# The Beauty of Simple

Michael Boelen
NLUUG - May 16th, 2017
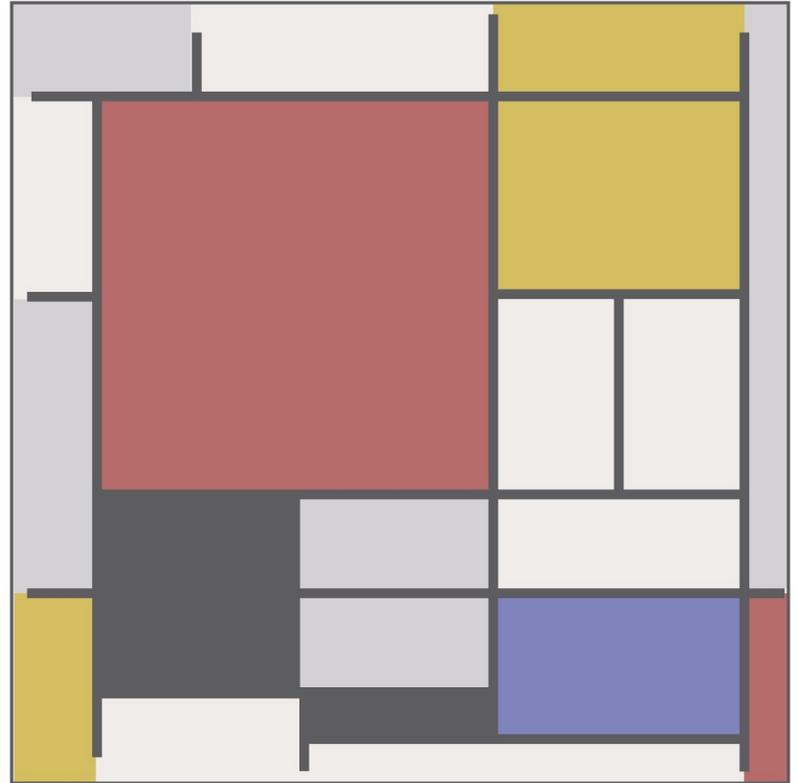
Today

