Hello again!

Thank you, Stelios!

Bridgefest
III - 2026

”The opposite
of security is not insecurity,
it's convenience”

This is not
“*Staying off the grid 101*”, being part of “*Anonymous*”, etc.

**Some principles can also be applied for the above , but not the focus here*

Bridgefest III - 2026

“On March 23, 2026, the Hong Kong government changed the implementing rules relating to the National Security Law.

It is now a criminal offense to refuse to give the Hong Kong police the passwords or decryption assistance to access all personal electronic devices including cell phones and laptops”

Bridgefest III - 2026

iPhone

"Google Threat Intelligence Group (GTIG) has identified a new and powerful exploit kit targeting Apple iPhone models running iOS version 13.0 (released in September 2019) up to version 17.2.1 (released in December 2023).

The exploit kit, named "Coruna" by its developers, contained five full iOS exploit chains and a total of 23 exploits."

https://cloud.google.com/blog/topics/threat-intelligence/coruna-powerful-ios-exploit-kit

Google Pixel

"We recently published an exploit chain for the Google Pixel 9 that demonstrated it was possible to go from a zero-click context to root on Android in just two exploits. While we had an exploit chain for the Pixel 9, we wanted to see if it was possible to write a similar exploit chain for Pixel 10."

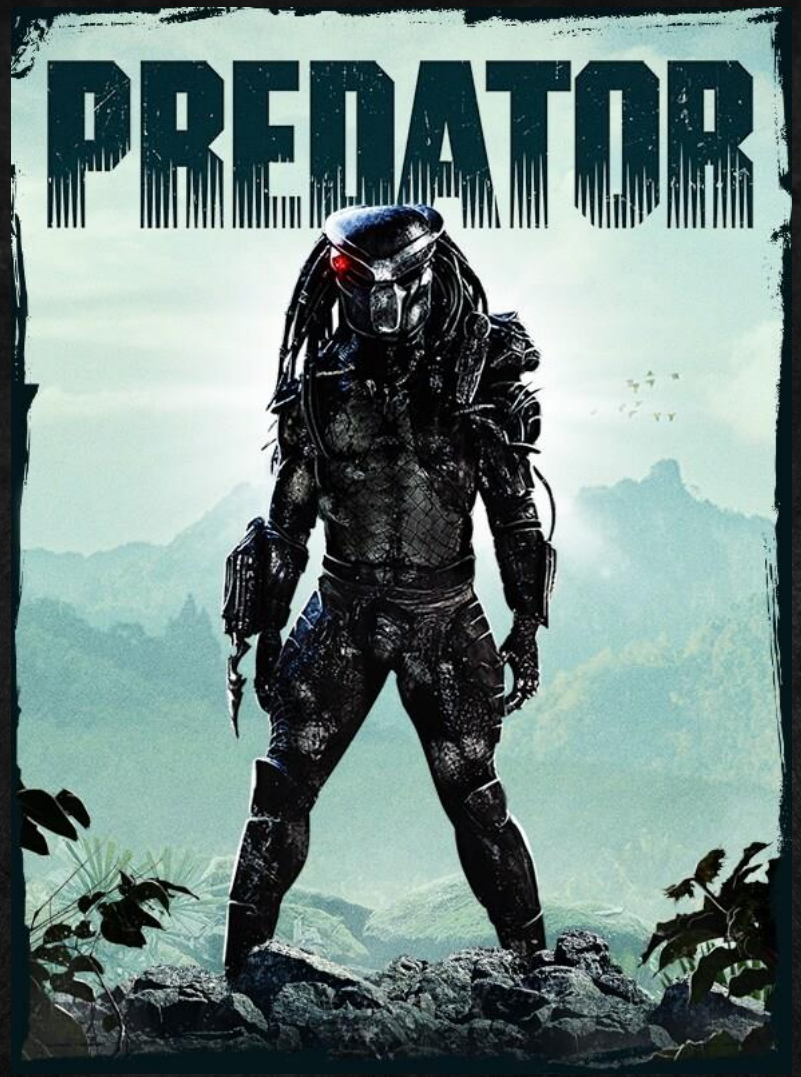
"*0-click, 0*-day RCE"
Lots of *0*!

https://www.offensivecon.org/speakers/2026/natalie-silvanovich-and-seth-jenkins.html
https://projectzero.google/2026/05/pixel-10-exploit.html

Bridgefest III - 2026

“In September 2019, Zerodium increased its bounty for Android exploits to $2,500,000, and for the first time the company paid more for Android exploits than iOS. Payouts for WhatsApp and iMessage had also been increased.

The company is now reportedly spending between $1,000,000 to $3,000,000 each month for vulnerability acquisitions”



Bridgefest III - 2026

Predator

A commercial "mercenary" spyware suite developed by Cytrox, a North Macedonian company that is part of the Intellexa Alliance — a consortium founded by former Israeli intelligence officer Tal Dilian. It is one of the most notorious spyware products in the world, often discussed alongside NSO Group's Pegasus.

