Try Harder 2 Be Yourself

Individuality is Key

Phenoelit

Why Do We Hack?

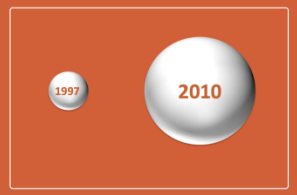
Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- It used to be all about curiosity
  - Access to rare stuff
  - “How the fuck did he do that?”
  - “I wonder if I could ...?”
  - Also: getting vendors to move
- Today’s reasons are different
  - Publicity + career points
  - Bug bounty programs
  - Exploit sales
  - Hacktivism
  - Speaking at conferences

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

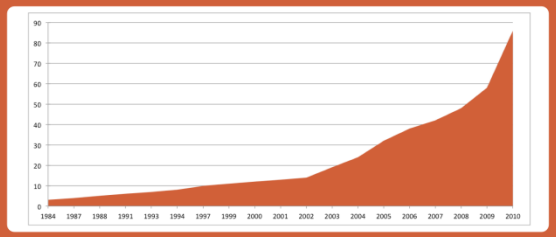
~~Setec Astronomy~~
Setec Confer Moan (yo!)

thinkst applied research

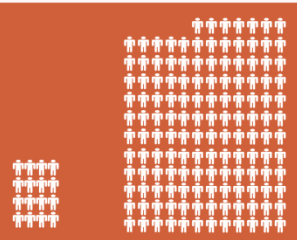


Number of Industry Related InfoSec conferences in 1997
vs.
Number of Industry Related Infosec conferences in 2010

Number of Conferences per year
(1984-2010)



The Established Conferences keep getting bigger...



Speakers (BlackHat 1997)

Speakers (BlackHat 2010)

At Least one InfoSec Conference is going on in any given month (with 19 in October alone!)

That means an infosec conference is taking place for 205/365 days of the year

http://blog.thinkst.com


March 14-16, 2012
ay, March 14
0:00
te:
fie
nt
tography

Why Do We Go To Conferences?

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Commonly cited reasons:
  - "To meet other like-minded people"
  - "Meet old friends"
  - "Meet new people"
- Actual reasons:
  - "I like alcohol and Oday!"
  - "I'm getting paid to talk to those people that like alcohol and zero day."
- Essentially, we ask to be influenced
  - That's a good thing!
    - Self-reflection
    - Respect
    - Learning

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

What Speaking Means (to me)

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- Not speaking:
  Do strange research you love
  vs.
- Speaking:
  Do strange research you love
  and present it to people smarter than yourself
  - The people in the audience are offering you an hour of their life time to review your shit!
  - This might be embarrassing
    - Halvar to me: “You fucked up every Turing reference you did. So give me a cigarette.”

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

How Hacking Is Done

Know Your History

Hacking in the 1960

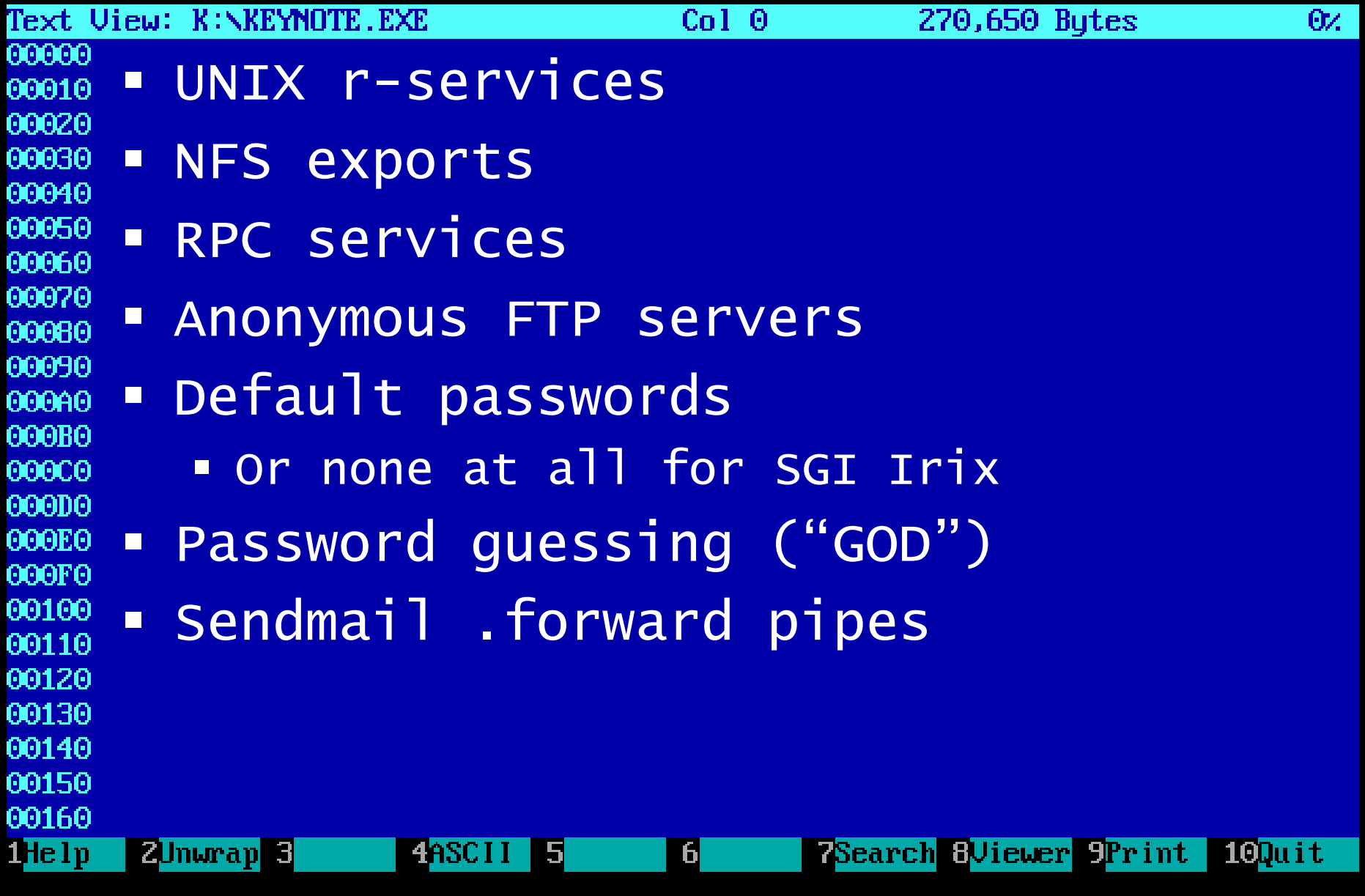
Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- Username: system
  Password: manager