- Define 'simple'
- Challenge complexity
- Simplify your life

@mboelen
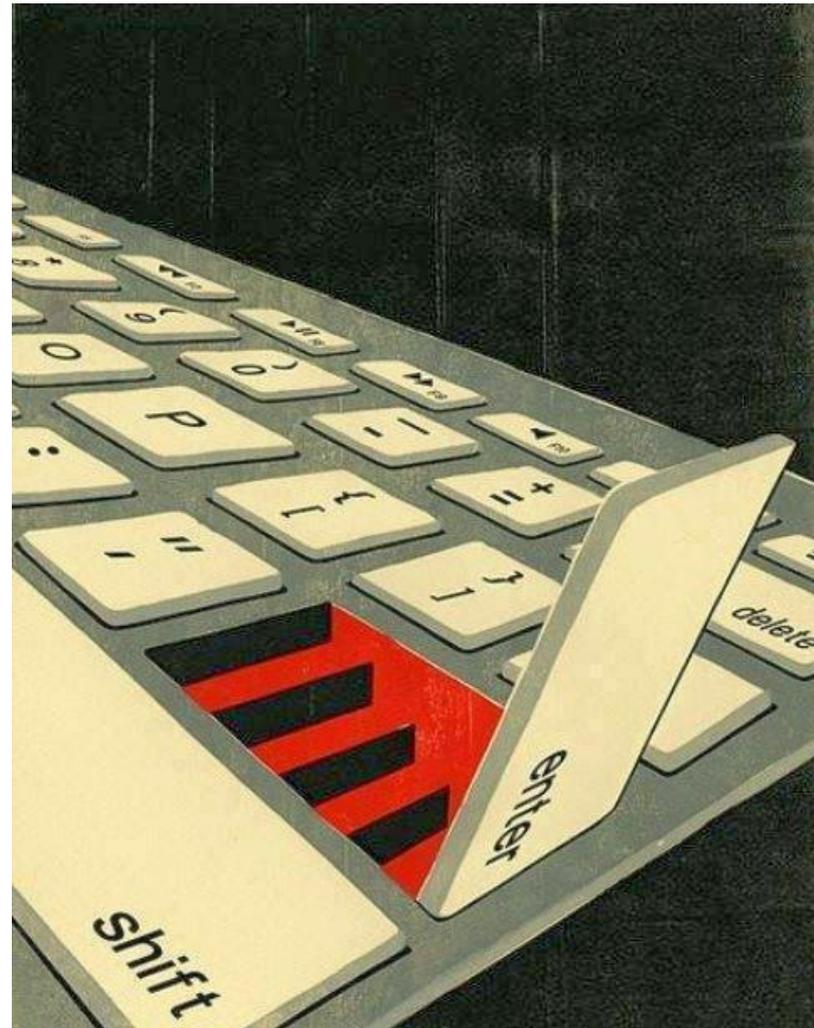