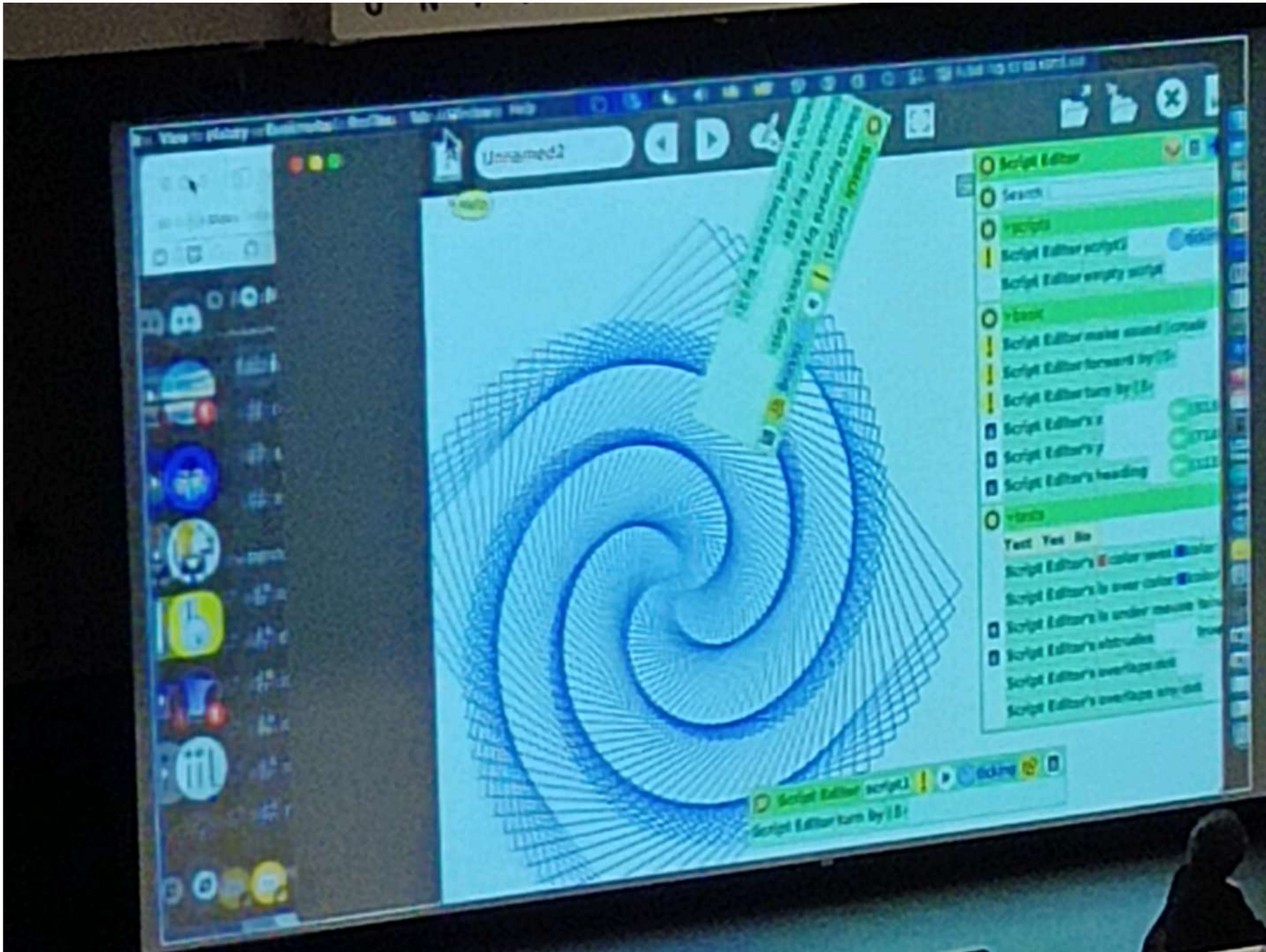
Fosdem 2025

Table des matières

Saturday

FOSDEM 2025 - Program to Learn: The Power of Creative Coding


Unnamed2
Script Editor
Script Editor script1
Script Editor empty script
Script Editor make sound
Script Editor forward by 15
Script Editor turn by 15
Script Editor's x
Script Editor's y
Script Editor's heading
Test
Yes
No
Script Editor's color sees color
Script Editor's is over color
Script Editor's is under mouse
Script Editor's obstruction
Script Editor's overlaps dot
Script Editor's overlaps any dot
Script Editor script1
Script Editor turn by 15

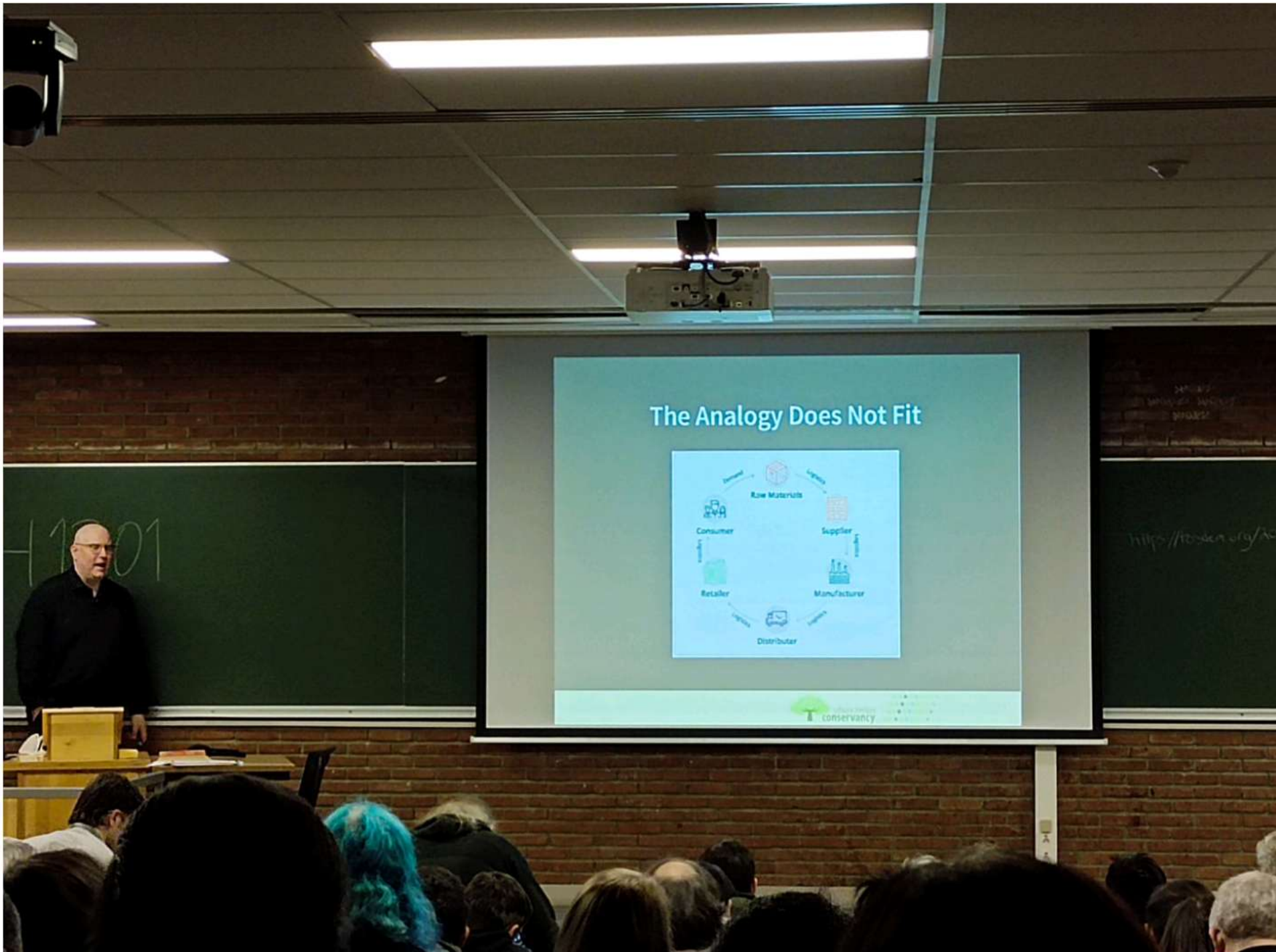

ULB
UNIVERSITÉ LIBRE DE BRUXELLES
FOSDEM
FOSDEM
FOSDEM'25

Janson 10h learn to code

- SketchJs (?)
- scratch
- Microblocks

from generating model/shape/sound to print/ even sewing machine/visualise
Build something

FOSDEM 2025 - Is There Really an SBOM Mandate?


The Analogy Does Not Fit
Raw Materials
Supplier
Manufacturer
Distributor
Retailer
Consumer
conservancy

H1301 11h00 sbom mandate in foss ?
Réalité de la supply chain (?) a-t-elle vraiment du sens au sens matériel/bien possédé ?
Pourquoi : assurer la traçabilité (?) fiabilité (?) d'un soft
Contradictoire avec le principe d’Open source software qui est partagé, modifié et réutilisé ?
Donc qu'est-ce que SBOM pour foss, comment pourrait-on le définir ? Est-ce nécessaire pour foss ?
Le terme supply chain est inhérent aux industries sans prendre en compte l'utilisateur, le terme de supply chain est peut-être galvaudé/utilisé à tort ?