Full device takeover: read messages (including E2E apps after decryption on-device), record microphone and calls, access camera, exfiltrate photos/contacts/files, harvest credentials, and track location.

Sold strictly to state customers
(intelligence and law-enforcement agencies). Documented or strongly suspected operators include:

Greece
Egypt (targeting exiled dissident Ayman Nour, journalists)
Armenia
Saudi Arabia
Madagascar
Côte d'Ivoire
Vietnam (targeting EU politicians)
Indonesia, Angola, Sudan, the Philippines, Kazakhstan (per Insikt Group / Recorded Future reporting)

Pricing leaks (notably from Intellexa proposals published by Haaretz and Citizen Lab) suggest:

Entry package: roughly €8 million for ~10 concurrent infections, one country of operation.

Full-feature contracts with multiple geographies, more concurrent targets, and 0-click capability have been quoted at €13–20+ million.

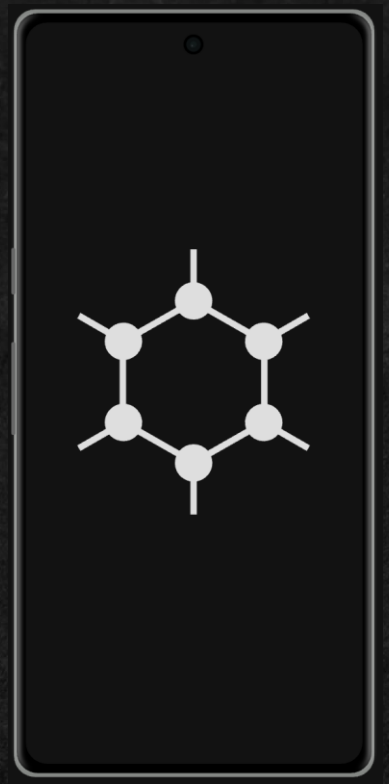
Annual maintenance / exploit refresh fees on top.

https://insidestory.gr/tagline/spyware
https://www.reportersunited.gr/11674/predator-files/

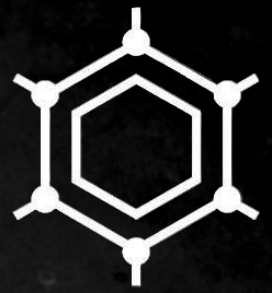
“The principle of least privilege”

and

“Compartmentalizasion”



GrapheneOS



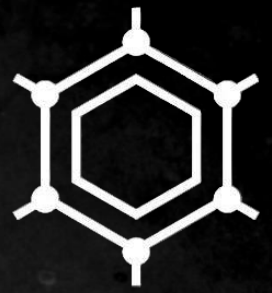
GrapheneOS

GrapheneOS is a private and secure mobile operating system with great functionality and usability.

It starts from the strong baseline of the Android Open Source Project (AOSP) and takes great care to avoid increasing attack surface or hurting the strong security model.

Works on:

Pixel 6, Pixel 6 Pro and Pixel 6a all the way up to Pixel 10, Pixel 10 Pro, Pixel 10 Fold, Pixel 10a, Pixel 10 XL



GrapheneOS

Permission model the user actually controls

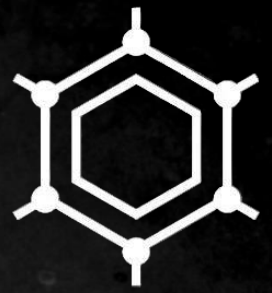
Network permission toggle per app (stock treats INTERNET as install-time).

Sensors permission toggle (gyro, accel, baro, etc., separately from camera/mic).

Storage Scopes and Contact Scopes — apps see only an explicit allowlist of files/contacts but believe they have full access, eliminating the all-or-nothing choice.

Granular toggles for clipboard, nearby-devices, etc., and the ability to strip permissions Android marks as install-time.

Physical / forensic attack resistance



GrapheneOS

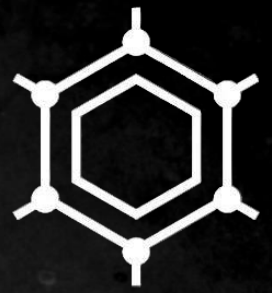
Auto-reboot after a configurable lock timeout returns the device to Before-First-Unlock state, where disk keys are not in memory — defeats most commercial forensic tools (Cellebrite, GrayKey) that rely on AFU exploitation.

USB-C peripheral control: disable USB data when locked or always, blocking juice-jacking and forensic dongles.

Duress PIN/password that wipes the device and eSIMs immediately.

PIN scrambling to defeat shoulder-surfing and smudge inference.

Disables fingerprint unlock after a short interval, requiring PIN re-auth.



GrapheneOS

Network attack surface

LTE-only mode disables 2G (and optionally 3G), defeating IMSI catchers / Stingrays that downgrade to insecure baseband protocols.