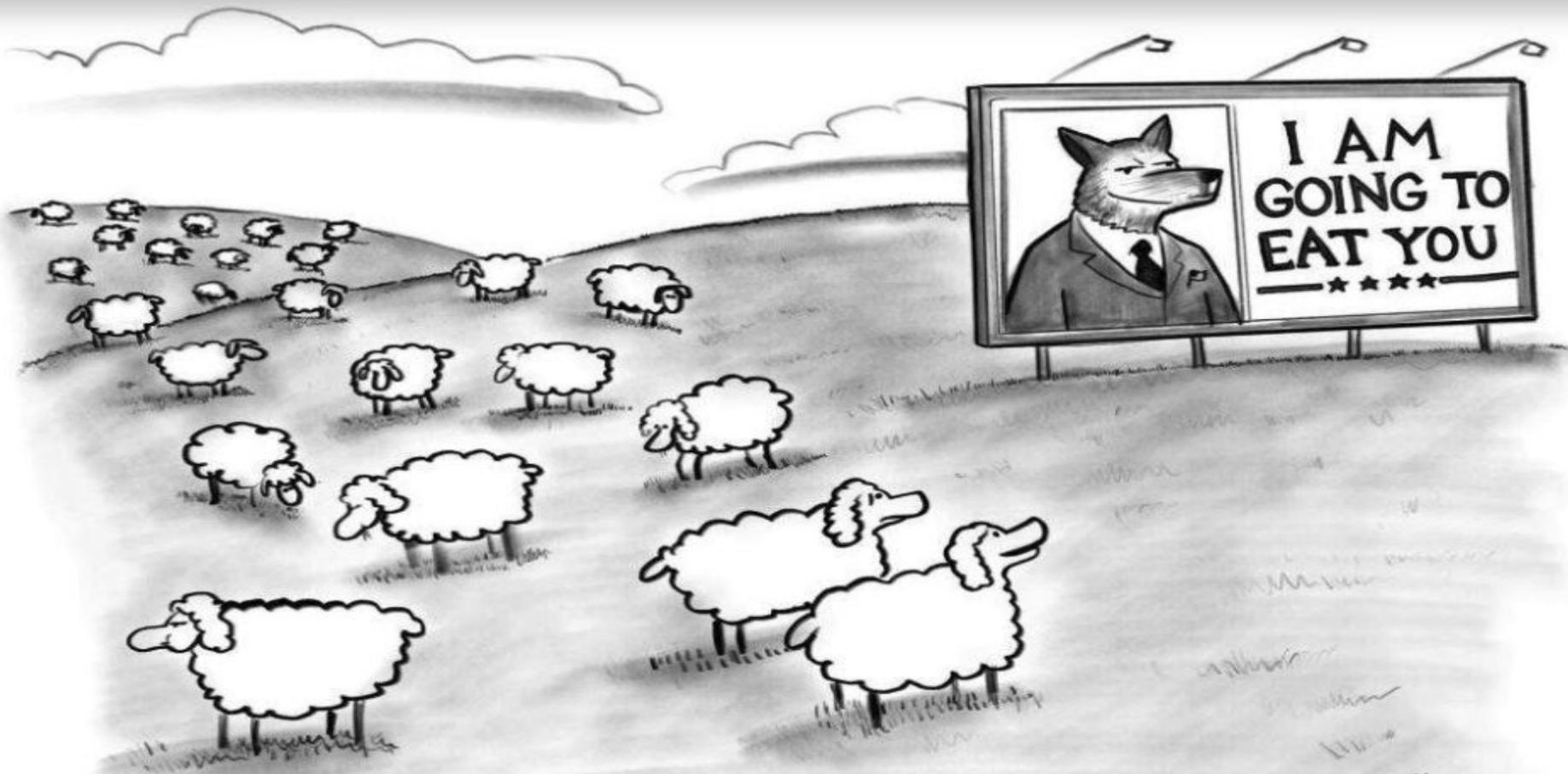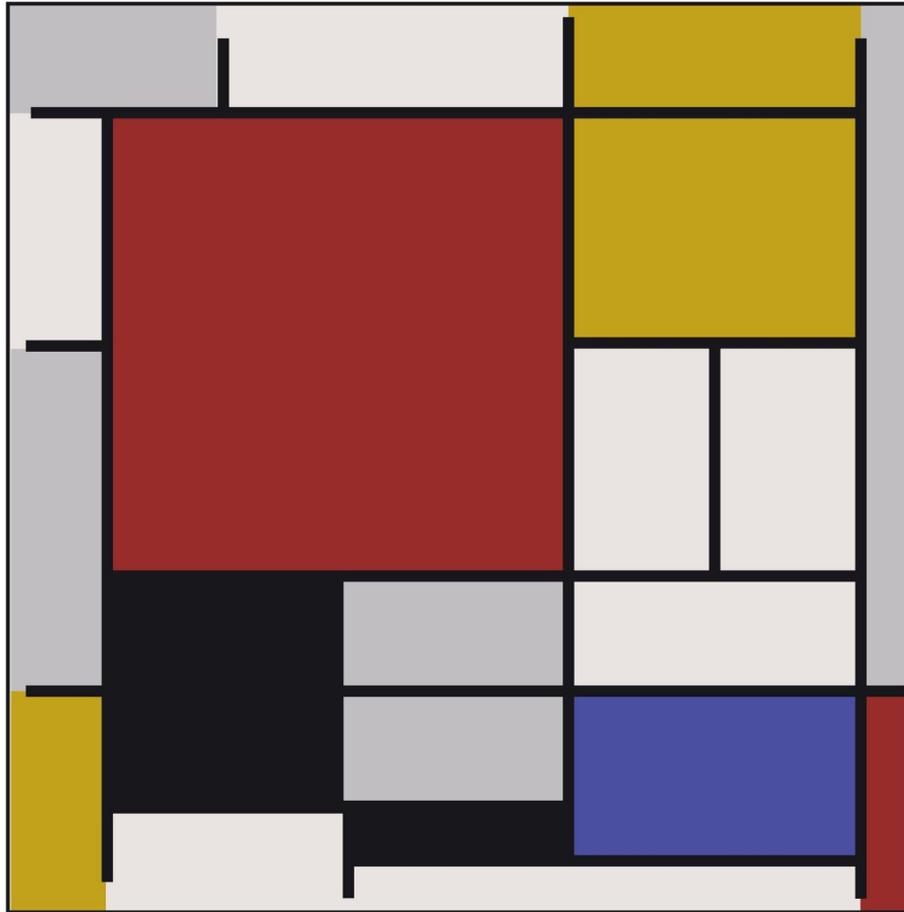
"Simple"