FOSDEM 2025 - How Does Heinz Have 80% of a Commodity Market?* – Leveraging Trademarks in Free Software


What is a trademark?
Trademark = Word + "Goodwill"
Goodwill = Reputation
When you let someone else use your trademark, you are letting someone else benefit from your reputation
4
H1301


The value proposition of brand
• You have greater familiarity with the software
• You have early knowledge of the roadmap
• You can exercise influence on the project direction
• You can customize more quickly
• You can manage the complexity of the software
• You will have more reliable and accurate builds
Brand loyalty – "no one got fired for using IBM"
16

11h30 leveraging trademarks (Chestek)
Trademark ? = Mot + "bonne volonté"
-> réputation
-> comparaison
Bénéfice d'utiliser un trademark > utilisation de la réputation (consciente ou inconsciente)
But : Protection contre la confusion
Endorsement, relation dans les 2 sens
Trademark (protéger l'utilisateur)=/=patent (protéger le concepteur)
Le trademark serait le seul concept propriétaire qui fait sens pour le foss
Commodity
Trademark ne rend pas les choses meilleurs mais définit l'attente des utilisateurs/ qu'est ce qui est considéré bon /bien /mieux dans leur tête
Le gain ? Le fait de faire connaître et simplifier l'utilisation ou réutilisation, la loyauté
La perte d'un trademark? La perte de la "définition" par l'incompréhension/utilisation à tort en masse/le fait de permettre cette confusion

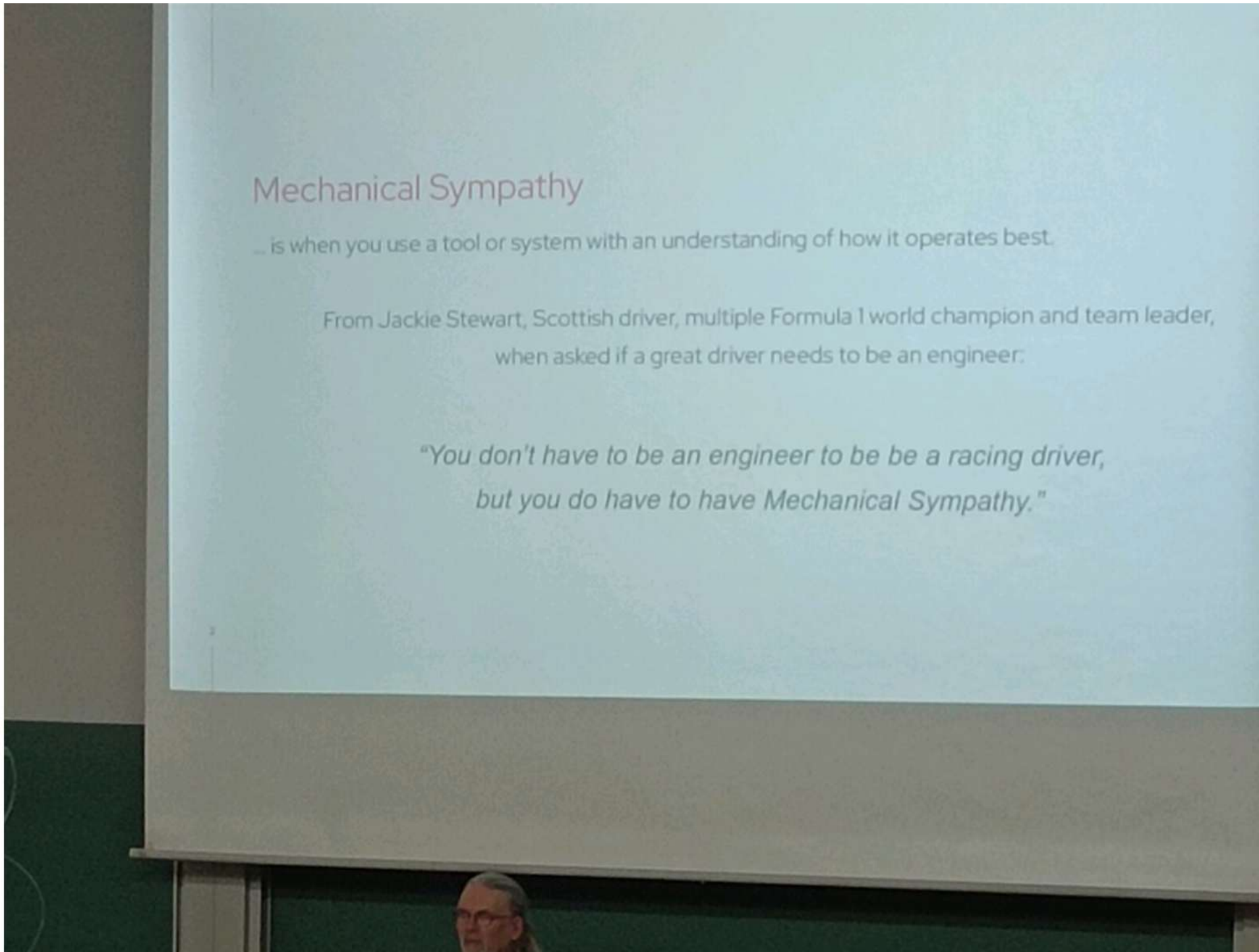
FOSDEM 2025 - Project Lilliput - Looking Back and Ahead


What is Lilliput about?
UA2118


GC Forwarding – Sliding Compaction
• Idea:
• 9 bits are enough to address 2⁹ = 512 words range
• Divide heap into 512 words (=4K B) blocks
• Use side-table with one entry per block (= 1/512th of heap size)
• Table stores forwarding base for each block
• It's the forwarding address of the first live object in the block
• Use 9 header bits to find forwarding address of object
fwd_addr = fwd_base[block] + fwd_bits << 3
JA2118

12h00 UA2.118 Henriot Free java Lilliput
Reduce memory footprint of java app
Depuis 2014 (jdk 14)
Réduction de 20%
En compressant et évitant l'espace inutilisé dans l'encodage ??

FOSDEM 2025 - (Almost) everything I knew about Java performance was wrong


Mechanical Sympathy
... is when you use a tool or system with an understanding of how it operates best.
From Jackie Stewart, Scottish driver, multiple Formula 1 world champion and team leader,
when asked if a great driver needs to be an engineer:
"You don't have to be an engineer to be be a racing driver,
but you do have to have Mechanical Sympathy."

12h30 Java perf
Consommation de puissance deux plus de puissance nécessaire pour chaque action, on récupère un résultat 1fois /2 d'où 2x plus de puissance nécessaire (cpu 4ghz serveur 2ghz?)
Améliorer la perf ? Plus vite ou plus vaste, on ne peut pas aller plus vite donc
Prédiction de la machine sur ce qui va être utiliser pour économiser
Clock cycle => latence d'une opération (diff en fonction du type de l'opération)
Où cela peut faire défaut ? Cache "scopevalie cache" qui permet la prédication et la diminution du délai
Hashed interface checkcast

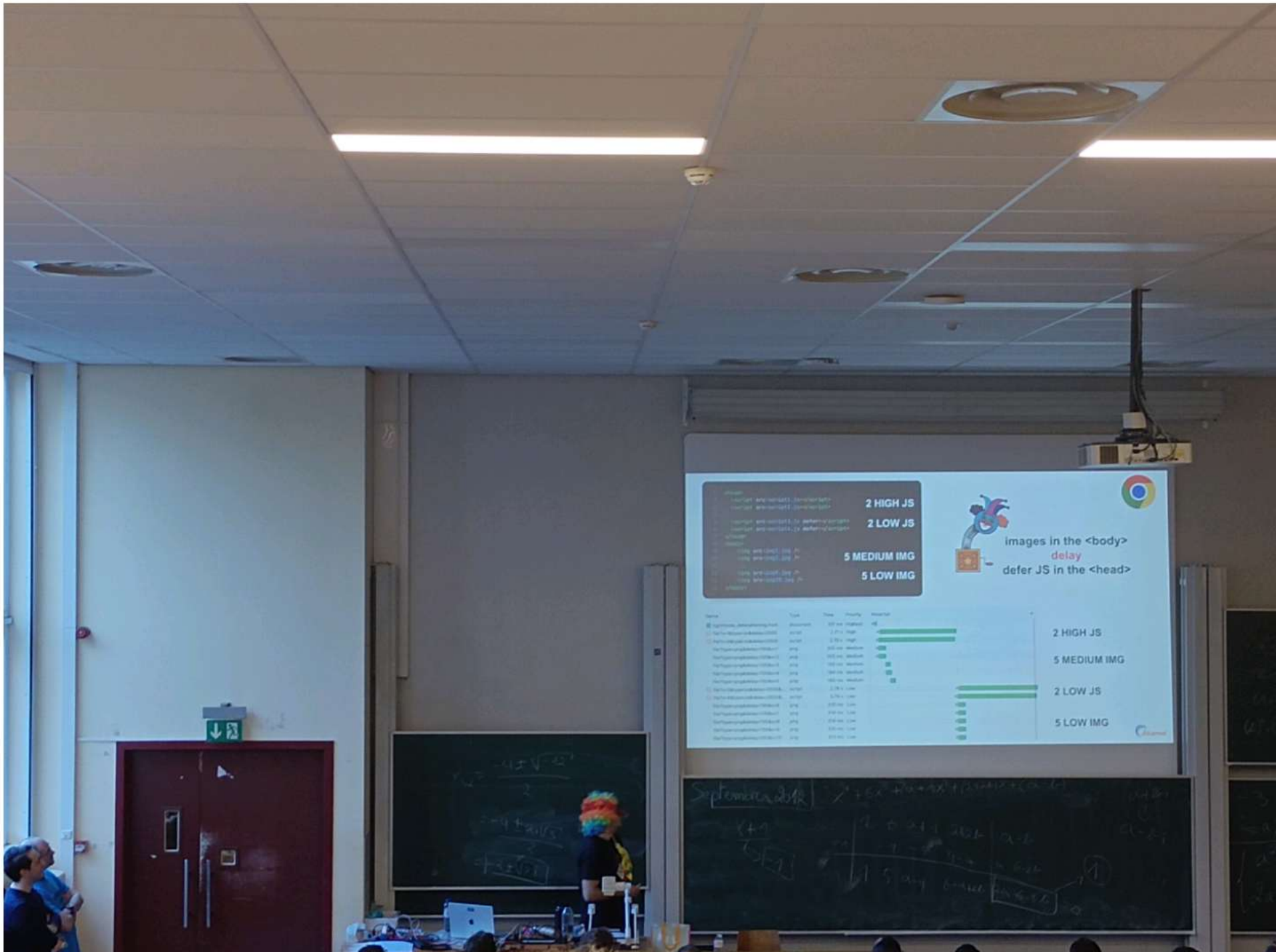
FOSDEM 2025 - Stratoshark: Applying the power of Wireshark to System Calls and Logs