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Hacking in the 1980s



Hacking in the 1990s

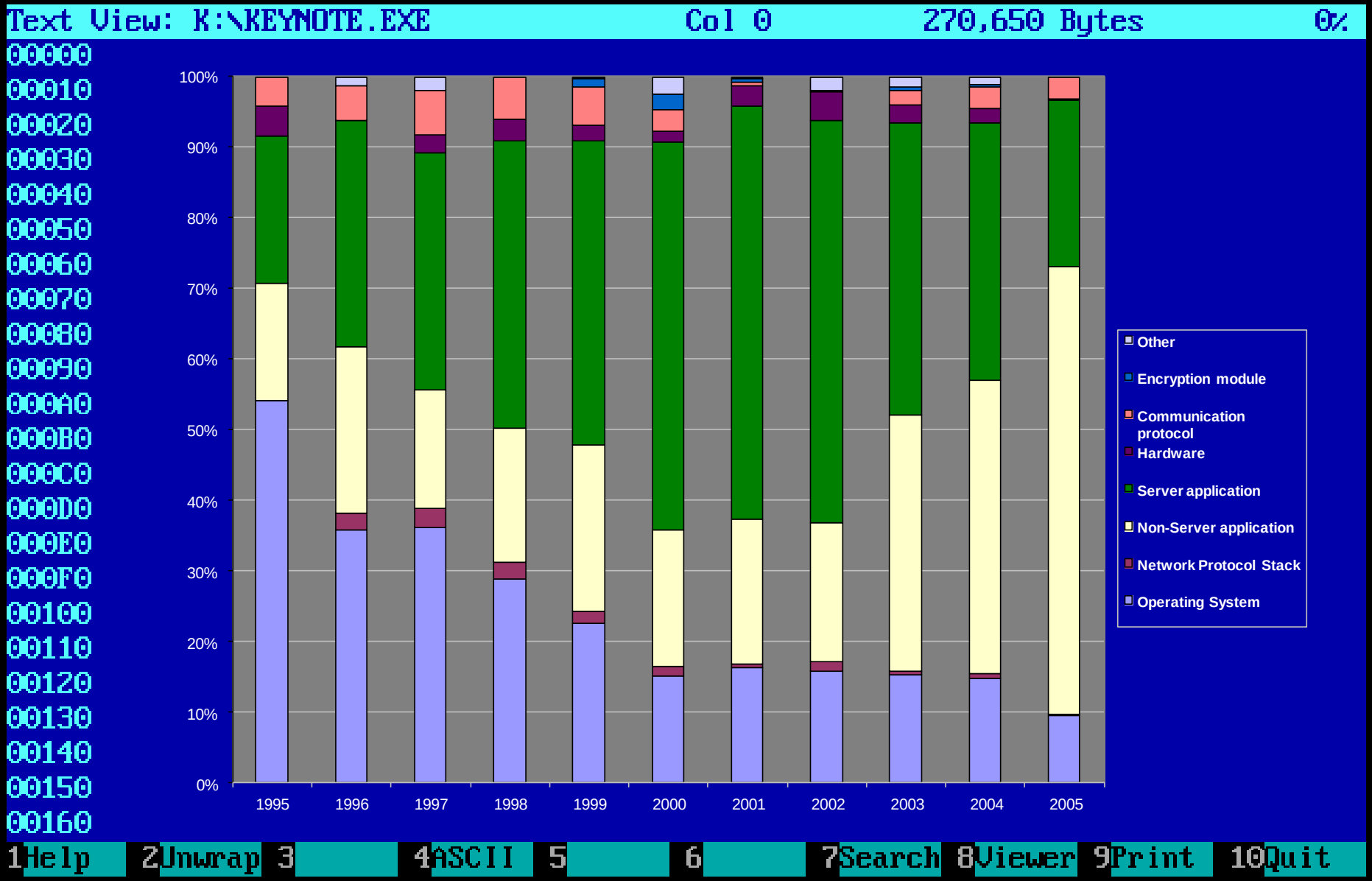
Hacking in the 2000s

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- cd ~/some/open/source && grep -E -e ‘printf\s*\([^”]+[,\)]’ *.c
- 7350 x2
- Solaris sadmind
- Cisco UDP echo
- Worms!!1!
- Heap Spraying
- Fuzzing
- Rise of the client-side attacks
- Rise of the web application bugs

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Hacking in the 2000s



Also...