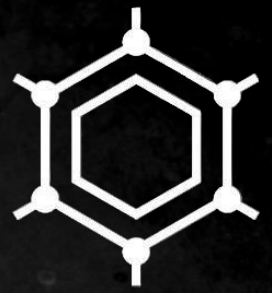
Per-connection randomized MAC (stock does per-SSID), plus randomized DHCP client identifiers.

Automatic Wi-Fi/Bluetooth disable after a configurable idle period.

User profile isolation

Heavy use of secondary users and the modern Private Space with end-session wipe of keys, plus a "user switcher from lock screen" and disable-of-running-apps for inactive profiles — useful for compartmentalizing work/play

GrapheneOS stacks multiple mitigations that directly undermine the exploit primitives exploits and exploit frameworks depend on:



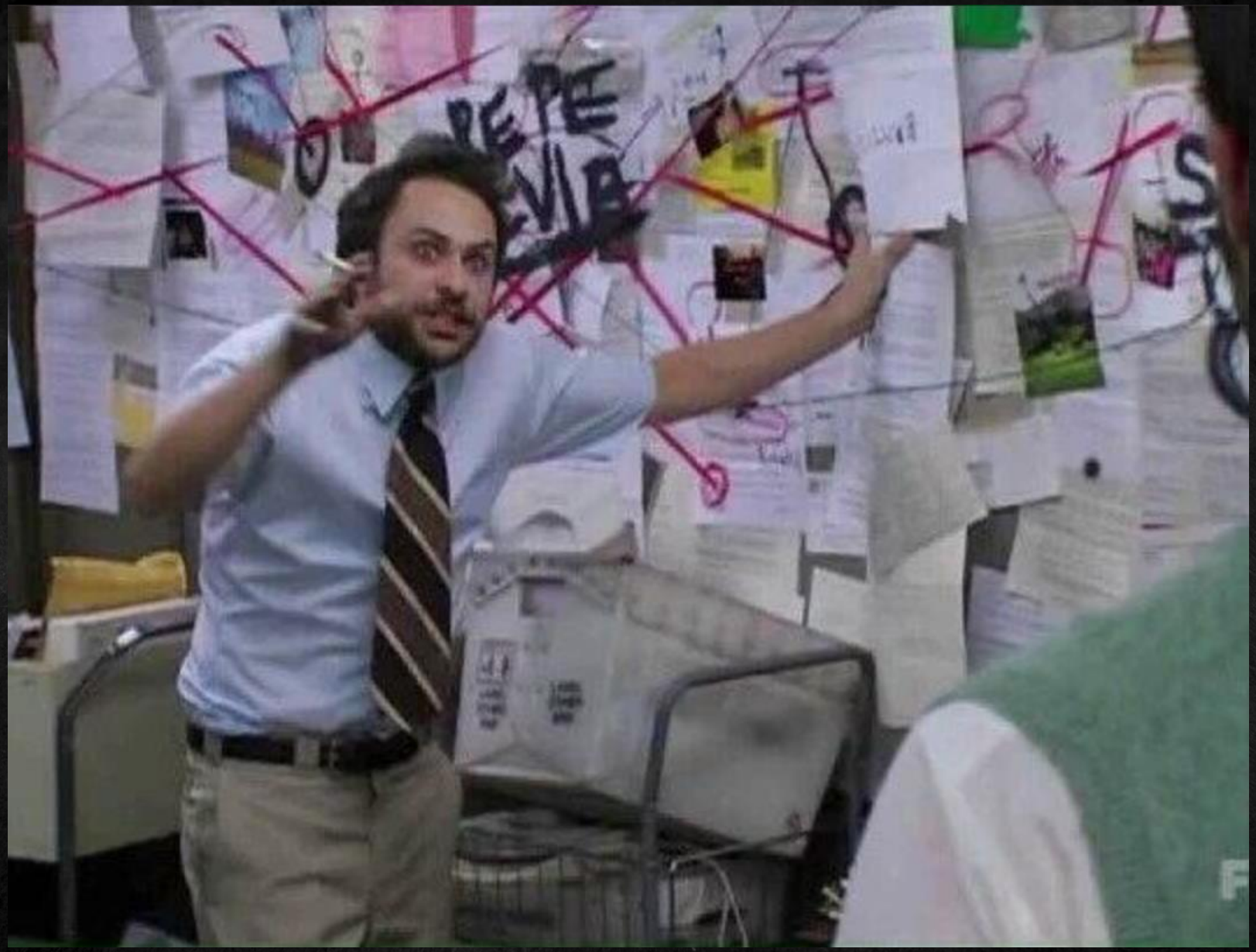
GrapheneOS

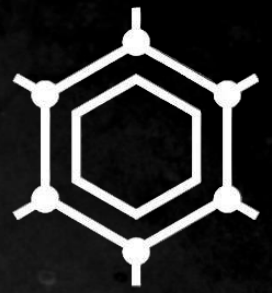
A hardened libc providing defenses against the most common vulnerability classes, along with a custom hardened malloc leveraging modern hardware capabilities to provide substantial defenses against heap memory corruption.