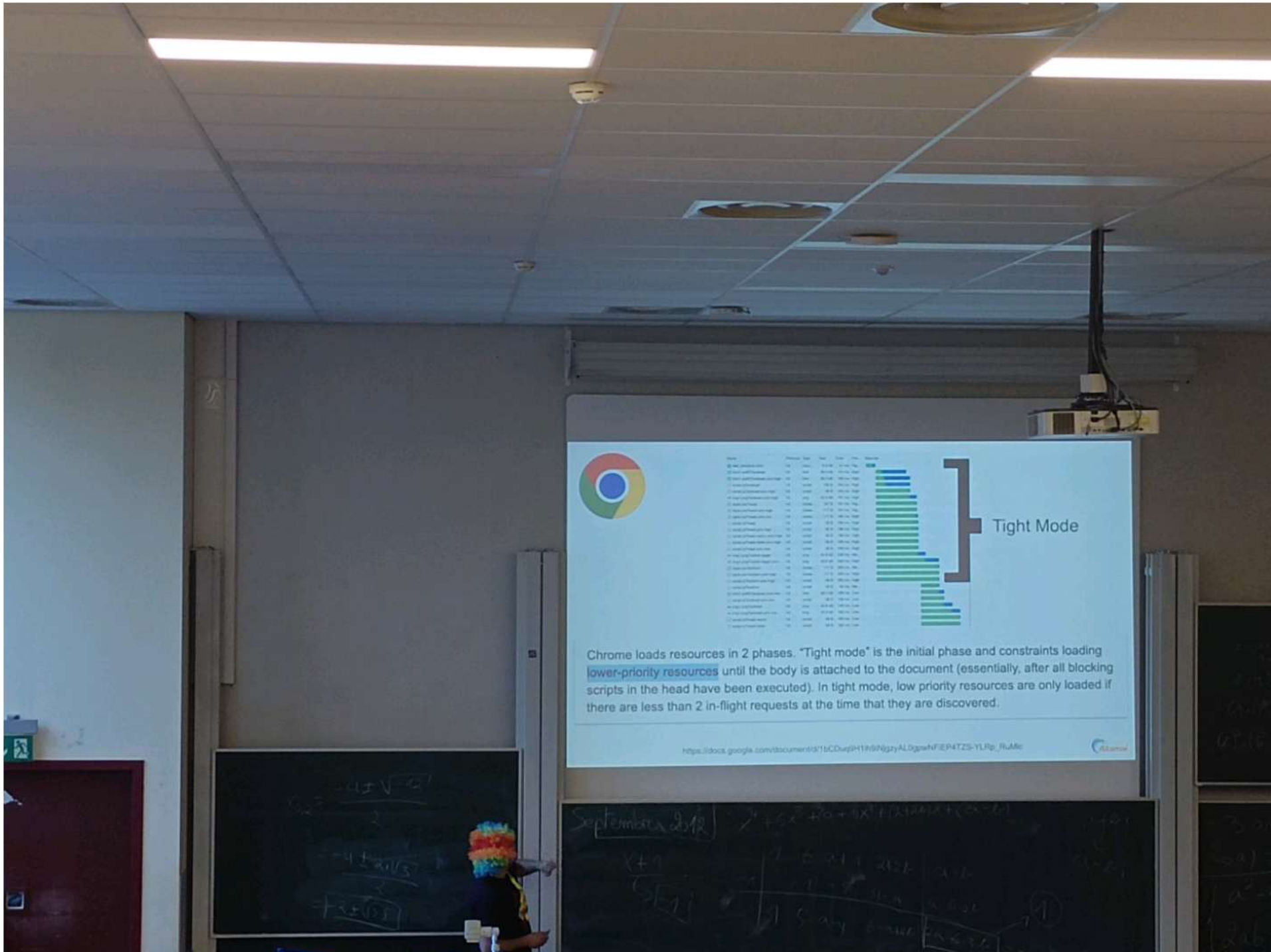

FOSDEM
A Journey forged in OSS
Falco and Sysdig open source tools were built for a new world of cloud-native computing and containers.
While inspired by the deep visibility of Wireshark, they have given back to Wireshark in the form of Stratoshark.
Founded by the creator of
WIRESHARK
Protocol analysis and network security
Inspired by Wireshark
Sysdig
Open Source
Deep container forensics and troubleshooting
D&R based on sysdig libraries
Falco
Cloud native threat and anomaly detection
Contributing back to the Wireshark Foundation
A byproduct of Falco & Wireshark
STRATOSHARK
System Call (SCAP) & Audit Log analysis via Falco plugins in a Wireshark interface
Stratoshark forked the Falco libraries
FOSDEM
FOSDEM

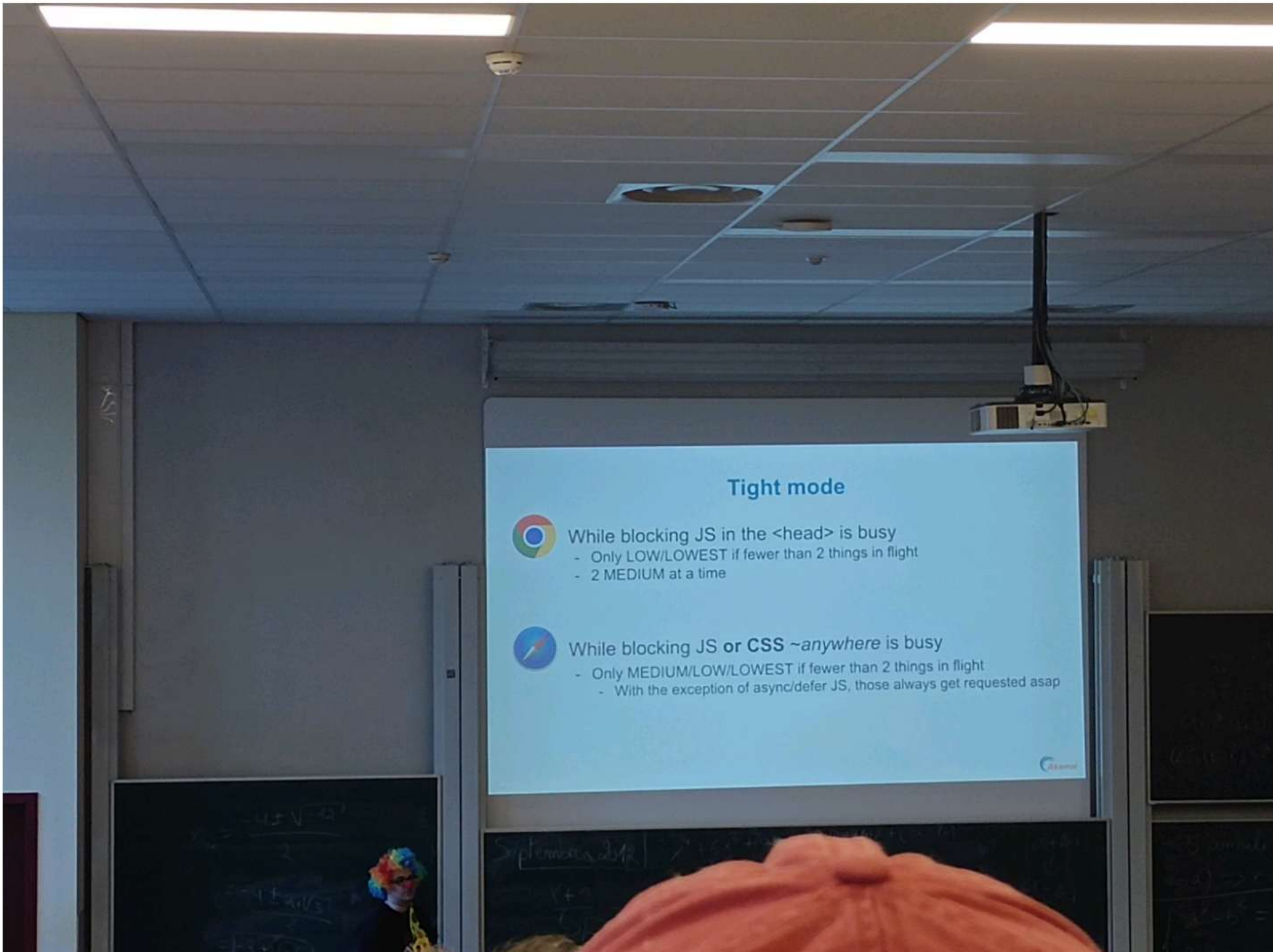
14h00 La fontaine Stratoshark
Define rules on how detect security threaths
Wireshark :protocol and network
Sysdig: container
Falco : librairies

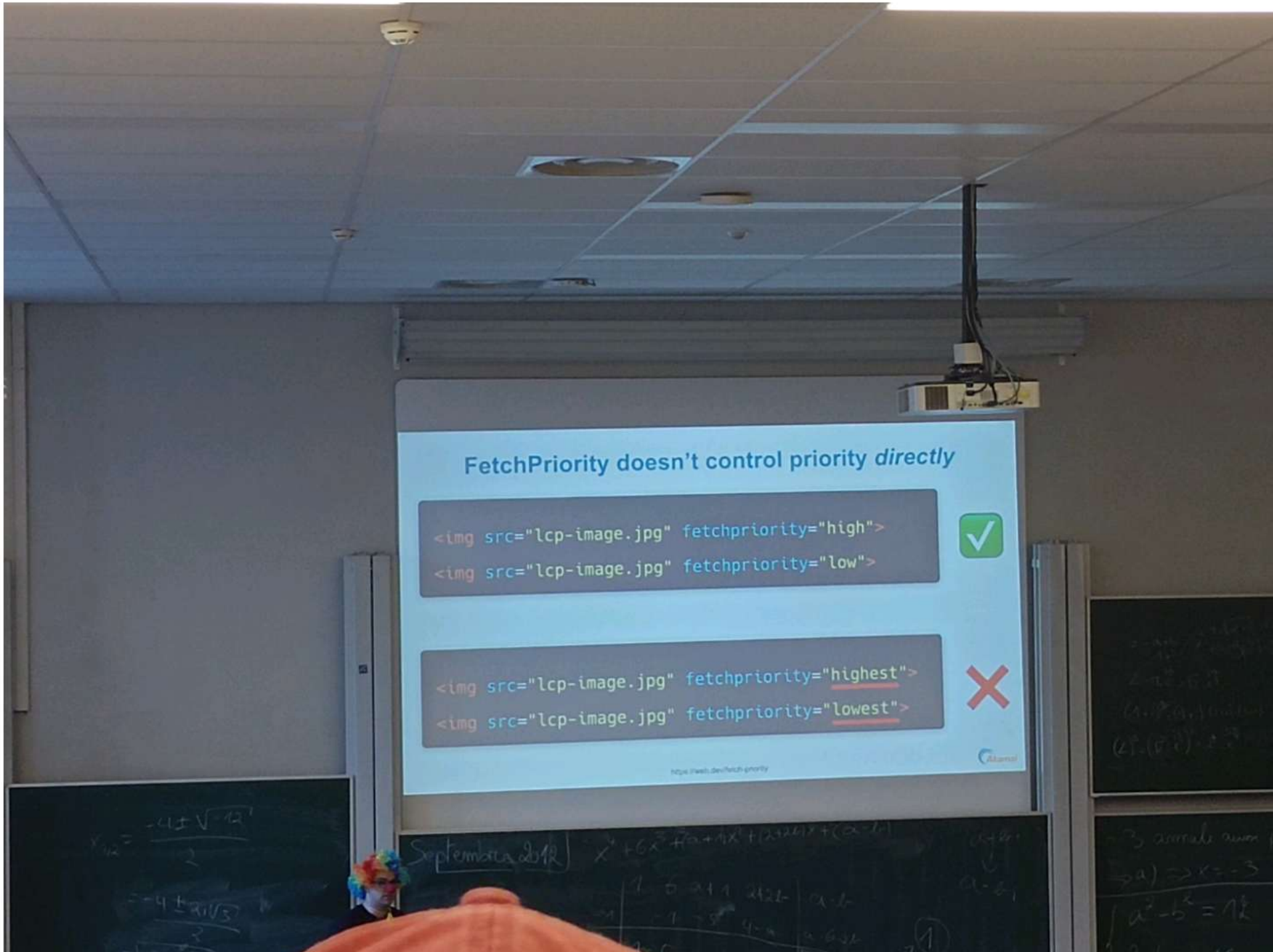
FOSDEM 2025 - How browsers REALLY load Web pages