Text View: K:\KEYNOTE.EXE
Col 0
270,650 Bytes
0%
00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160
1Help
2Unwrap
3
4ASCII
5
6
7Search
8Viewer
9Print
10Quit

Hacking in the 2010s

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- W^X, DEP, ASLR, KASLR, Safe-SEH, stack cookies, fortify source
  - ROP goes mainstream
- Jailbreaks
- Kingcope's BSD telnetd Remote Root
- Java client side bugs
- for i in $(cat emails.txt);do(cat fish.txt|mail -s "Facebook Account Verification" $i);done
  - Google, Dropbox, Amazon, iCloud
- Anonymous!!1!

1Help 2Unwrap 3 4ASCII 5 6

And Now?

Where Are We Heading?

What Is Big Right Now: The Cloud

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- The Cloud™ means Virtualization technologies everywhere
  - OS virtualization
  - Network virtualization
  - Storage virtualization
  - Several metric tons of management
- The change in "ownership" is important for the researcher
  - Even if you don't "own" the software, testing, fuzzing and debugging a local copy is pretty hard to prevent
  - Testing and playing with the cloud can land you in jail pretty quickly
    - Plus, you might hand your 0day over the moment you find it
  - Few clouds allow testing (e.g. Microsoft)

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

What Is Big Right Now: The Cloud

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- The Cloud™ means that hacking goes back to a mainframe host scenario
  - There are two reasons that mainframe exploits are so rare:
    1. They were actually designed and built with a lot of security in mind
    2. They were pretty hard to get to
- IMHO, hacking PAS and SAS will tend to be much more observation centric than testing centric
  - Observation is hard to prevent
  - Few and far between testing is hard to detect
- IAS comes down to finding Xen breakouts and building the image

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

What Is Big Right Now: Mobile Devices

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Mobile devices are the natural counter-point to Cloud services
- The security models differ significantly depending on the goal of the vendor
  - Apple protects their business model
  - Google protects the user's believes
- Mobile Apps roll software security back to the 90s
  - Written by former Adobe Flash coders
  - Mass produced in numbers never seen before
  - Objective-C is a programming language that could not have been designed worse if it were intentional
- Many underestimated attack vectors

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

What Is Big Right Now: SCADA !!1!

Also...


Text View: K:\KEYNOTE.EXE
Col 0
270,650 Bytes
0%
00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160
SORRY MARIO
THE PRINCESS
IS IN ANOTHER
CASTLE
1Help
2Unwrap
3
4ASCII
5
6
7Search
8Viewer
9Print
10Quit

Military Hacking

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Military and intelligence hacking is nothing new
  - Neither the practice nor the targets
- Stuxnet, Gaus, Flame etc. only allowed the general public a glimpse
- The difference is in the resources, tactics and techniques
  - The military industrial complex now invests more in attack technologies than the cybercrime market
  - This opens a lot of possibilities for the attackers in terms of R&D
    - Case in point: Nobody pulls a new MD5 collision attack out of their ass
  - Depending on international developments, it might also be the only area of unpunished in-the-wild hacking for a while

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

What Might Get Big

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Cryptography Bugs
  - Cryptography is still considered fairy dust: Have crypto, be secure!
  - Check Greg's excellent talk "Non-obvious bugs by example"
- Parallel Execution Bugs
  - Very hard to spot in source code
  - Almost impossible to find by fuzzing
  - Almost everything today has multiple cores or CPUs or both
- Lower level processors
  - Trusted by the application CPU
  - Already started with GSM Baseband research
  - System Management Controllers, ILO, etc.
  - There is a ton of this in today's devices