Simplicity
is the
ultimate
sophistication.
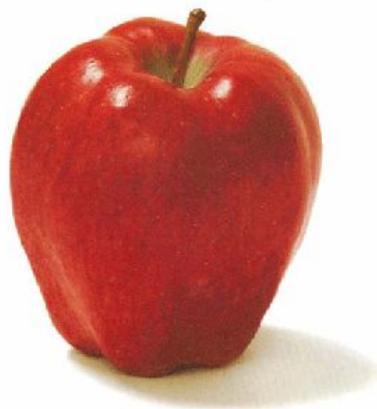
Introducing
Apple II,
the personal
computer.

Keep it simple, stupid.

Kelly Johnson, KISS principle

Simplicity is prerequisite for reliability.

Edsger W. Dijkstra, How do we tell truths that might hurt? (1975).

Simplicity is the shortest path to a solution.

Ward Cunningham, "The Simplest Thing that Could Possibly Work"

Simplicity — the art of maximizing the amount of work not done — **is essential.**

Principles behind the Agile Manifesto (2001).

Less is more.

Robert Browning, Andrea del Sarto (1855).

Complexity
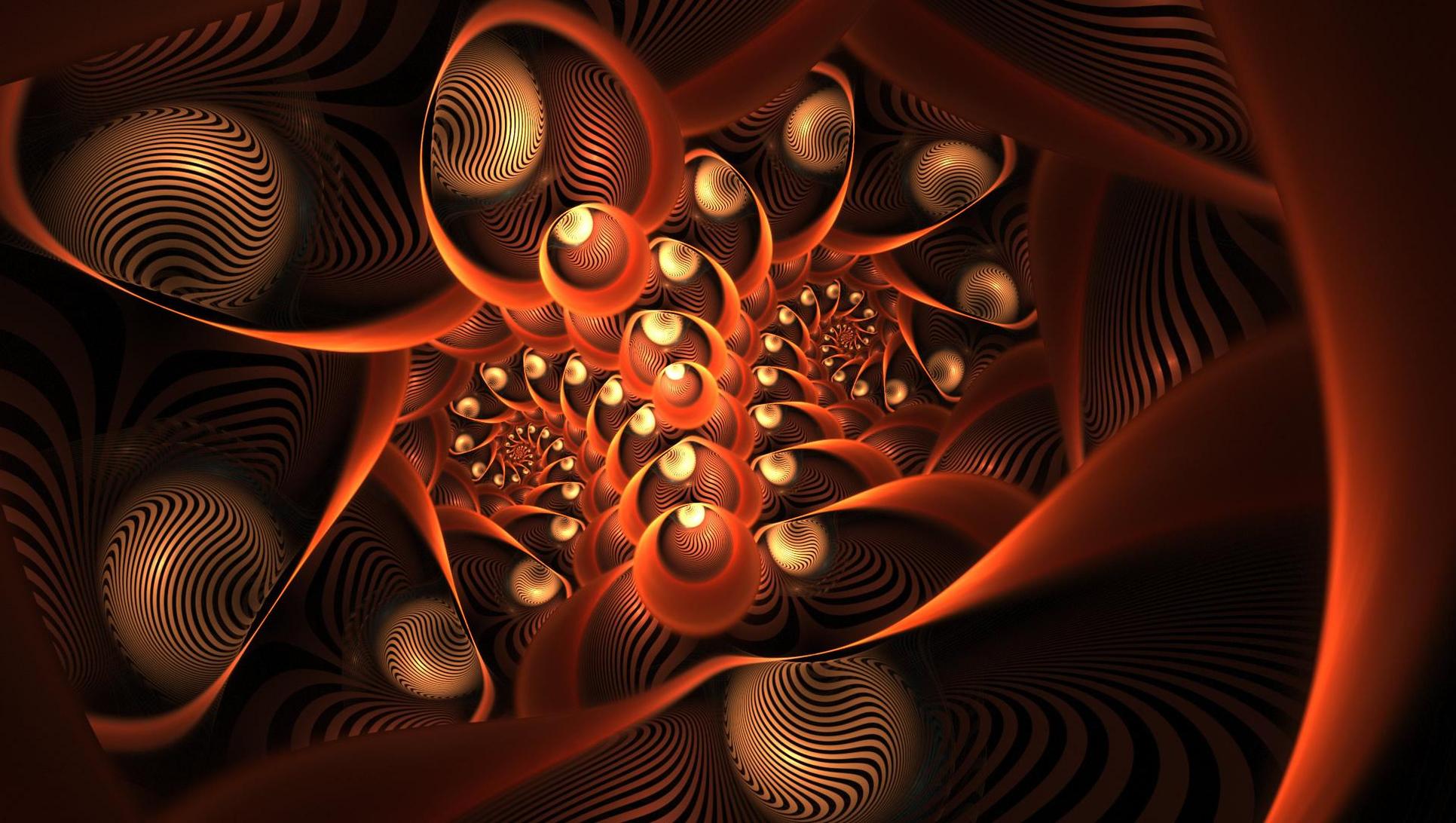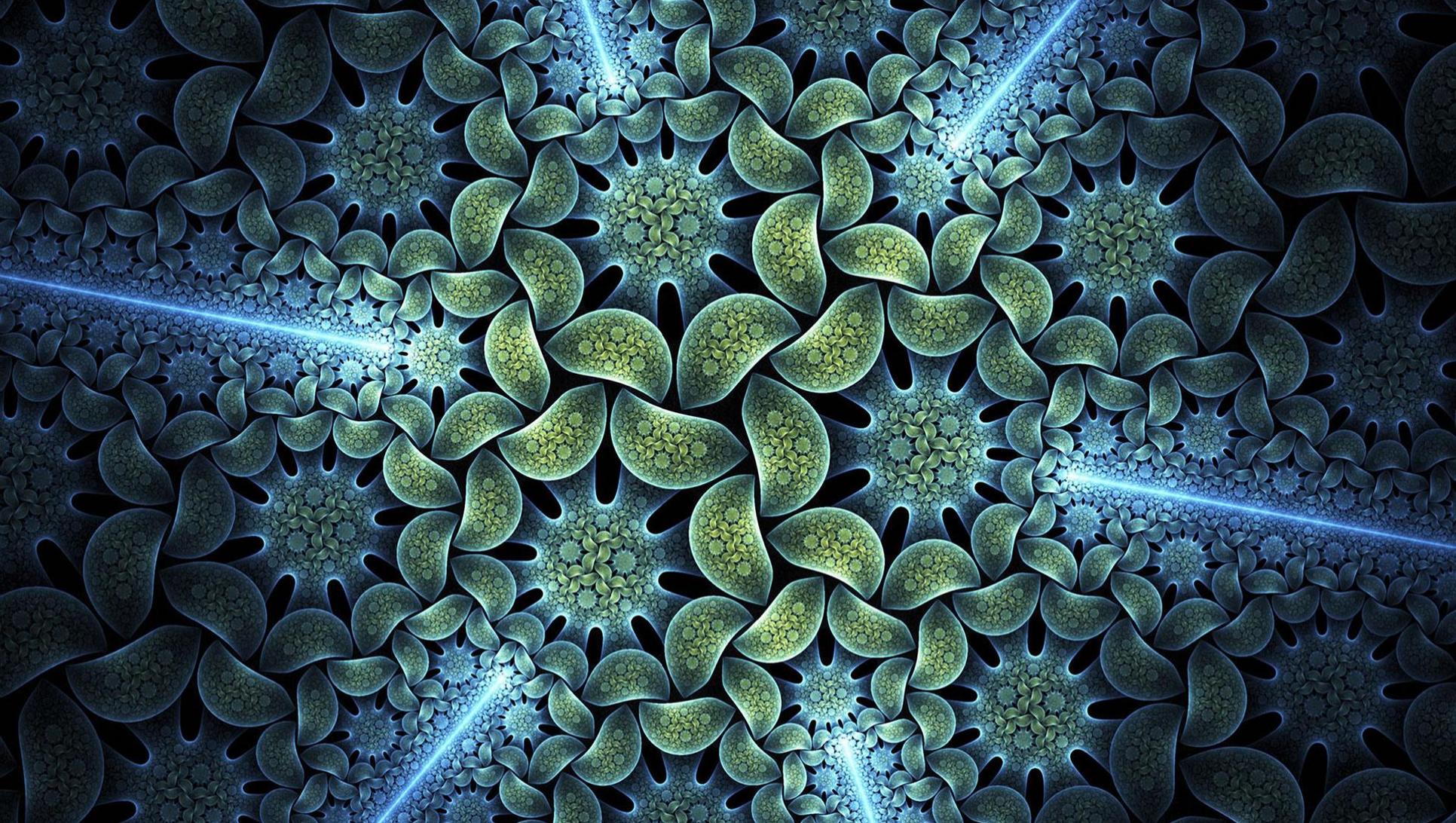
Choices