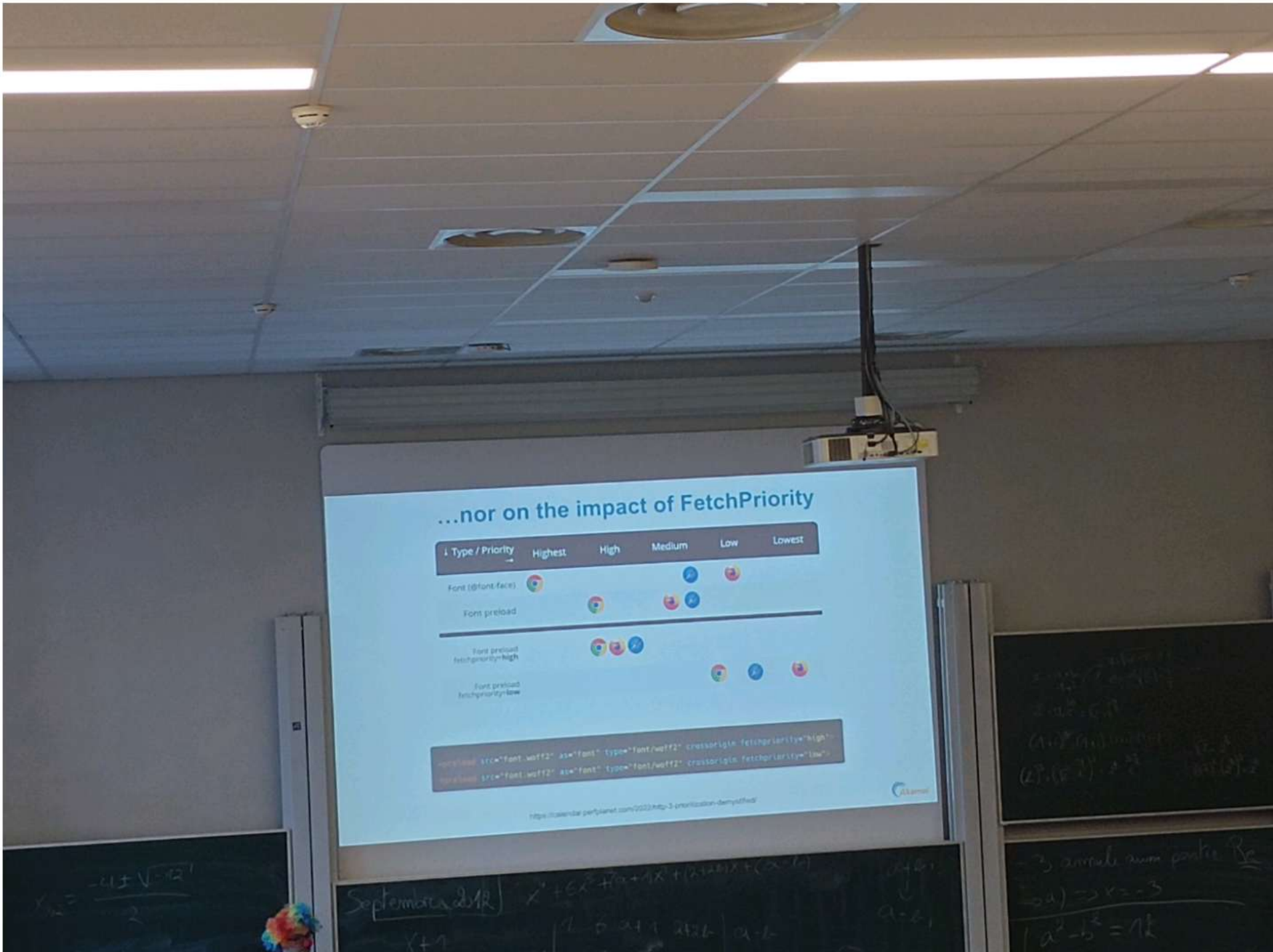

Priority: where stuff is in HTML and how it's loaded
JS

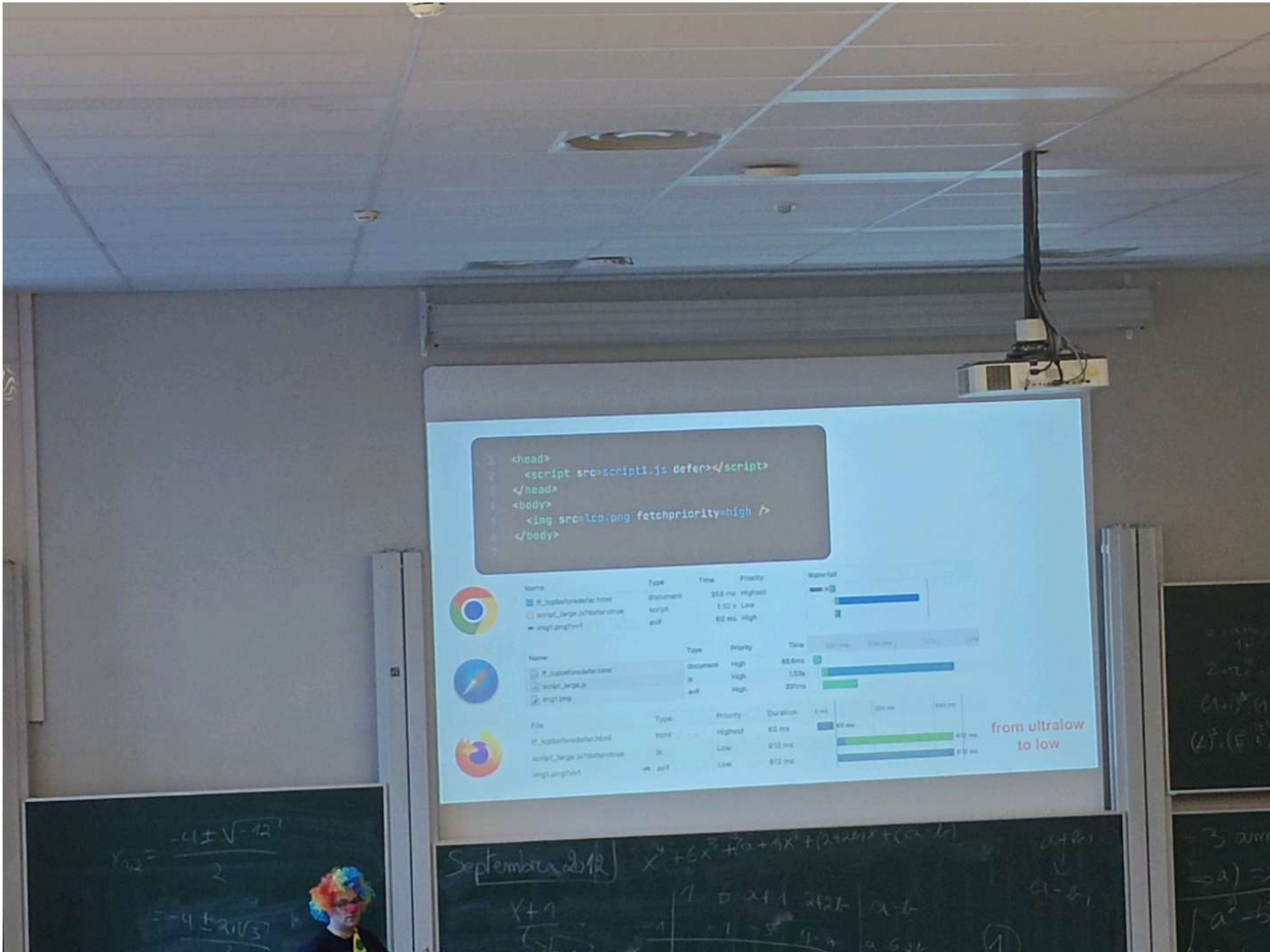

2 HIGH JS
2 LOW JS
5 MEDIUM IMG
5 LOW IMG
images in the <body>
delay
defer JS in the <head>
2 HIGH JS
5 MEDIUM IMG
2 LOW JS
5 LOW IMG


Tight Mode
Chrome loads resources in 2 phases. "Tight mode" is the initial phase and constraints loading lower-priority resources until the body is attached to the document (essentially, after all blocking scripts in the head have been executed). In tight mode, low priority resources are only loaded if there are less than 2 in-flight requests at the time that they are discovered.