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

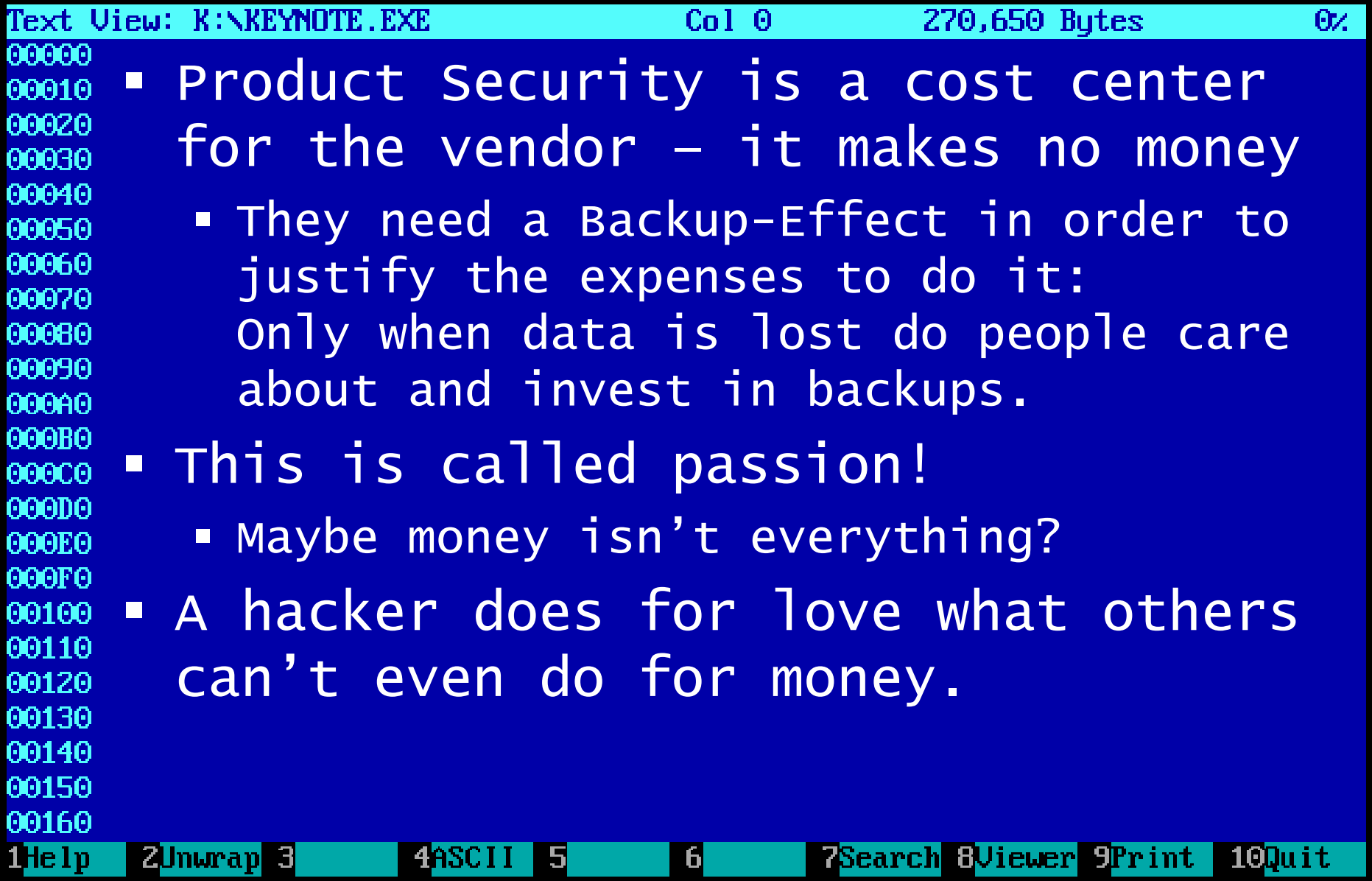
When Bug Count Isn't Everything

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- When hacking, I believe one can also do something for the common good:
  - Before Barnaby Jack publicly hacked insulin pumps, only one medical device vendor cared
  - Before Dillon Beresford took a deeper look at Siemens PLCs, no vendor cared about their base operating system
    - Now Siemens is the only one not caring
  - Nils' PinPadPwn demonstration should change quite a few payment systems
- While hackers, we are also humans
  - At some point, even you and me will have to use a PIN-Pad to pay for stuff

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

When Bug Count Isn't Everything



- Product Security is a cost center for the vendor – it makes no money
  - They need a Backup-Effect in order to justify the expenses to do it: Only when data is lost do people care about and invest in backups.
- This is called passion!
  - Maybe money isn't everything?
- A hacker does for love what others can't even do for money.

Target Selection

Where Individuality Shines

Stay Naïve

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- Naivety was always an important part of hacking
  - Remember the movie “Hackers”? The kiddy was the one hacking the Gibson.
- Whether you think that you will find a vulnerability or not, you will be right.
- Stubbornness is pretty useful
  - It also compensates for talent ;)
- Hacking is often about frustration resilience more than anything else
  - Or about not getting frustrated in the first place, a.k.a. expectation management

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Target Selection

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- It helps to find targets that genuinely interest you
  - Targets that are boring you to death are missing the inherent motivation
  - Rage can be pretty motivating
- Don’t hack things just because everyone else is hacking them
  - Unless you are hunting for bug bounties
- Understand whether your target environment is competitive by nature
  - Act accordingly

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Size Does Matter

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Bigger targets are usually juicier
  - More code =
  - More attack surface =
  - More chances for vulnerabilities
- Average of vulnerability per lines of source code is relatively stable
- Bigger targets are admin bitches
  - Harder to set up and configure right
  - Your tools will have a harder time
  - More code to wade through, because it's not relevant

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Means To An End

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

Purpose	Methods
Criminal	Browser injectors Kernel rootkits and key logger AV evasion Fishing and C&C site management
Bug bounties Vulnerability sales	Fuzzing at scale & in .fi style Automation and industrialization Static analysis
Exploit sales	Targeted fuzzing Static and runtime analysis Exploit reliability
Publicity	Fancy target selection Hardware hacking Output frequency
Fun	☺