Hardware Memory Tagging Extension (MTE) support is extended to more system components than stock Android, with the option to apply it globally to user apps.

The default browser, Vanadium, disables the V8 JavaScript JIT compiler by default for attack surface reduction — this eliminates a massive class of browser-based exploit chains.

Unnecessary features like NFC and Bluetooth are disabled either by default or when the screen is locked, reducing exposure to remote, local, and proximity-based attack surfaces.





GrapheneOS

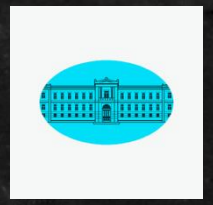
https://grapheneos.org/features

Bridgefest III - 2026






GrapheneOS

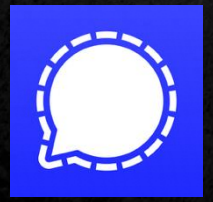














Uber

Bridgefest
III - 2026

GrapheneOS

Nokia 105 4G,
Definitely not compatible with GrapheneOS

Bridgefest III - 2026

Qubes OS

Bridgefest III - 2026

Joanna Rutkowska

“How much security do I need?”

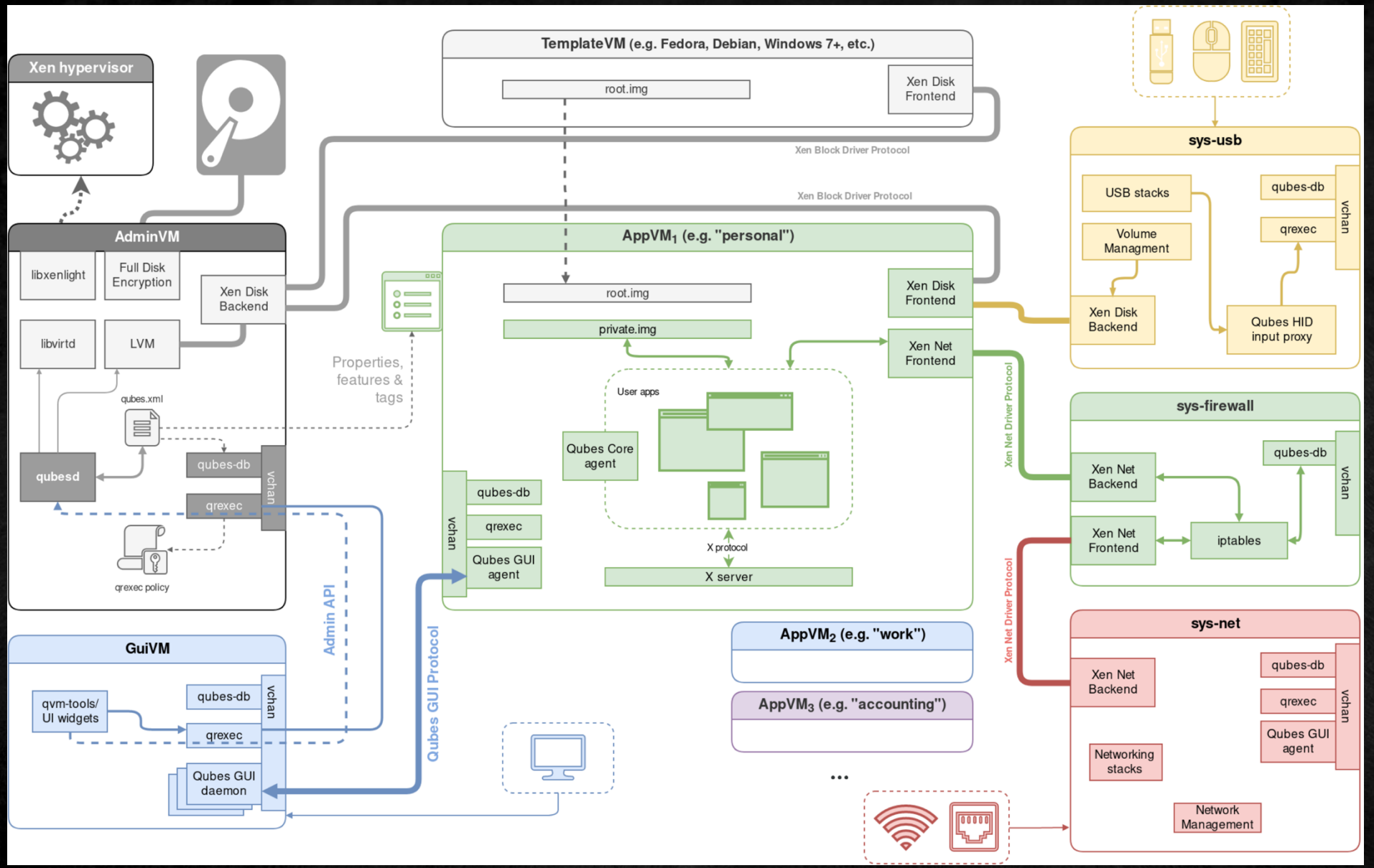
“Yes”