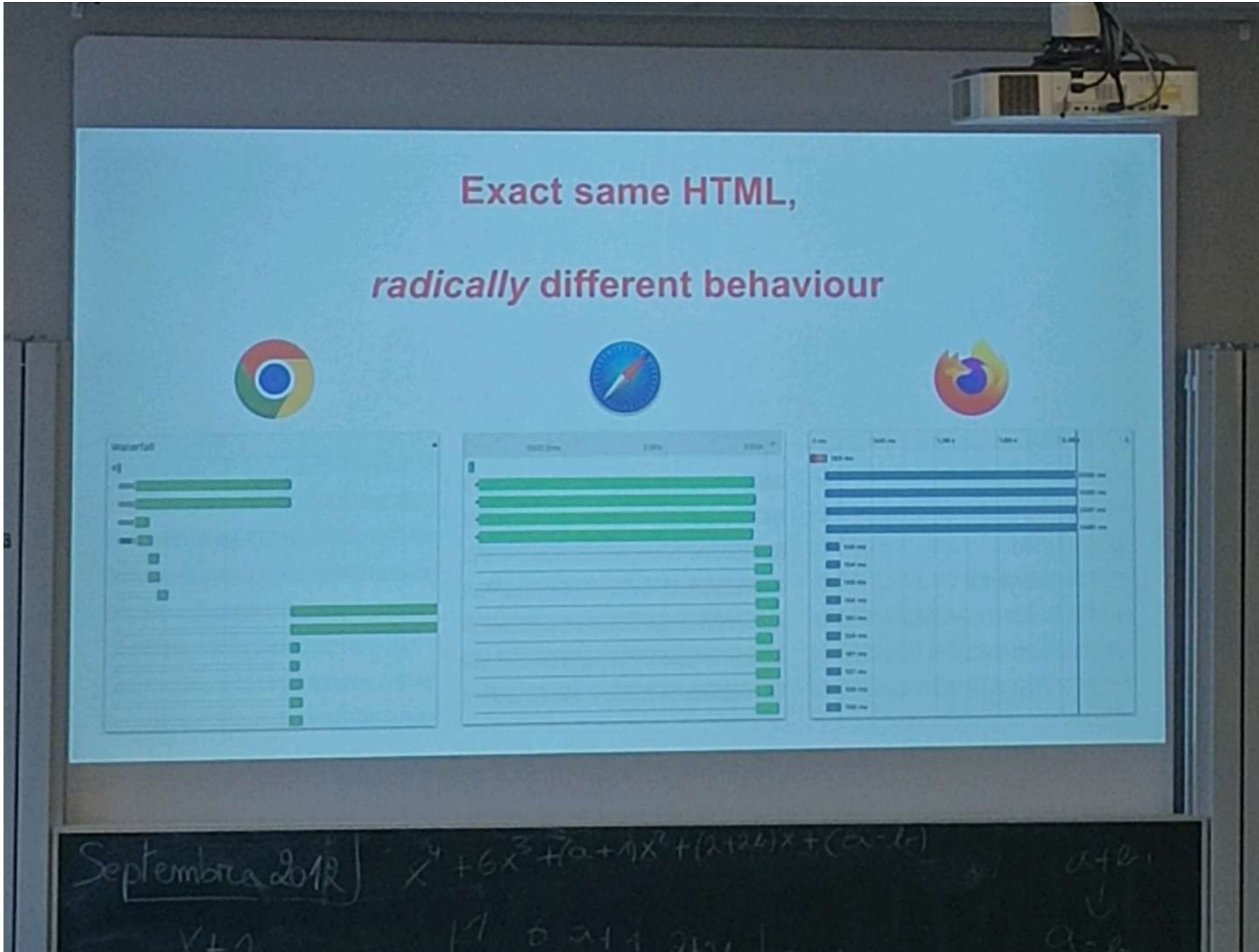

Tight mode
While blocking JS in the <head> is busy
- Only LOW/LOWEST if fewer than 2 things in flight
- 2 MEDIUM at a time
While blocking JS or CSS ~anywhere is busy
- Only MEDIUM/LOW/LOWEST if fewer than 2 things in flight
- With the exception of async/defer JS, those always get requested asap


FetchPriority doesn't control priority *directly*
<img src="lcp-image.jpg" fetchpriority="high">
<img src="lcp-image.jpg" fetchpriority="low">
<img src="lcp-image.jpg" fetchpriority="highest">
<img src="lcp-image.jpg" fetchpriority="lowest">
https://web.dev/fetch-priority
Akamai


...nor on the impact of FetchPriority
↓ Type / Priority →
Highest
High
Medium
Low
Lowest
Font (@font-face)
Font preload
Font preload fetchpriority=high
Font preload fetchpriority=low


<head>
<script src=script1.js defer></script>
</head>
<body>

</body>
from ultralow
to low


Exact same HTML,
radically different behaviour
Waterfall

15h10 UA2.220 how web page are loaded
Généralement les navigateurs chargent les données en 2 batch "two step waterfall"
Retour des réponses parfois en inversé, le serveur renvoie en premier la dernière demande
Priorité donnée par la hiérarchie du code ? Priorité mis en place,
Si on envoie 1 demande majeure et toute de suite une mineure puis une autre ..., le canal est surchargé (comme une entrée sortie de rame) et augmentation du risque d'envoyer n'importe quoi n'importe quand
Ce qui amène à différents comportements des navigateurs (différents 2step waterfall)
Exemple : chrome (tight mode/actively delayed) prioritise le html et retarde le JS async ou defer (explicitement demandé en différé) (photo)
La priorité n'est pas donnée par la hiérarchie mais par le type (IMG,JS,etc)
Dans chrome le script est bloqué s'il est dans le head mais pas si il est dans le corps (tout est envoyé en même temps)
Safari ne bloque pas (tight mode) sur le script (mais le fait bien sur les images)
Mozilla n'a pas de tight mode tout est traité immédiatement (trusts the code, importance des best practices)
Comment améliorer / gérer ?
=> FetchPriority
=> Lower or higher (not fixed)
FetchPriority ne marche pas sur safari, ok sur chrome (combiné avec tight mode), très utile sur Firefox (fine grain)
Pbs comment faire fonctionner pour plusieurs navigateurs en même temps ? Les règles ou les interprétations sont parfois complètement contradictoires entre navigateurs

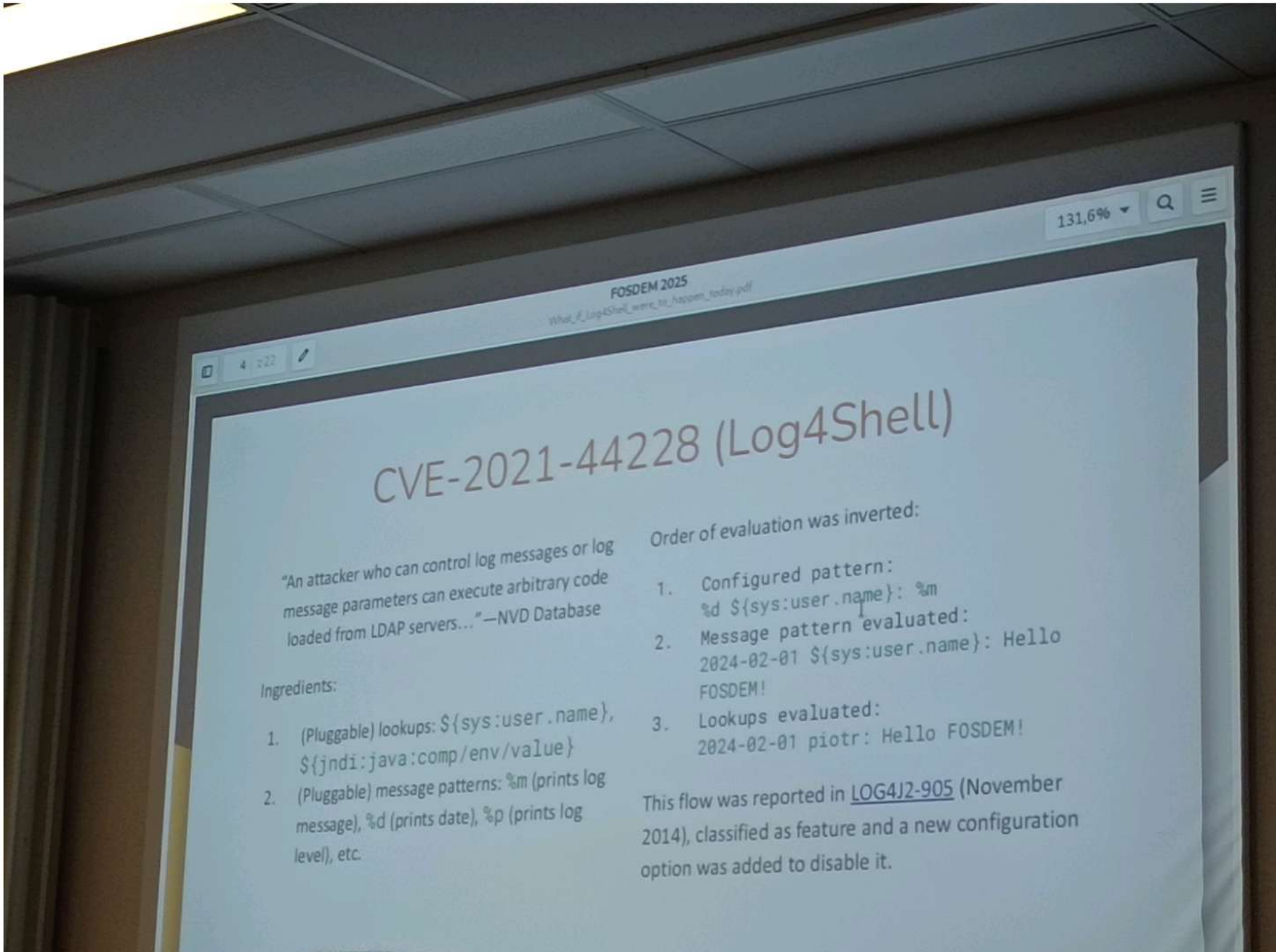
FOSDEM 2025 - [RESCHEDULED] CERN CTA Service: writing LHC data to tape with opensource software on commodity hardware

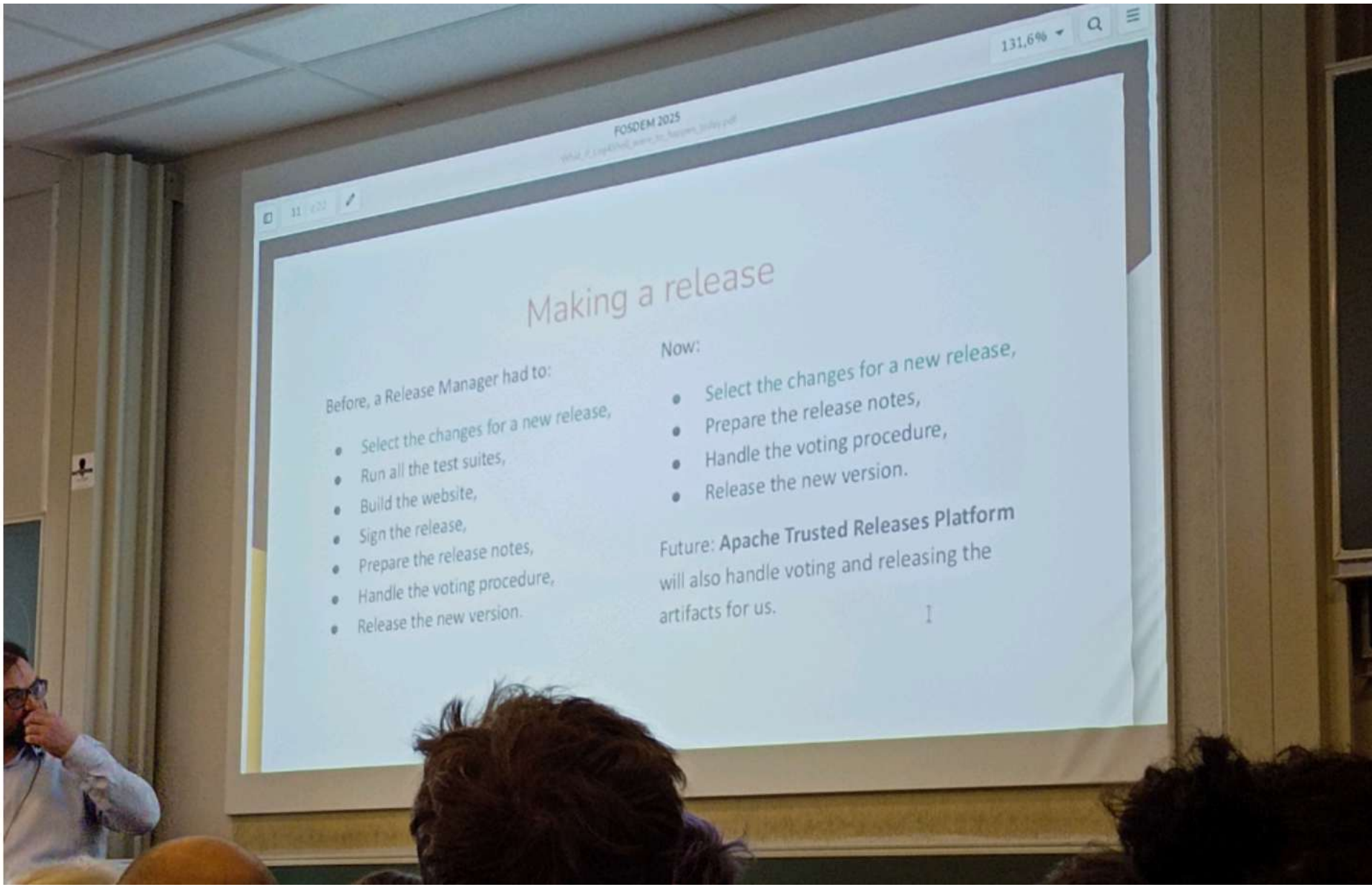

Tape namespace statistics at CERN
Data on tape has more than doubled since start of Run-3
+250PB in 2024
2024-08
840PB
2022-07
Start of Run-3
420PB
2018
End of Run-2
340PB
2015
Start of Run-2
100PB
401
GLOBE