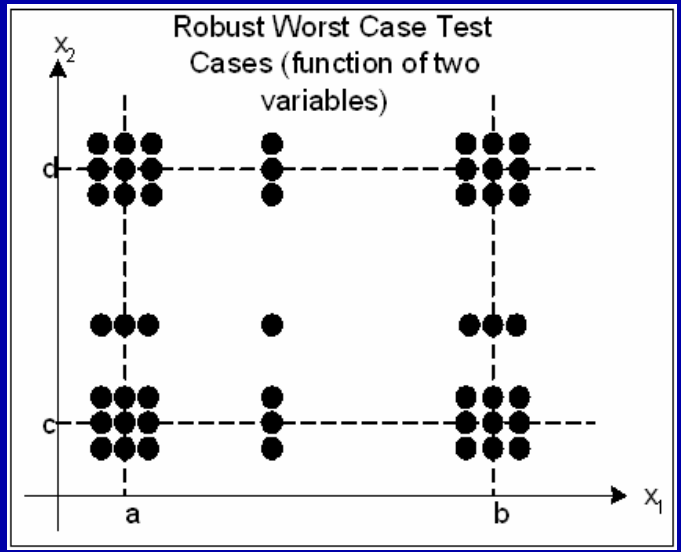
1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

A Word About Fuzzing

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- I concur that fuzzing finds a lot of bugs these days
  - Especially in complex software (e.g. Browsers)
- That doesn't prove fuzzing to be superior – it only proves the shitty state our software is in
- What you are doing is called Robust Worst Case Testing
  - It has an exponential effort grow with the number of variables being the exponent



1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Method Selection

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- There are many ways to find vulnerabilities:
  - Manual testing
  - Fuzzing
  - Static source code analysis
  - Static binary code analysis
  - Runtime analysis
  - Diffing
  - Reading Specifications
- The key is to do what suites you best
  - Not everyone reads code like Halvar
  - Not everyone breaks crypto like Greg
- Be individual!

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Bad News

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- There is no Silver Bullet in Computer Security
  - Yes, that includes offense!

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

And You?

Where Do You Stand?

Don’t Let Anyone Tell You What To Do

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- Most people that lecture you on ethics don’t follow those themselves
  - Digital human rights activists who also head companies selling to military or criminal mob
  - People bashing Microsoft while sitting at their campus getting paid by them
  - People writing spy software for oppressive governments while claiming to be left wing activists
  - Do you think Adrian Lamo is an exception?
- There are many aspects to consider
  - Other people’s opinion isn’t one of them

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

To Sell or Not To Sell?

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Is selling exploits like selling weapons?
  - Do you think it should be illegal?
  - Do you think you can control what your exploit is used for?
  - Do you care?
  - What about regulating use?
  - Is it better or worse than leaking docs to Wikileaks?
- „Do whatever you want. Trust your guts, your humanly feelings, your very limited knowledge. This is best effort.” – Julio Auto

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Vendor Communication?

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Should you talk to the vendor?
  - Do they even have a contact address?
  - Did you consider their previous track record?
  - Maybe ask someone with prior experience?
  - If in doubt, hand it off to a CERT.
- How much time should you allow for a fix?
  - RFPolicy 2.0 calls for 2 weeks warning
  - Most fix times declared by vendors are bullshit
    - Some are not
    - Use your best judgment and gut feeling
  - Can you accept being beaten by someone else releasing before you?
    - If the vendor half-releases, that's going to happen
- Don't let a vendor scare you away from disclosure with legal threats
  - I have not heard of a successful legal action that didn't have another aspect
    - If you violated NDAs, you are fucked anyway

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

To Anonymous or Not To Anonymous?

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Which Anonymous are we talking about?
  - Many independent groups
  - Probably as many goals as “members”
  - Difficult to assess
- Considerable risk
  - See The Grugq’s talk
  - Obvious and hence high priority target for law enforcement
    - Consider that LEO people have KPIs too
- A highly personal decision
  - One that should probably be kept private
  - One that can have significant consequences

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

To Cyberwar or Not To Cyberwar?

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Militaries and intelligence services around the world are dying for skilled personal
  - Their demand probably exceeds the currently available global supply
- Not everyone's favorite idea of a working place
  - "Plush Bunker"
- Depending on your country, quitting might not be an option
  - Once intelligence, always intelligence
  - Security clearances can become chain on your leg for life
- Still, a surprising number of people choose this path
  - See Military Hacking

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Why I Always Stayed Legal & Public

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- It’s easier to reason with others
  - Defends against politician's arguments
- It’s better paid
  - No need to monetize but plenty of options
  - It’s a global business, no need to sell locally
- It’s more relaxing
  - OpSec is pretty annoying over time
  - When you get older, you want it easy
- You get to talk to other people without being worried that they fuck you over

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Some Things Cannot Be Individualized

Why I loved PTS-DOS,
but don't like Kaspersky.

