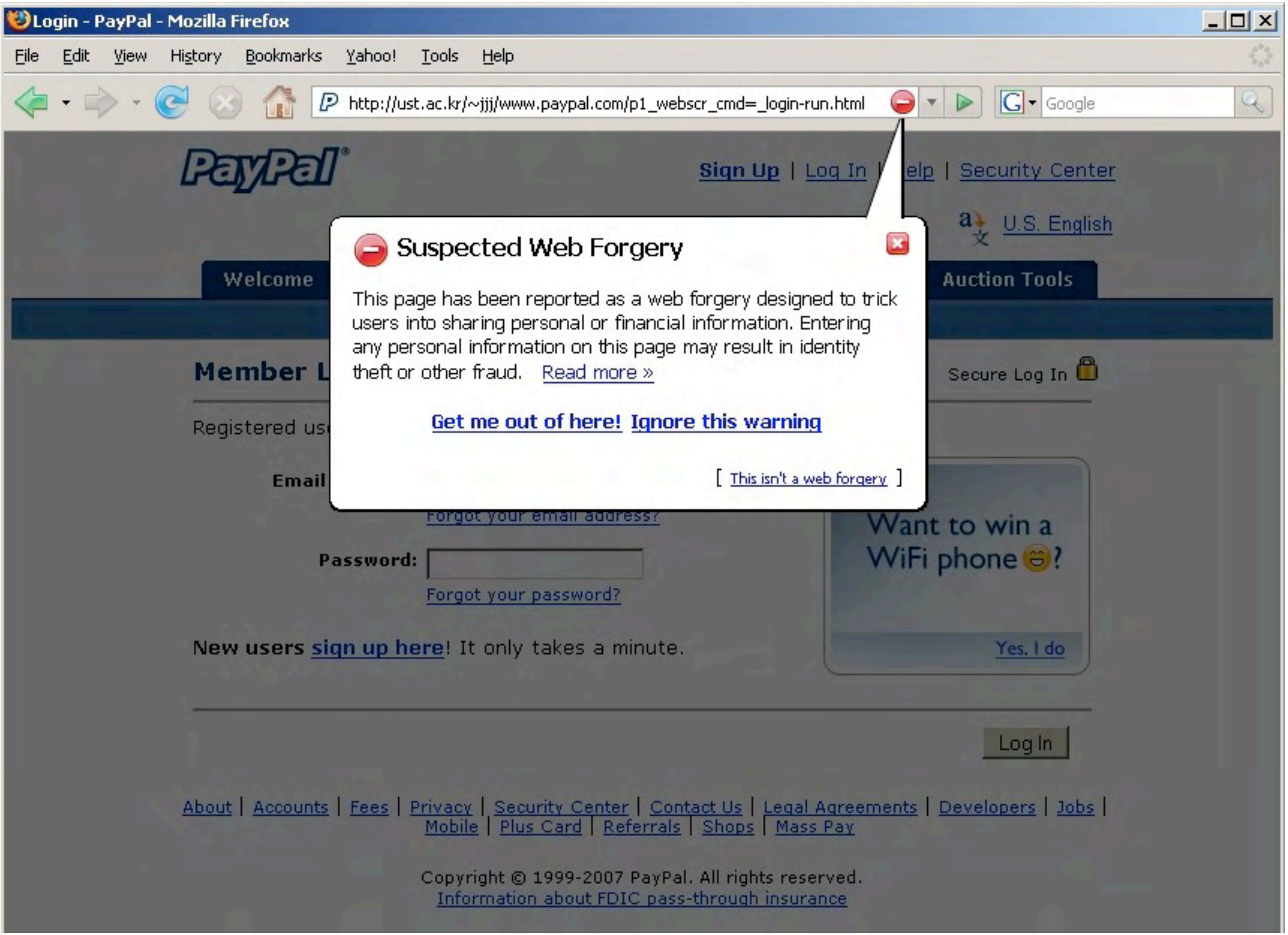
AU: idle Down Disk: 387GB

Lightning Question Placeholder

dirty tricks

only as strong as...

backdoor



Login - PayPal - Mozilla Firefox

http://ust.ac.kr/~jjj/www.paypal.com/p1_webscr_cmd=_login-run.html

Suspected Web Forgery

This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Read more »