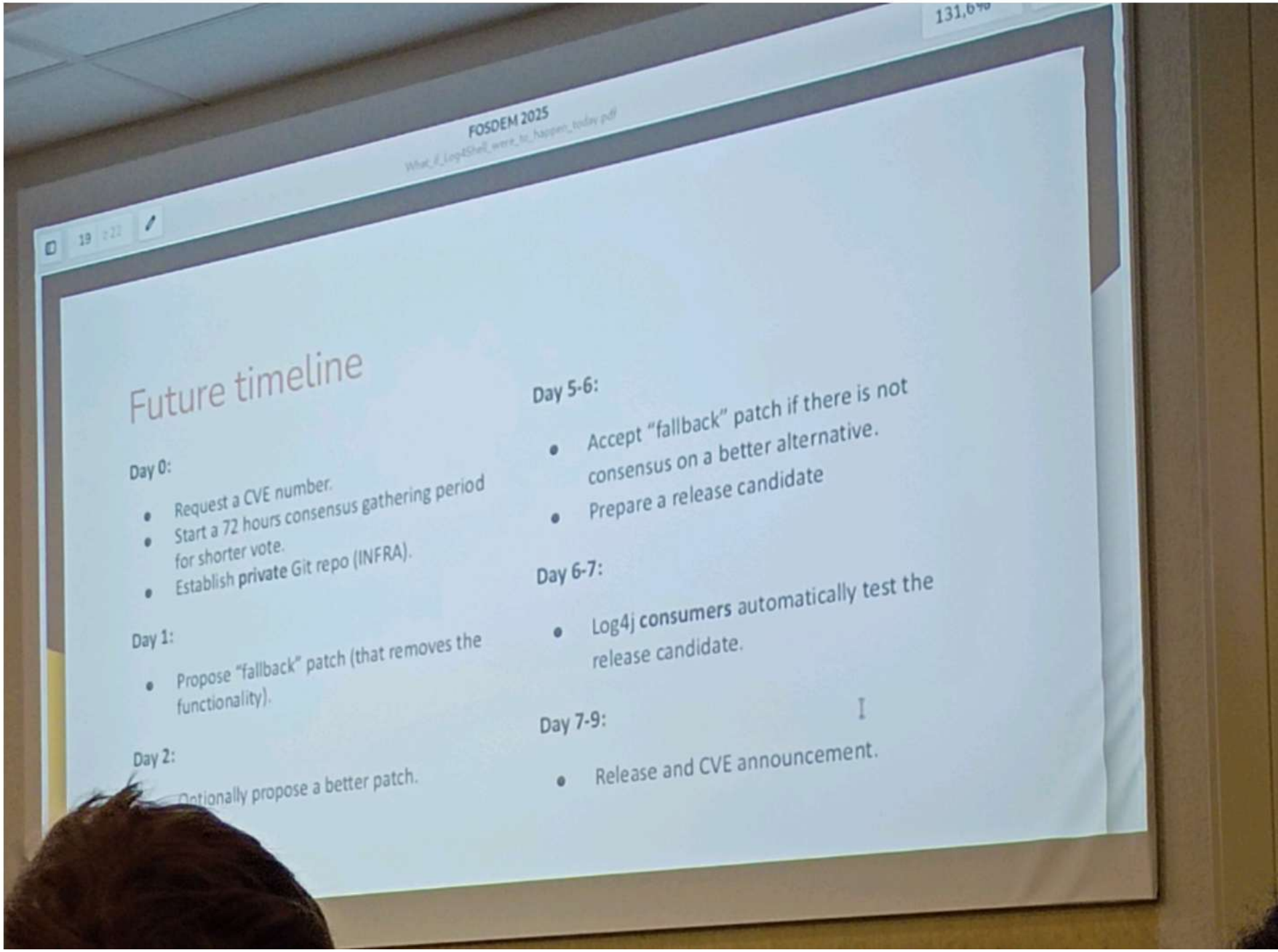

CERN continuous improvement of EOSCTA operations
RUNDECK
podman
influxdb
fluentd
Grafana
HELM
GitLab
berlin swamp fest

15:55 Software define storage Cern to tape
Exponential data amount (840PB / 2015 100PB) expected 1.3EB around 2025
Store in both private and open techno
Castor => EOS+FTS+tape
CTA
Balance entre l'archivage et la lecture, flexible sur la répartition mais toujours garde de la dispo pour l'archivage d'un côté et la lecture de l'autre

FOSDEM 2025 - What if Log4Shell were to happen today?


FOSDEM 2025
What_if_Log4Shell_were_to_happen_today.pdf
131,6%
CVE-2021-44228 (Log4Shell)
"An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers..." —NVD Database
Ingredients:
1. (Pluggable) lookups: ${sys:user.name}, ${jndi:java:comp/env/value}
2. (Pluggable) message patterns: %m (prints log message), %d (prints date), %p (prints log level), etc.
Order of evaluation was inverted:
1. Configured pattern: %d ${sys:user.name}: %m
2. Message pattern evaluated: 2024-02-01 ${sys:user.name}: Hello FOSDEM!
3. Lookups evaluated: 2024-02-01 piotr: Hello FOSDEM!
This flow was reported in LOG4J2-905 (November 2014), classified as feature and a new configuration option was added to disable it.


FOSDEM 2025
131.6%
Making a release
Before, a Release Manager had to:
Select the changes for a new release,
Run all the test suites,
Build the website,
Sign the release,
Prepare the release notes,
Handle the voting procedure,
Release the new version.
Now:
Select the changes for a new release,
Prepare the release notes,
Handle the voting procedure,
Release the new version.
Future: Apache Trusted Releases Platform will also handle voting and releasing the artifacts for us.


FOSDEM 2025
Future timeline
Day 0:
Request a CVE number.
Start a 72 hours consensus gathering period for shorter vote.
Establish private Git repo (INFRA).
Day 1:
Propose "fallback" patch (that removes the functionality).
Day 2:
Optionally propose a better patch.
Day 5-6:
Accept "fallback" patch if there is not consensus on a better alternative.
Prepare a release candidate
Day 6-7:
Log4j consumers automatically test the release candidate.
Day 7-9:
Release and CVE announcement.

17h00 UB4.132 what if log4shell
Cve 2021 44228 remote execution code
Reason: inverted order of evaluation (known and fixed on optional feature in 2014-5 and then forgotten?)
How improve ?

- Reproducibility
- Constant upgrade if tests ok
- Ensure CI/CD
- Ensure tests

testing: the pb lot of tests with failures, long time to process, how to improve? :