Bridgefest III - 2026

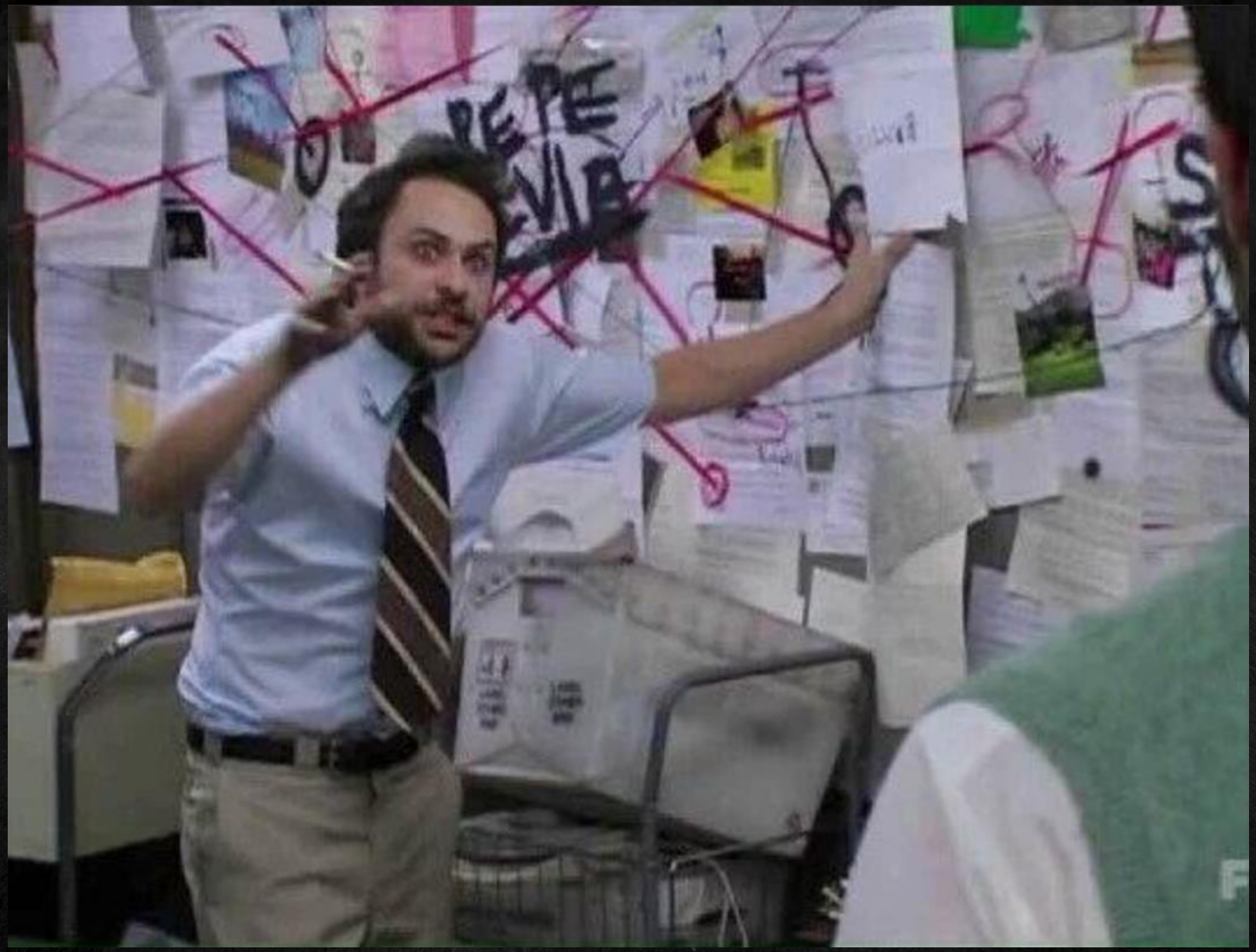
“Qubes OS’s main security improvement over both vanilla Debian and vanilla Windows 11 is that it makes strong, VM-level compartmentalization the primary security primitive, integrated into the whole UX, instead of treating isolation as an optional add-on.”