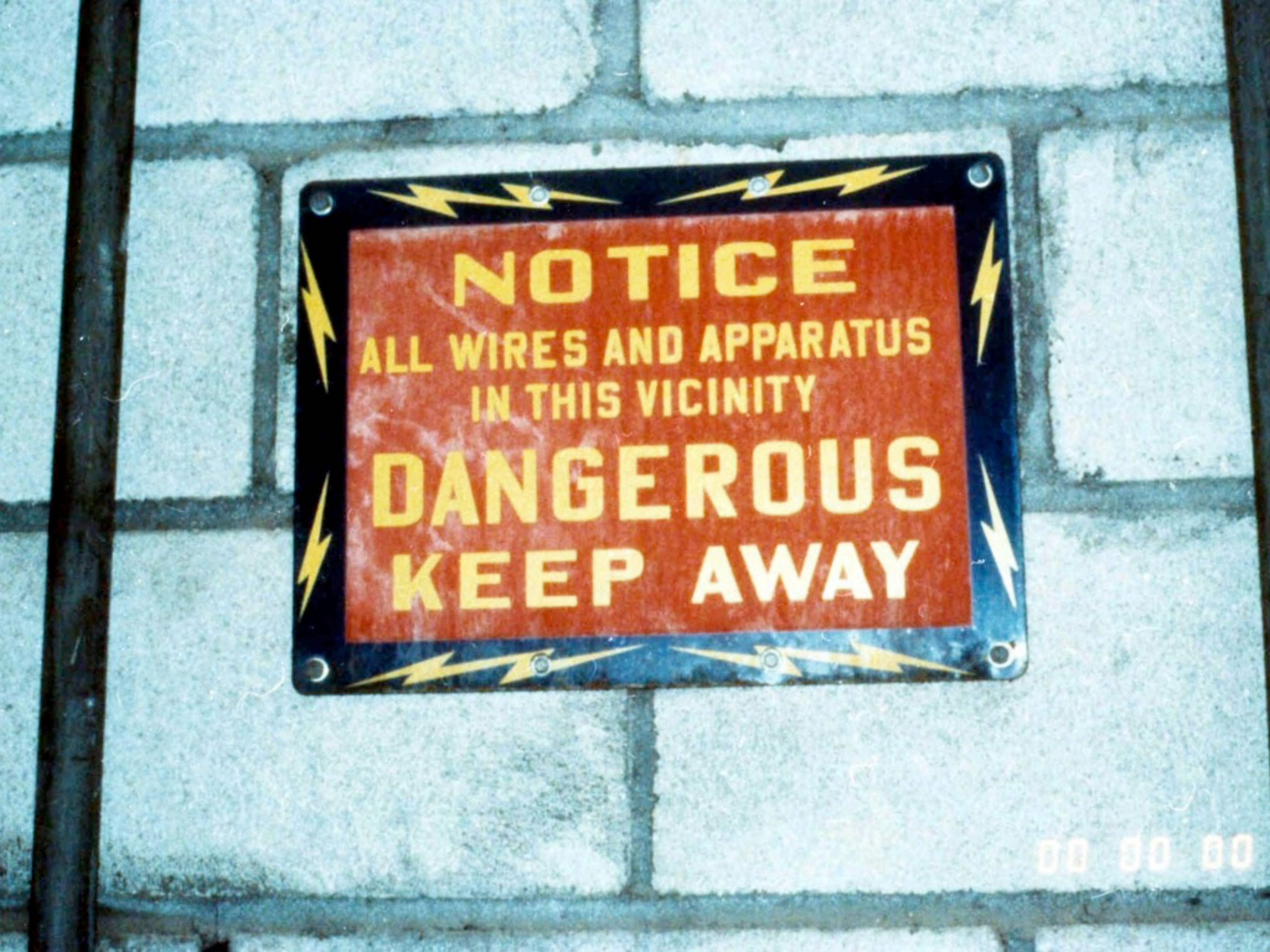
Get me out of here! Ignore this warning

[This isn't a web forgery]

New users sign up here! It only takes a minute.

Copyright © 1999-2007 PayPal. All rights reserved.
Information about FDIC pass-through insurance

File
Edit
View
History
Bookmarks
Yahoo!
Tools
Help
Google
PayPal
Sign Up | Log In | elp | Security Center
U.S. English
Welcome
Auction Tools
Member L
Secure Log In
Registered us
Email
Forgot your email address?
Password:
Forgot your password?
Want to win a WiFi phone?
Yes, I do
Log In
About | Accounts | Fees | Privacy | Security Center | Contact Us | Legal Agreements | Developers | Jobs |
Mobile | Plus Card | Referrals | Shops | Mass Pay