OMEN by HP

Gaming reinvented. Ominous power.

HP EliteBook 850

Sophisticated travel pro.

HP EliteBook x360 1030 G2

New and innovative security solutions

HP Spectre

Artisan materials and striking craftmanship.

HP ENVY 15

Impossibly thin. Enviably engineered.

HP Pavilion 17

Watch more, play more, store more.

HP ProBook 640

Built for performance

CISOFY
AUDITING-HARDENING-COMPLIANCE

MacBook
MacBook Air
MacBook Pro
New
iMac
Mac Pro
Mac mini
Accessories
macOS Sierra
Compare

MacBook Pro

A touch of genius.

Learn more ›   Buy ›

Choices

```
hardening-~ [0]# nmap
Nmap 7.01 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
```

Up VS ....?

```
Usage: vagrant [options] <command> [<args>]

    -v, --version                   Print the version and exit.
    -h, --help                      Print this help.

Common commands:
    box             manages boxes: installation, removal, etc.
    connect         connect to a remotely shared Vagrant environment
    destroy         stops and deletes all traces of the vagrant machine
    global-status   outputs status Vagrant environments for this user
    halt            stops the vagrant machine
    help            shows the help for a subcommand
    init            initializes a new Vagrant environment by creating a Vagrantfile
    login           log in to HashiCorp's Atlas
    package         packages a running vagrant environment into a box
    plugin          manages plugins: install, uninstall, update, etc.
    port            displays information about guest port mappings
    powershell      connects to machine via powershell remoting
    provision       provisions the vagrant machine
    push            deploys code in this environment to a configured destination
    rdp             connects to machine via RDP
    reload          restarts vagrant machine, loads new Vagrantfile configuration
    resume          resume a suspended vagrant machine
    share           share your Vagrant environment with anyone in the world
    snapshot        manages snapshots: saving, restoring, etc.
    ssh             connects to machine via SSH
    ssh-config      outputs OpenSSH valid configuration to connect to the machine
    status          outputs status of the vagrant machine
    suspend         suspends the machine
    up              starts and provisions the vagrant environment
    vbguest
    version         prints current and latest Vagrant version
```

```
Usage: rkhunter {--check | --unlock | --update | --versioncheck |
                 --propupd [{filename | directory | package name},...] |
                 --list [{tests | {lang | languages} | rootkits | perl | propfiles}] |
                 --config-check | --version | --help} [options]

Current options are:
        --append-log            Append to the logfile, do not overwrite
        --bindir <directory>... Use the specified command directories
 -c, --check                    Check the local system
 -C, --config-check             Check the configuration file(s), then exit
--cs2, --color-set2             Use the second color set for output
        --configfile <file>     Use the specified configuration file
        --cronjob               Run as a cron job
                                (implies -c, --sk and --nocolors options)
        --dbdir <directory>     Use the specified database directory
        --debug                 Debug mode
                                (Do not use unless asked to do so)
        --disable <test>[,<test>...]  Disable specific tests
                                (Default is to disable no tests)
        --display-logfile       Display the logfile at the end
        --enable  <test>[,<test>...]  Enable specific tests
                                (Default is to enable all tests)
        --hash {MD5 | SHA1 | SHA224 | SHA256 | SHA384 | SHA512 |
               NONE | <command>}  Use the specified file hash function
                                (Default is SHA1, then MD5)
  -h, --help                    Display this help menu, then exit
--lang, --language <language>   Specify the language to use
                                (Default is English)
        --list [tests | languages |  List the available test names, languages,
               rootkits | perl |    rootkit names, perl module status
               propfiles]           or file properties database, then exit
  -l, --logfile [file]          Write to a logfile
                                (Default is /var/log/rkhunter.log)
        --noappend-log          Do not append to the logfile, overwrite it
        --nocf                  Do not use the configuration file entries
                                for disabled tests (only valid with --disable)
        --nocolors              Use black and white output
        --nolog                 Do not write to a logfile
--nomow, --no-mail-on-warning   Do not send a message if warnings occur
   --ns, --nosummary            Do not show the summary of check results
--novl, --no-verbose-logging    No verbose logging
        --pkgmgr {RPM | DPKG | BSD |  Use the specified package manager to obtain or
                 SOLARIS | NONE}     verify file property values. (Default is NONE)
        --propupd [file | directory |  Update the entire file properties database,
                  package]...          or just for the specified entries
  -q, --quiet                   Quiet mode (no output at all)
 --rwo, --report-warnings-only  Show only warning messages
  --sk, --skip-keypress         Don't wait for a keypress after each test
        --summary               Show the summary of system check results
                                (This is the default)
        --syslog [facility.priority]  Log the check start and finish times to syslog
                                (Default level is authpriv.notice)
        --tmpdir <directory>    Use the specified temporary directory
        --unlock                Unlock (remove) the lock file
```

```
[ Lynis 2.4.8 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2017, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
--------------------------------


  Usage: lynis command [options]


  Command:

    audit
        audit system                   : Perform local security scan
        audit system remote <host>     : Remote security scan
        audit dockerfile <file>        : Analyze Dockerfile

    show
        show                           : Show all commands
        show version                   : Show Lynis version
        show help                      : Show help

    update
        update info                    : Show update details
        update release                 : Update Lynis release


  Options:

    --no-log                           : Don't create a log file
    --pentest                          : Non-privileged scan (useful for pentest)
    --profile <profile>                : Scan the system with the given profile file
    --quick (-Q)                       : Quick mode, don't wait for user input

    Layout options
    --no-colors                        : Don't use colors in output
    --quiet (-q)                       : No output
    --reverse-colors                   : Optimize color display for light backgrounds

    Misc options
    --debug                            : Debug logging to screen
    --view-manpage (--man)             : View man page
    --verbose                          : Show more details on screen
    --version (-V)                     : Display version number and quit
```