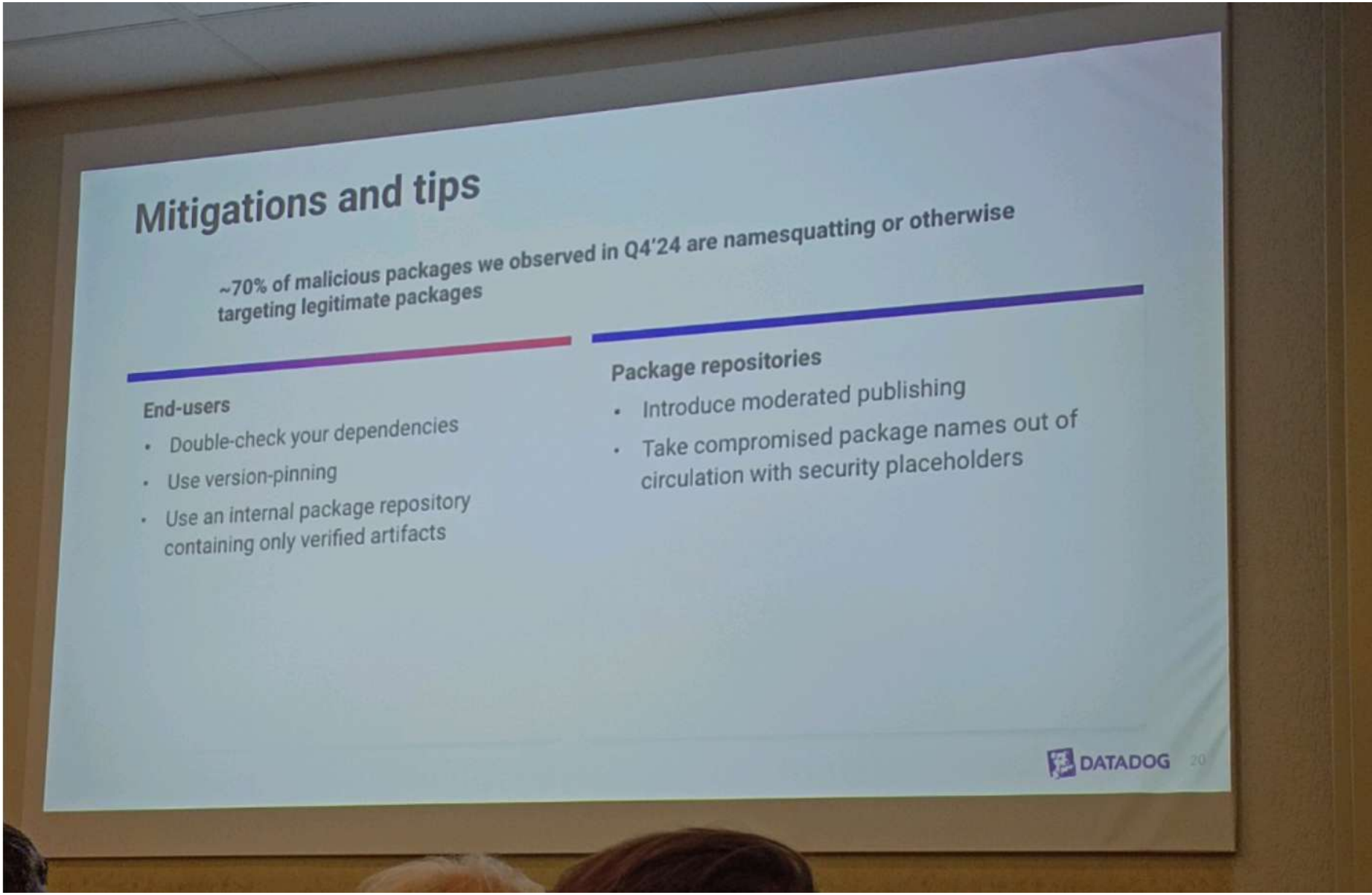
- Fuzzing
- Dynamic tests

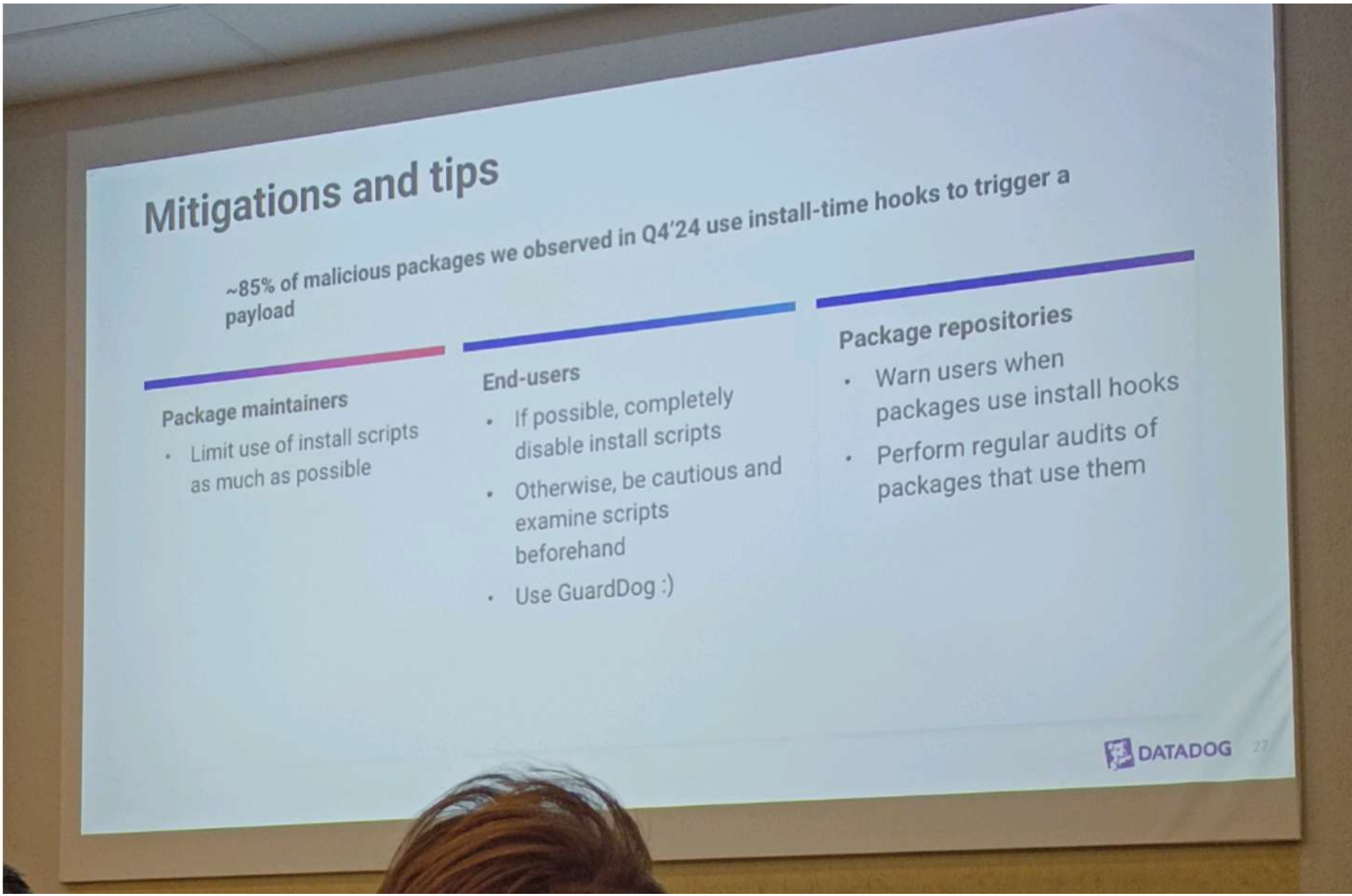
Handling feature:
SBOM:
Documentation:

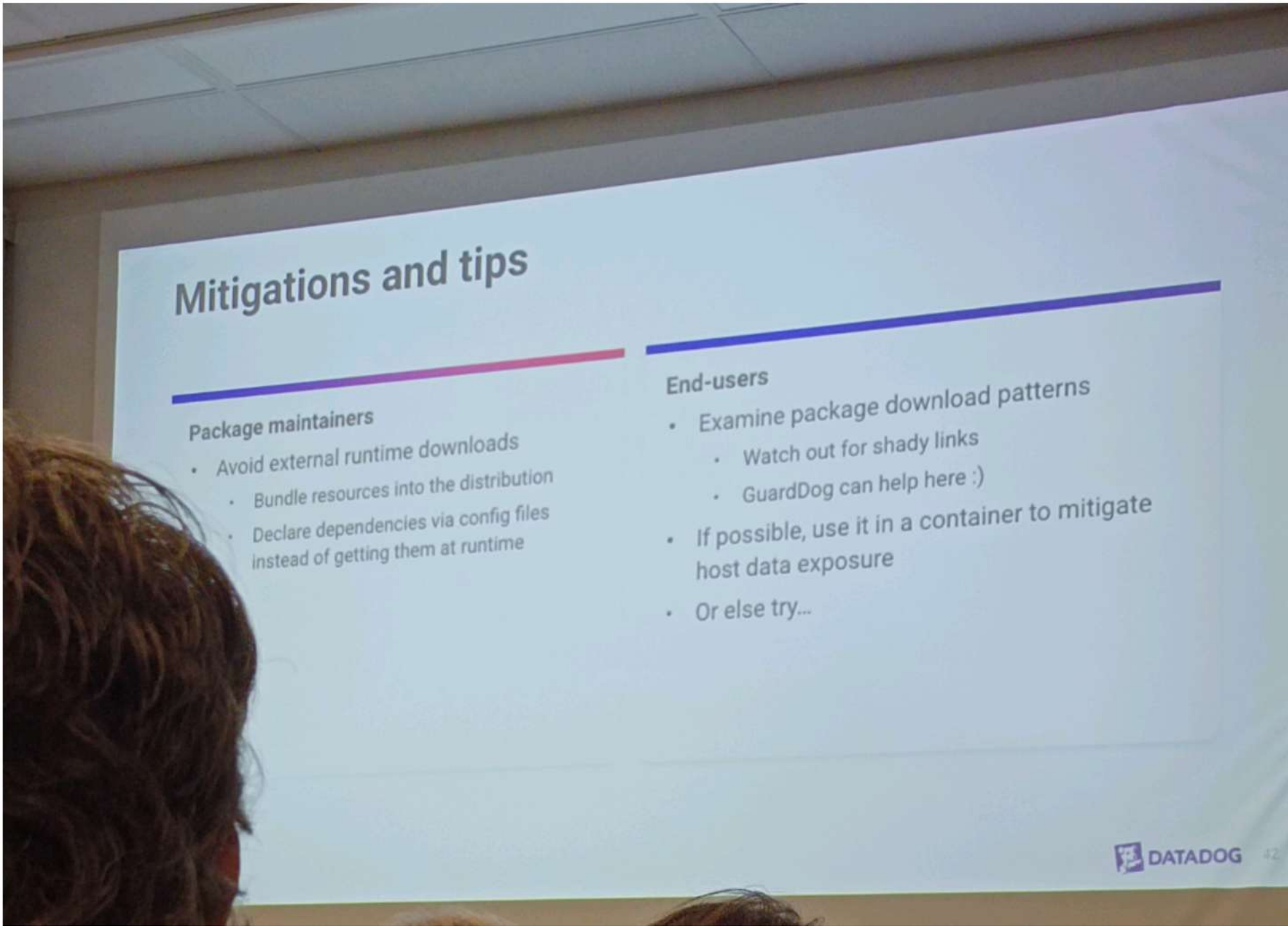
FOSDEM 2025 - How Threat Actors Are Weaponizing Your Favorite Open-Source Package Registry


Software supply-chain attacks
Source integrity
Build integrity
Unauthorized change
Compromise source repo
Build from modified source
Compromise build process
Upload modified package
Compromise package repo
Use compromised package
Source
Build
Package
Developer
Consumer
Use compromised dependency
Dependency
DATADOG


Targeting developers via popular packages
Namesquatting
Publish a malicious package whose name resembles that of a targeted package
Combosquatting
Combine ecosystem or app-specific terms with targeted package name
requests → py-requests
Typosquatting
Malicious package name is a typo of the targeted package name
requests → reqeusts
Package takeover
Compromise an existing legitimate package
Compromise maintainer creds
Submit malicious PR
Corrupt build process
Target the package repository
DATADOG


Mitigations and tips
~70% of malicious packages we observed in Q4'24 are namesquatting or otherwise targeting legitimate packages
End-users
Double-check your dependencies
Use version-pinning
Use an internal package repository containing only verified artifacts
Package repositories
Introduce moderated publishing
Take compromised package names out of circulation with security placeholders
DATADOG
20


Mitigations and tips
~85% of malicious packages we observed in Q4'24 use install-time hooks to trigger a payload
Package maintainers
Limit use of install scripts as much as possible
End-users
If possible, completely disable install scripts
Otherwise, be cautious and examine scripts beforehand
Use GuardDog :)
Package repositories
Warn users when packages use install hooks
Perform regular audits of packages that use them
DATADOG
27


Mitigations and tips
Package maintainers
Avoid external runtime downloads
Bundle resources into the distribution
Declare dependencies via config files instead of getting them at runtime
End-users
Examine package download patterns
Watch out for shady links
GuardDog can help here :)
If possible, use it in a container to mitigate host data exposure
Or else try...
DATADOG

17h30 threat actors weaponize registry (Datadog)
Supply chain attack: eg. Solar winds
Plusieurs points d'attaque possible
Comment protéger

- Guarddog
- Rigueur et awareness
- Ne pas accepter du code illisible /obstrué
- Supply chain firewall