Know Your Basics

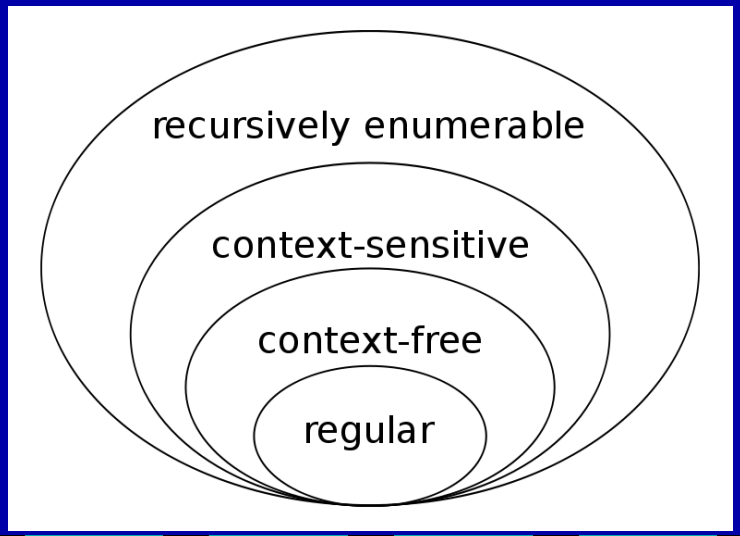
```
Text View: K:\KEYNOTE.EXE          Col 0          270,650 Bytes          0%
00000
00010 #!/usr/bin/perl --machine=fullturing
00020
00030 $n=<>;
00040
00050 while($n!=1){
00060
00070 if($n%2==0){$n=$n/2;}
00080
00090 else{$n=3*$n+1;}
000A0
000B0 printf("%u\n",$n);
000C0 }
000D0
000E0
000F0
00100
00110 ▪ Credits:
00120
00130    ▪ Alan Turing
00140
00150    ▪ Lothar Collatz
00160
1Help  2Unwrap 3      4ASCII 5      6      7Search 8Viewer 9Print 10Quit
```

Know Your Basics

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

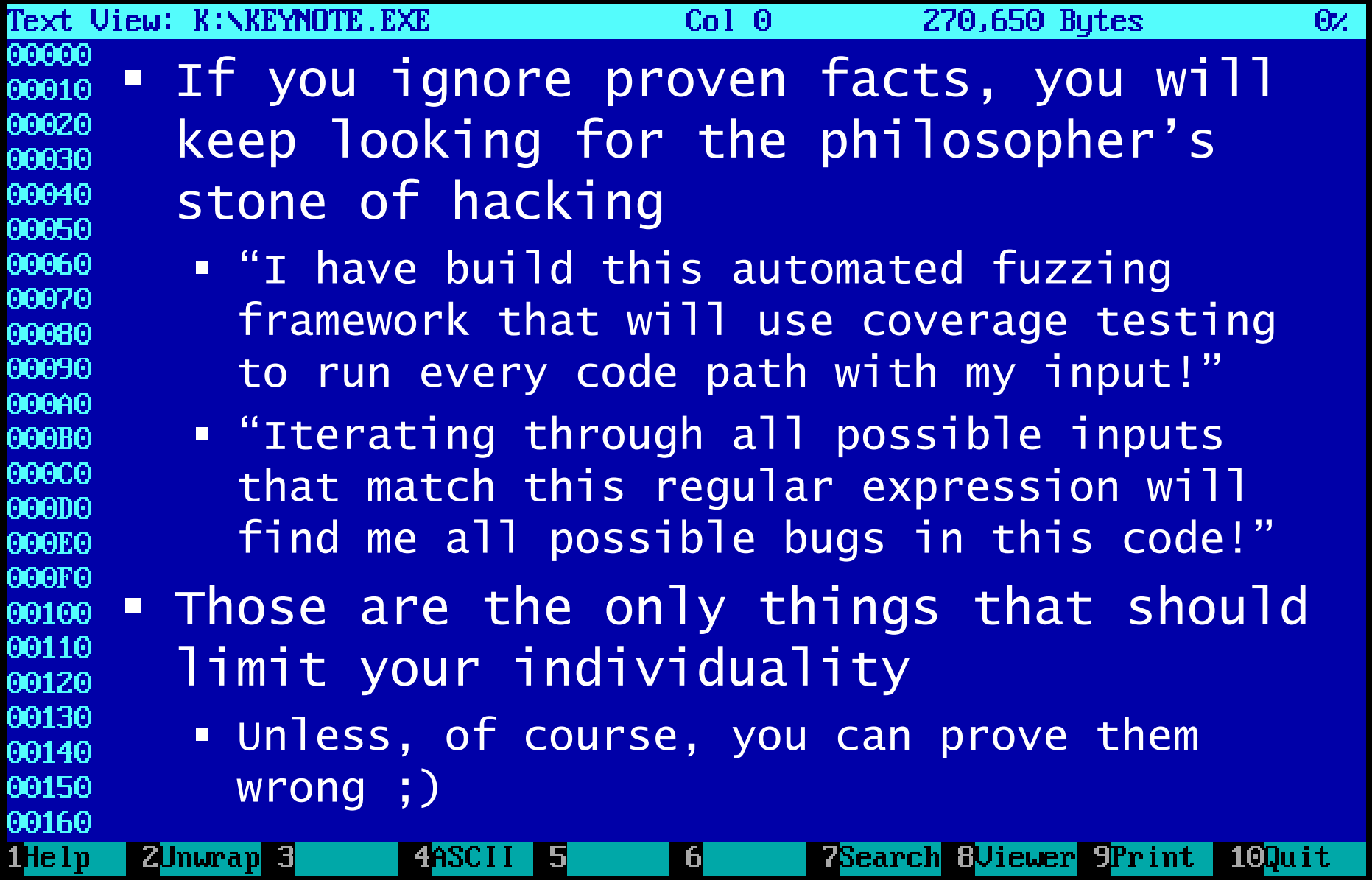
00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160

- "Never bring a regular expression to a context-free grammar fight."
  – Meredith L. Patterson
  - If you build defense, this is vital
  - If you build offense, this is more relevant than you would think



1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Know Your Basics



Be Yourself

And (optionally) get paid for it.