Confusion

jacurtis 12 hours ago

I am glad im not the only one confused by this. I went to the webpage first, couldnt really figure out what exactly it did. So i went to HN comments to see if i could figure out the purpose of this product through the comments. Turns out everyone is confused as well, lol.

akerro 11 hours ago

BUT DOES IT SCALE ON THE CLOUD

Useless Errors
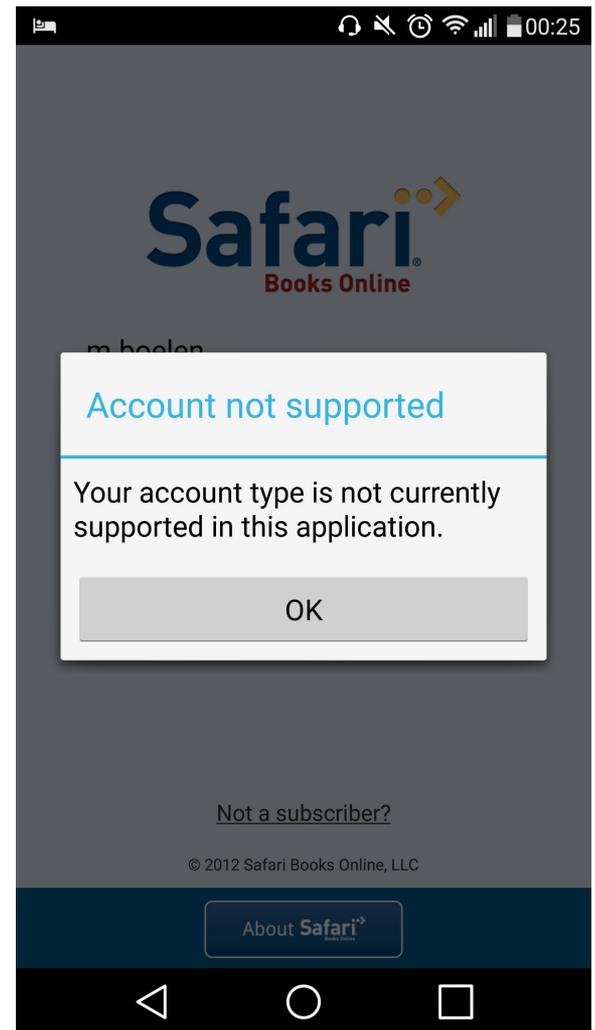
Reading
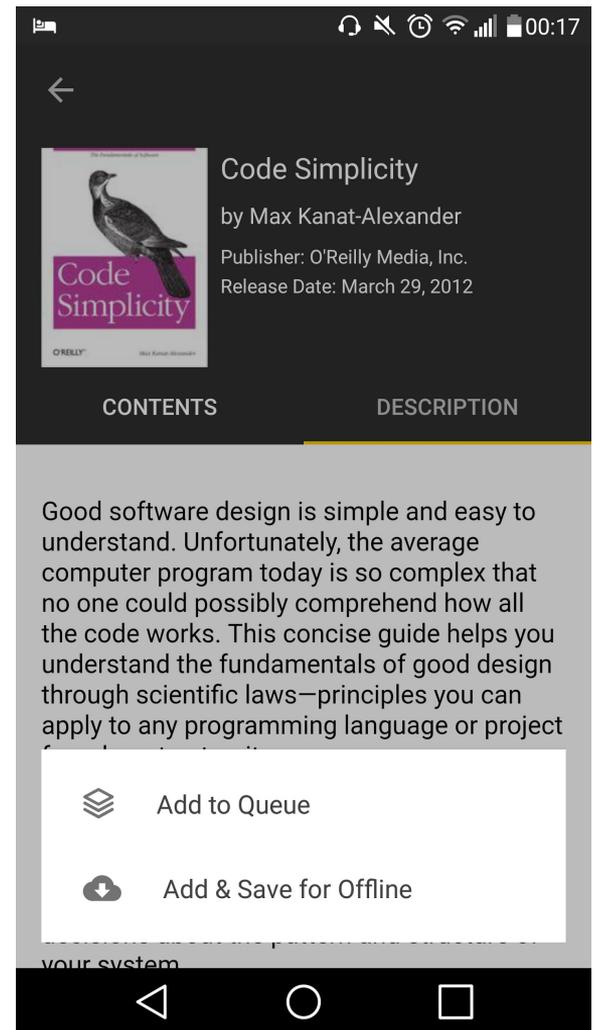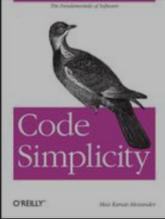
Chartjunk