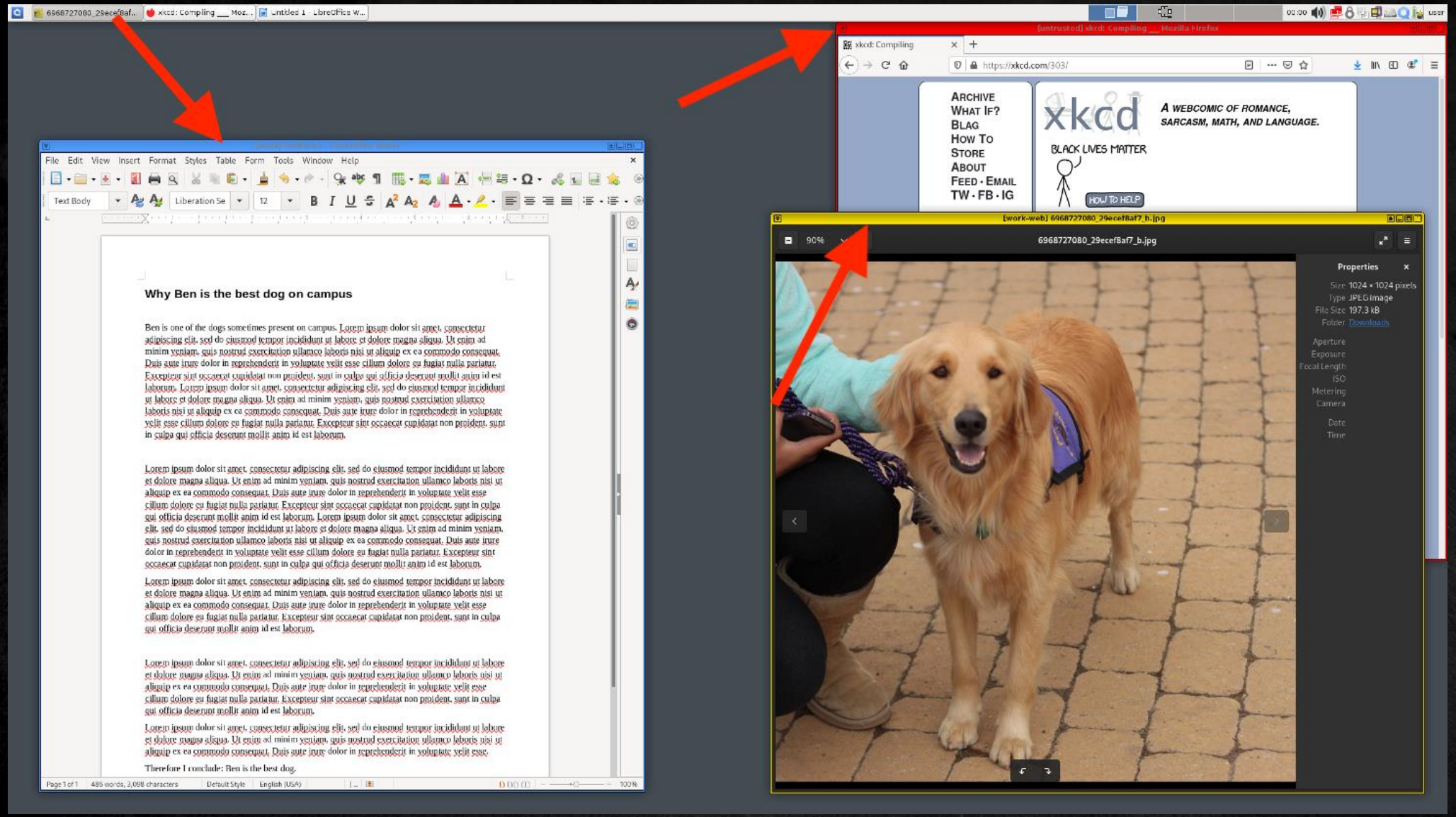
https://www.qubes-os.org/

Bridgefest III - 2026

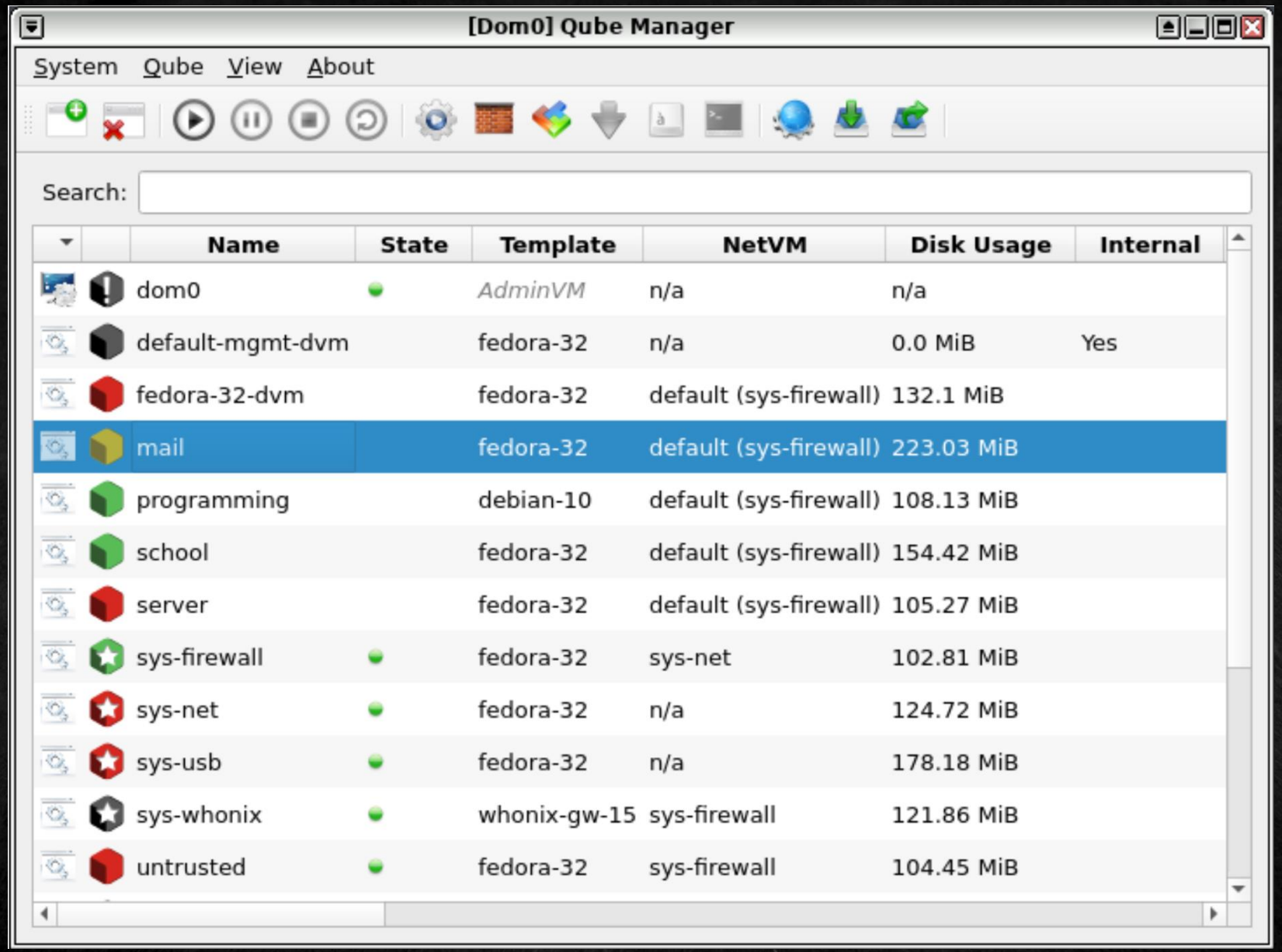


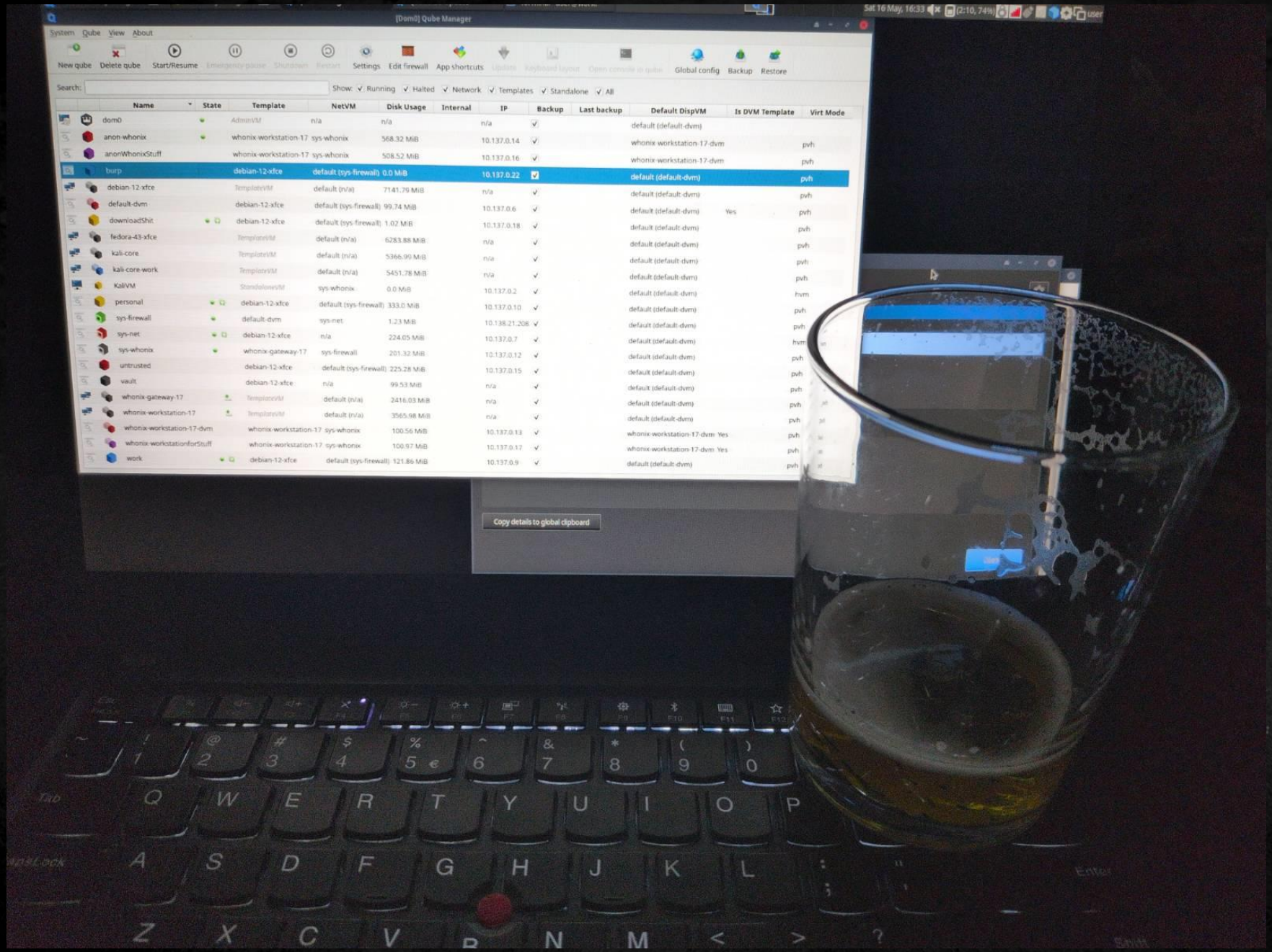