NOTICE

ALL WIRES AND APPARATUS
IN THIS VICINITY

DANGEROUS

KEEP AWAY

Vim

Hands-on

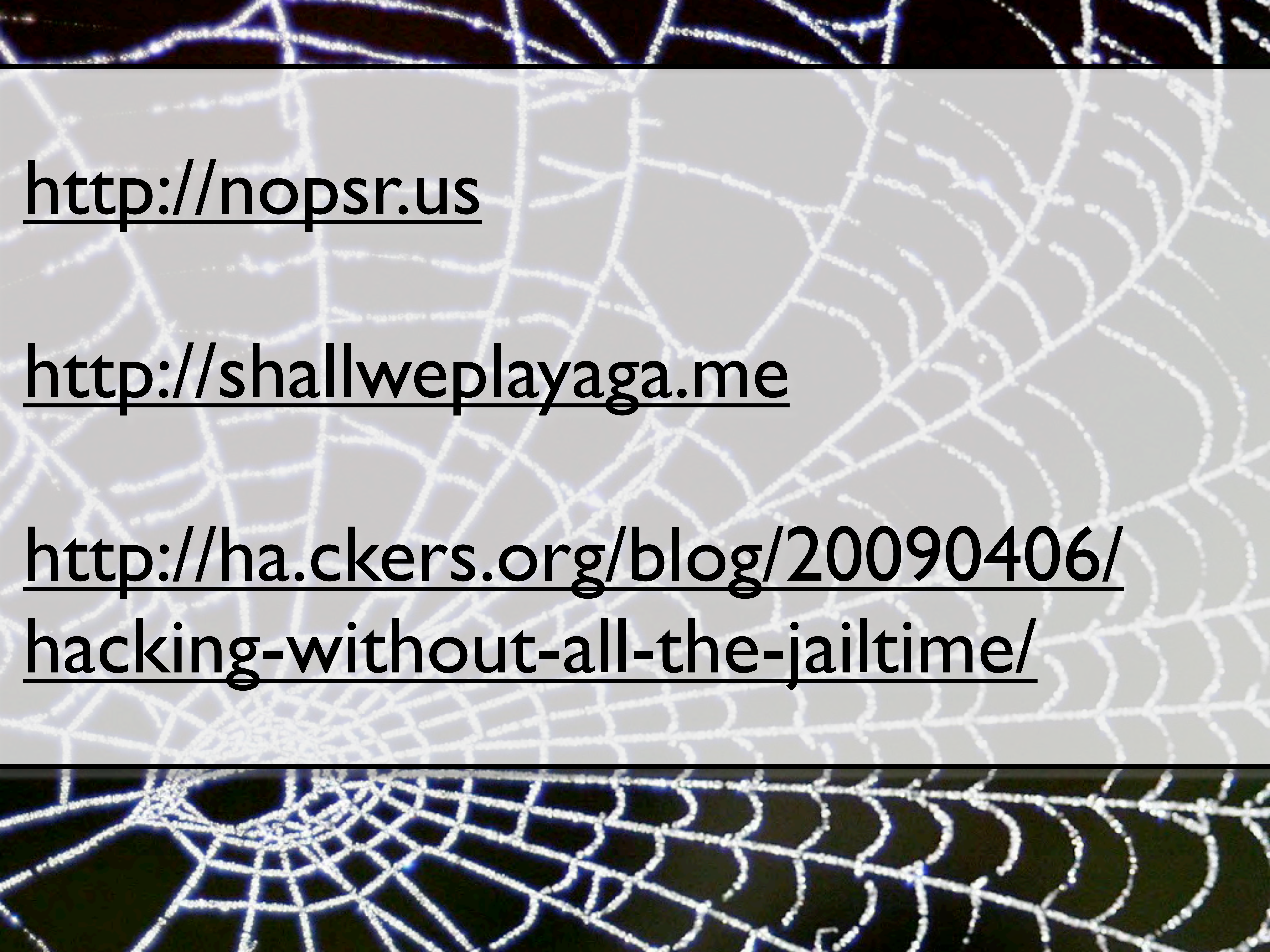
AUTO REPAIR MANUAL
1977
40th Edition
automotive diagnosis and tune-up
THE PSYCHOLOGY OF DRIVING
Feedback and Control Systems
DIGITAL PROCESS FOR SAMPLED DATA SYSTEMS
MICROMECHATRONICS
FEEDBACK CONTROL
Auto Service and Repair
COMPLETE OFFICIAL SPITFIRE 1500
CAPRI COMPLETE SERVICE MANUAL
HAYNES
BICYCLE MECHANICS
Bikes and Bicycling
SPACE TRAVEL
MC 68HC11 An Introduction Software and Hardware Interfacing
I, CYBORG
SPACE
SPACE AGE
SPACE ALMANAC
Soviet Rocketry
ROBOT

references

tools and techniques

scriptalicious

reversing



http://nopsr.us

http://shallweplayaga.me

http://ha.ckers.org/blog/20090406/hacking-without-all-the-jailtime/

The Fine Print

(Some Rights Reserved)

Creative Commons Attribution-Share Alike 3.0 United States License

http://creativecommons.org/licenses/by-sa/3.0/us/

All photos of companies or products trademarked/copyright their respective companies. Others found on flickr under (CC) licenses.

backdoor.txt	http://www.flickr.com/photos/daquellamanera/414574355/
lastplace.txt	photo used with permission from Dave Bullock, eecue.com
library.txt	http://www.flickr.com/photos/jasonvance/1194678729/
many-flags.txt	http://www.flickr.com/photos/nyllows/3633429935/
mechanics.txt	http://www.flickr.com/photos/seattlemunicipalarchives/3576509006/
play-house-free-candy.txt	http://www.flickr.com/photos/endora57/49474343/
rolls.txt	http://www.flickr.com/photos/bcmom/66951454/
school-of-root.txt	http://www.flickr.com/photos/leduardo/2755245443/
toilet-paper.txt	http://www.flickr.com/photos/mukluk/249464276/
toy-soldiers-team.txt	http://www.flickr.com/photos/janramroth/1302905330/
two-toy-soldiers.txt	http://www.flickr.com/photos/janramroth/2264184078/
web.txt	http://www.flickr.com/photos/foxypar4/2124673642/
wrench.txt	http://www.flickr.com/photos/kylemay/2078979917/