You And The Community

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

- Cultivate relations to others with respect for them
  - It's OK to loose the respect later if they don't deserve it
  - Respect is a symmetric connection: priority and limits work both ways
- Most people share your ideals
  - But they might have other needs, motivations or interests

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Working in InfoSec

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

Nmap: The Internet Considered Harmful - DARPA Inference Cheking Kludge Scanning

In this article, we disclose specially for Hakin9 magazine the inner working of the DARPA Inference Cheking Kludge Scanner, an extension of the world famous NMAP scanner. Even though we believe most readers of Hacking9 shall be familiar with classic Nmap use as a port scanner, using Nmap as a weaponized tool for remote backdooring is essentially not public.

Since this project is DARPA classified, we will unfortunately not be able to share the source code of this project. We will nonetheless share demos of the tool, and provide concrete evidence that pushing CPU microcode updates to the Windows 8 kernel after a kernel pool heap overflow is practical, hence achieving permanent full remote compromise of the scanned computer.

00FF0
00100
00110
00120
00130
00140
00150
00160

- You should not fall for charlatans
  - My rule of thumb: The more often the person appears in shitty TV shows, the more likely that person is a charlatan.

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

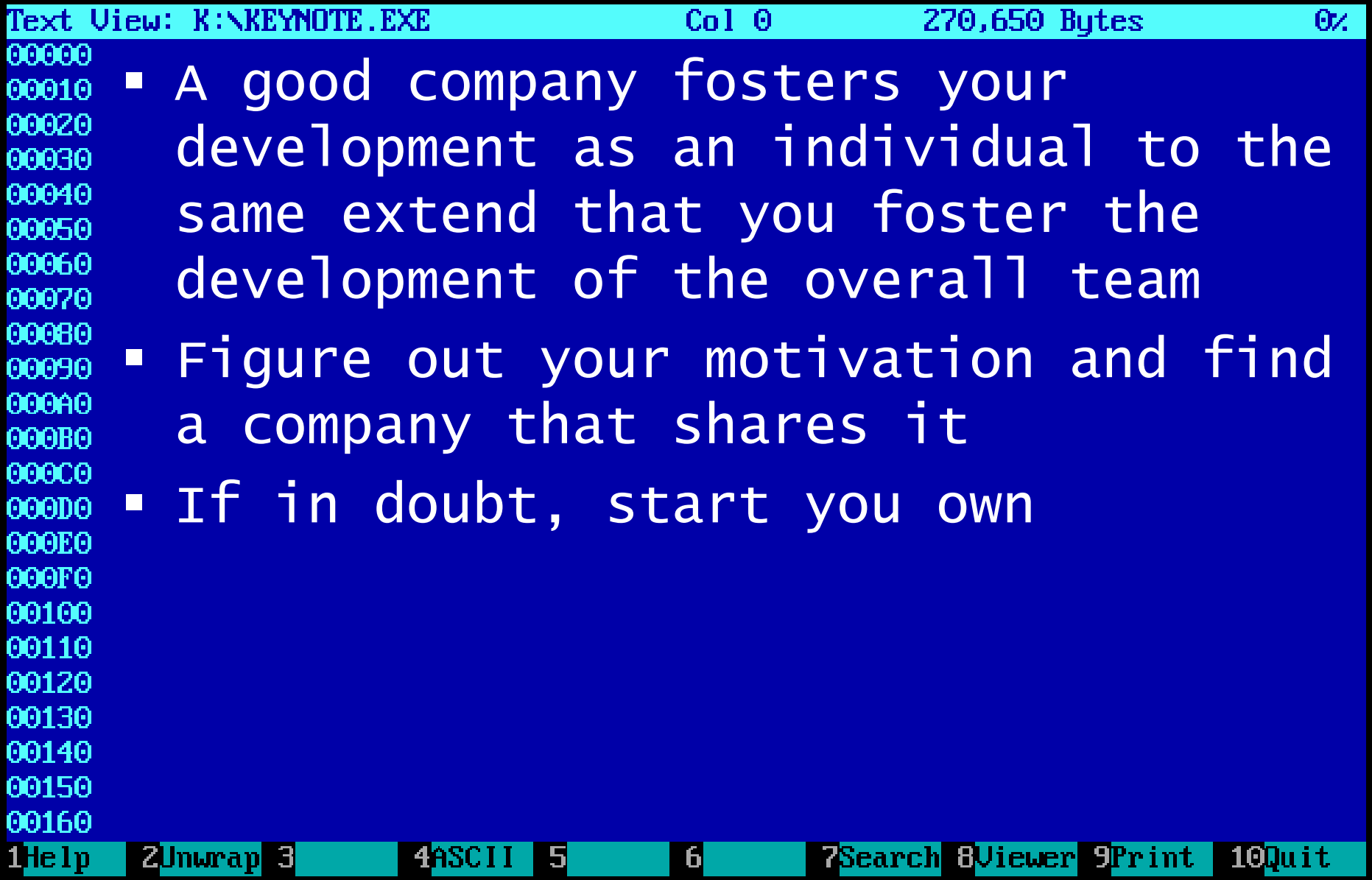
Working in InfoSec

Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%

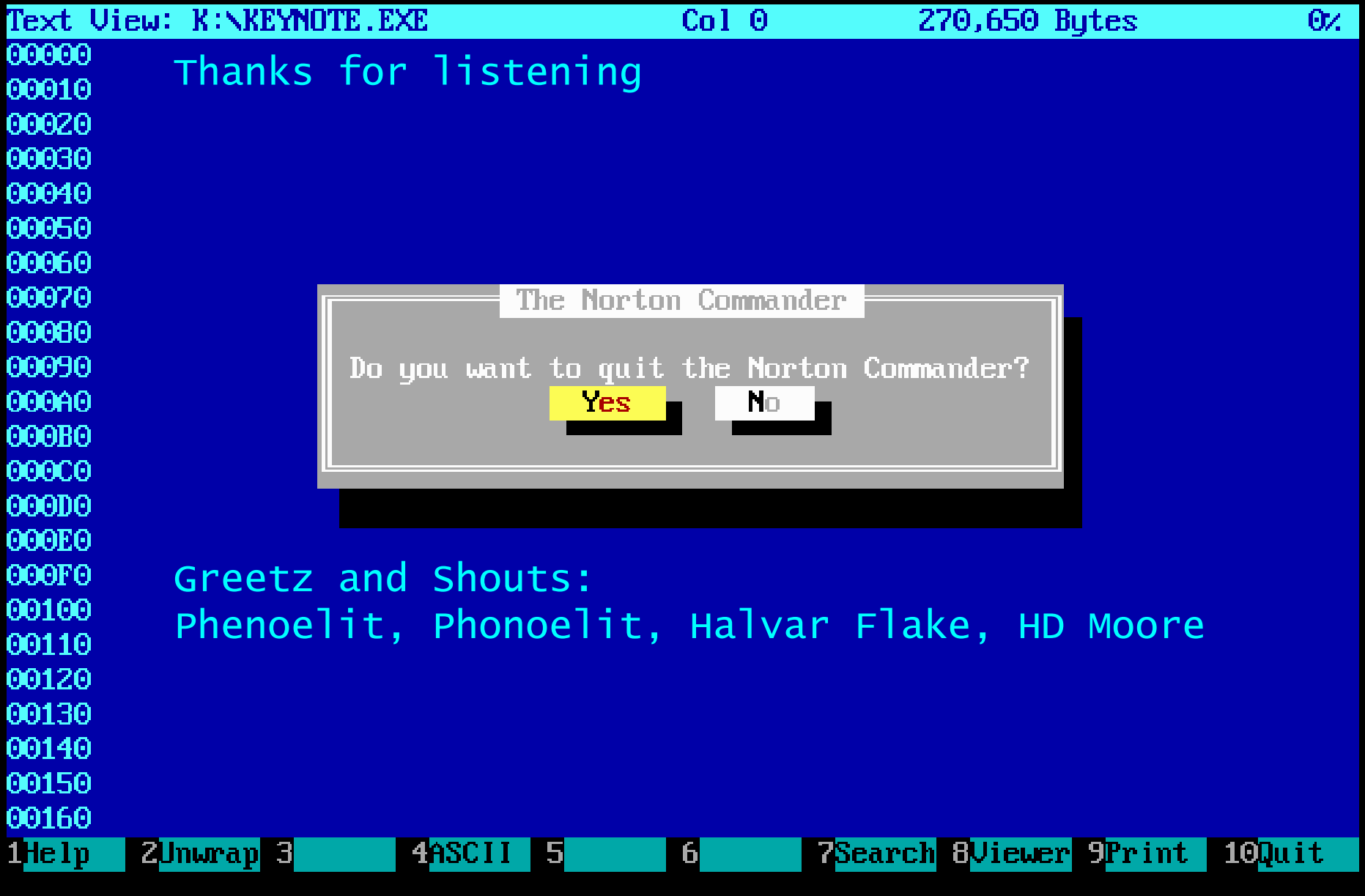
- In every work environment, you find 100 types of people:
  - 00: asshole
  - 01: asshole considered nice
  - 10: nice considered asshole
  - 11: nice
- That doesn't make InfoSec any better or worse than other jobs
- Also: If you find yourself in a hole, stop digging.
  - If a job sucks, find a new one

1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit

Working in InfoSec



Done.


Text View: K:\KEYNOTE.EXE Col 0 270,650 Bytes 0%
00000
00010
00020
00030
00040
00050
00060
00070
00080
00090
000A0
000B0
000C0
000D0
000E0
000F0
00100
00110
00120
00130
00140
00150
00160
Thanks for listening
The Norton Commander
Do you want to quit the Norton Commander?
Yes
No
Greetz and Shouts:
Phenoelit, Phonoelit, Halvar Flake, HD Moore
1Help 2Unwrap 3 4ASCII 5 6 7Search 8Viewer 9Print 10Quit