https://upload.wikimedia.org/wikipedia/commons/c/c9/Chartjunk-example.svg
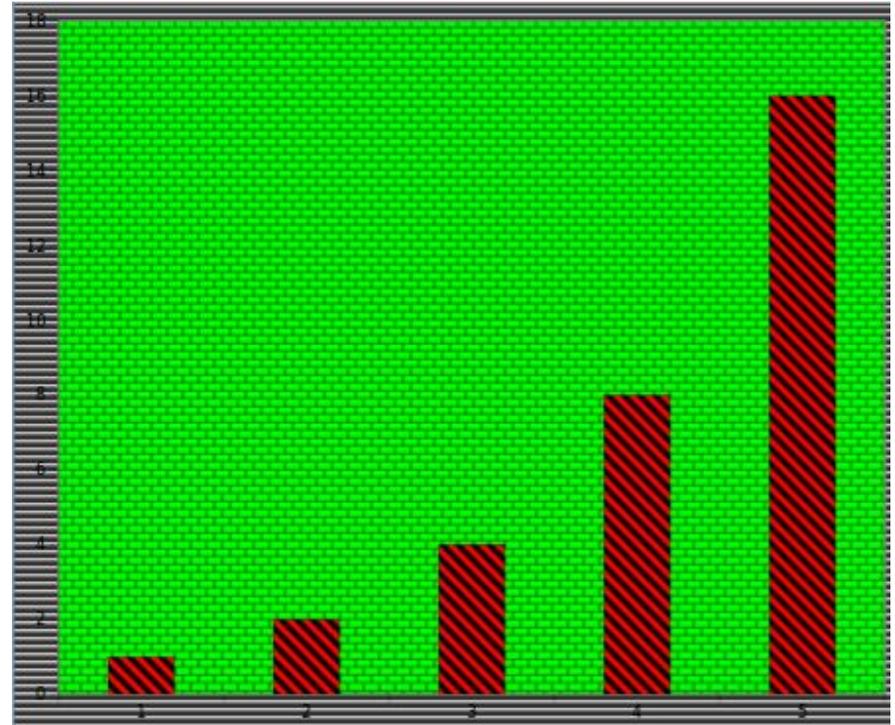
How to kill complexity?

- First impression

- Simplicity

- Next step

Example: Open Source Projects

- Good description, "Get started"

- Colors, sane defaults

- Show log file, link with more details

Simplify Life

How?

- Identify

- Reduce

- Organize

Method: 5S

- Seiri (整理)   Sort
- Seiton (整頓)   Set in order
- Seisō (清掃)   Shine
- Seiketsu (清潔)   Standardize
- Shitsuke (躾)   Sustain

☀ AccuWeather.com
‡ 2/2   🔄 ⚙

12:49   13°c   Bunnik
Mon, May 1

The wet weather continues.
Rain for the rest of the day.

Sleep   **Learning**   **Message
                                              and Music**

                             Travel   **Phone**

                             Business   **Online**

More

THE LAWS OF
SIMPLICITY

DESIGN, TECHNOLOGY, BUSINESS, LIFE

John Maeda

Thanks

(and enjoy the conference!)

Programming

- You aren't gonna need it (YAGNI)
- Don't repeat yourself (DRY)
- Minimum Viable Product (MVP)
- Feature creep, creeping featurism or featuritis
- Principle of good enough
- Wirth's law (software VS hardware)