Bridgefest III - 2026



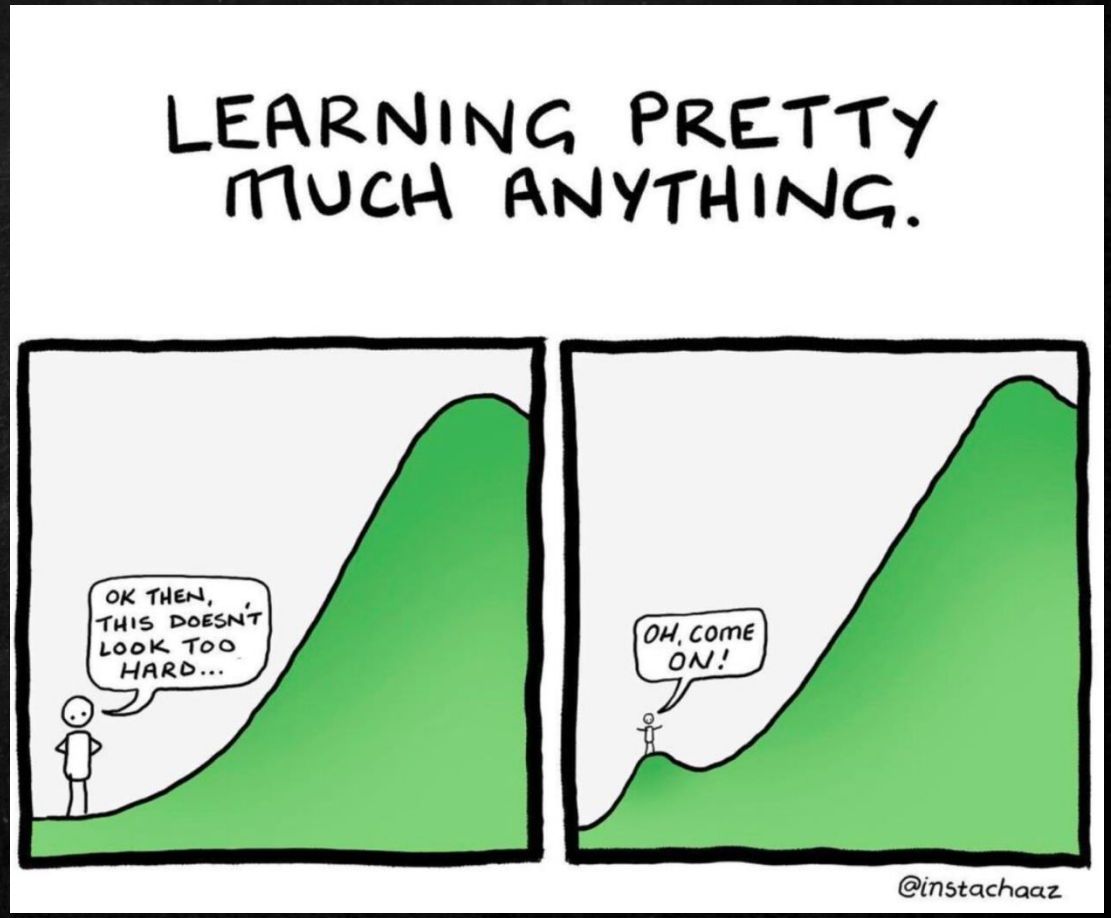


Bridgefest III - 2026





Bridgefest III - 2026



Bridgefest III - 2026

Bridgefest III - 2026

”Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.”

Ed Snowden

Bridgefest III - 2026

Bridgefest III - 2026

Thank you!