Type d'attaque

- Nommage de paquet qui ressemble
- Incitation a télécharger et exécuter du code malicieux à notre insu
- Planquer le code malicieux dans du code difficilement lisible

https://github.com/DataDog/guarddog GuardDog is a CLI tool that allows to identify malicious PyPI and npm packages or Go modules. It runs a set of heuristics on the package source code (through Semgrep rules) and on the package metadata.
https://github.com/DataDog/supply-chain-firewall Supply-Chain Firewall is a command-line tool for preventing the installation of malicious PyPI and npm packages. It is intended primarily for use by engineers to protect their development workstations from compromise in a supply-chain attack.
https://github.com/DataDog/malicious-software-packages-dataset This repository is an **open-source dataset of 6488 malicious software packages** (and counting) identified by Datadog, as part of our security research efforts in software supply-chain security. Most of the malicious packages have been identified by GuardDog.
https://securitylabs.datadoghq.com/ Datadog Security Labs

Sunday

FOSDEM 2025 - GIMP 3 and beyond


More usage in Science
Jeff Struven @jstroov · 2 years ago
Author
Hi Jacob, Thanks for replying to my issue. The medical device we're developing scans slides at high magnification. The software we are developing for the device generates what we call a pyramid TIFF file where the first directory entry is the whole slide image roughly 90,000x100,000 pixels. The next directory entry is a reduced image that is half the size in each width and height of the whole slide image. The next directory entry is a reduced image that is 1/4th the size in each width and height of the whole slide image. And so on. These images run about 1.5 GB to 4.2 GB so I'm not sure where I could put one so you could work with it. Regards,Jeff
citing gimp in research?
Edit
Open
Issue created 18 hours ago by Cameron Leahy
Hi,
Sorry if this is not quite the right place to post this, but I wanted to make sure it got viewed by someone who could answer my question. I am using gimp in my research (astronomical image processing) for various reasons, and I was wondering if there was a way to cite gimp. It performs an important step in my algorithm (it's not like I'm just using it to touch up plots) so I think it definitely deserves a citation, but I'm not sure how to do this. So please let me know if there's a way I can cite gimp.
Thanks, Cam
FOSDEM'25


UNIVERSITÉ LIBRE DE BRUXELLES
FOSDEM'25

10h00 Janson Gimp 3
Better Support PSD
Tiff
More non destructive editing : from blur to original for example
Plugin API
Ctx (vector, …)
Gimp 3 RCs ongoing, final soon (follow on Gitlab)

FOSDEM 2025 - Room changeover & Intro to the Public sector Open Source block

11h EU AW1.120 presentation & open discussion

FOSDEM 2025 - Making Workspaces Work Together (And Across Borders)


INTERDIT
DE BOIRE
ET MANGER
Dans votre intérêt,
aidez-nous
garder ce local propre.
AW1120

11h20 working together across borders
(FR DE gov)
OpenDesk (DE)
'lasuite' (FR)
Accelerating the process on sharing and working together
Added (NED) to the challenges
https://lasuite.numerique.gouv.fr/
https://www.opendesk.eu/en

FOSDEM 2025 - openDesk and beyond: building the EuroStack

11h35 Eurostack
Nécessité d'indépendance sur les technologies pour l'Europe, mise sur OSS provenant d'Europe
Actuellement on essait de définir qu'est ce que l'eurostack qu'on veut mettre en place, identifier les composants
Q Existe il un retour sur l'expérience de ces challenges A avec l'arrivée de NED le process de retour d'expérience pourrait se construire
Q how garanti it's not going to die A both OSS and partners to keep on going , through cooperation, more implications nor only garanti on tools/products but also people
Q projet planifié initialement de 2020~ à 2027, mais après ? A wider scope, create opportunities?
Q how promote in the EU (like opendesk or laduite) ? A first presentation leverage, prove by example that it will help a better co-working between gov, educate the colleagues in the parlement
Q how can we involve private sectors ? A now how govs work and their needs, because they want to work from now, start with OSS because is accessible and usable already ,
Q OSS make private techno evolve so fast A agreement
Communication issue, education issue , need to improve

FOSDEM 2025 - Digital Identies in disarray

12h Digit identites
eID (European identy)
Why ? Because now we use ID like Google, apple and so, not European ID, we don't know where the data go

FOSDEM 2025 - Accelerating Digital Transformation in Europe: The Role of Digital Public Goods and Open Source Collaboration


Primero deployment options
Tier 1
DIY
Tier 3
UNICEF Hosted SaaS
Tier 4
Hybrid
Fully supported hosting on UNICEF's Azure cloud. Includes support to deploy, configure, operate, remote training, regular upgrades and technical support.
Support to install production server locally. This includes support to deploy, secure, operate, remote training, regular upgrades and technical support.
CYBERSTAND.EU

12h15 digit commons Eu digit transformation
Digit public good: commodity for ppl provided by gov for no cost to the users
DPG standards (voir présentation)
Primero: a digital public good developed for children protection (unicef, …) instead of duplicate for each org, an OS tool to handle a common issue/need,

FOSDEM 2025 - Government Collaboration - Intro

13h10 AW1.126 gov collab - digit sovereignty across Eu and world

FOSDEM 2025 - How is Development and Collaboration Done in Public Sector Open Source Software Projects? Insights from Six Mature Case Studies

13h15 6 cases study

- Energyplus
- Os2form
- Oskari
- Geotrek
- Dinum
- Io-app

Core team: 15~ ppl team
GitHub
Formal & agile process
Centered around 1 entity
Decisions top-down
Vendors / suppliers: local / national
Users scope : first limited for then much wider
Improve: public involvement, growing , transparency

FOSDEM 2025 - OSOR Handbook on Open Source Software in Public Administration


OSOR
Knowledge Centre
Reports, guidelines, research papers, case studies, and repositories useful for public administration and for all users of FOSS.
OSOR latest milestones
OSOR Handbook, new training courses, paper on policy and trends

13h30 Osor handbook
OSOR: OS observatory for Eu
Handbook: guide to Eu public sector
From 2022
Feedback and open workshop in 2024
Sharing into public sector
How / Rex

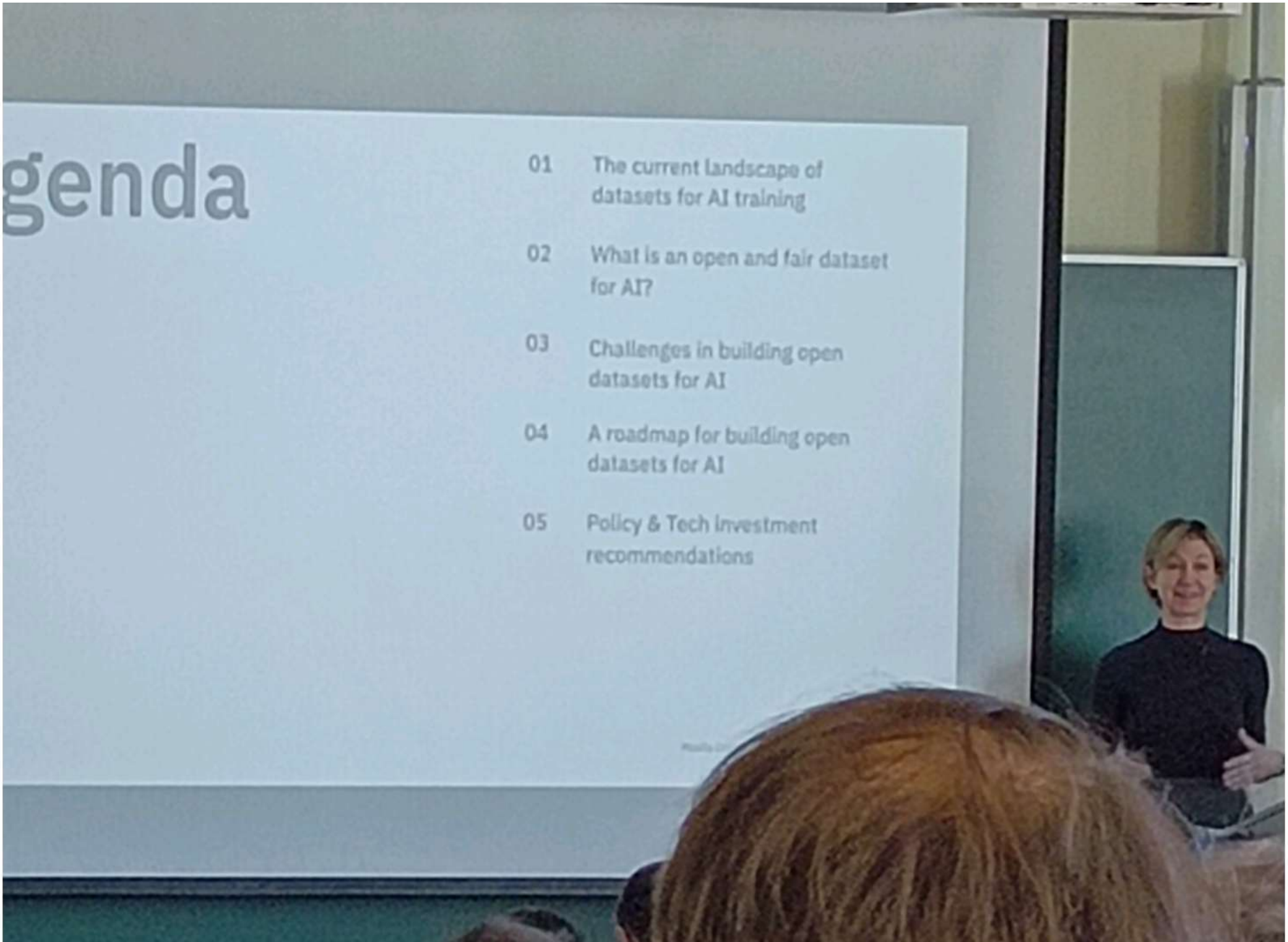
- Consultation
- Simplify (from technique knowledge and policies knowledge)
- Community

FOSDEM 2025 - Nubo: the French government sovereign cloud


Sovereignty: a Definition Attempt
« The ultimate authority in the decision-making process of the State and in the maintenance of order » (Britannica Academic)
Context of a State's cloud
« a computing environment that is owned, controlled, and operated by the State »
Ensures data and services are subject to its laws and regulations
It is not just mere independence
nubo
OpenInfra
FOUNDATION

13h45 Fr cloud Nubo
OpenStack (15yo, used for public and private, around the world)
OpenInfra:
Need for local infrastructure
Why OS: avaibility transparency independence interoperability
Nubo: PIA, tooling & hosting, from 2016, exposed to internet & RIE, Kubo (kubernetes),
Free software: product vs project
bzg.fr/logiciel-produit-projet/
Sovereignty: owned controlled operated by the state
Q security/diffusion restreinte and using cloudp (?) A not yet for diffusion restreinte and working with cloudp
Q how manage many teams in the project A ministries
Q specific range and scope, how involve A incite to try and working in parallel
Q how explain to another ministry (outside Fr) to involve A no receipe, public aspose(?)
Q timeline for distribution A not yet

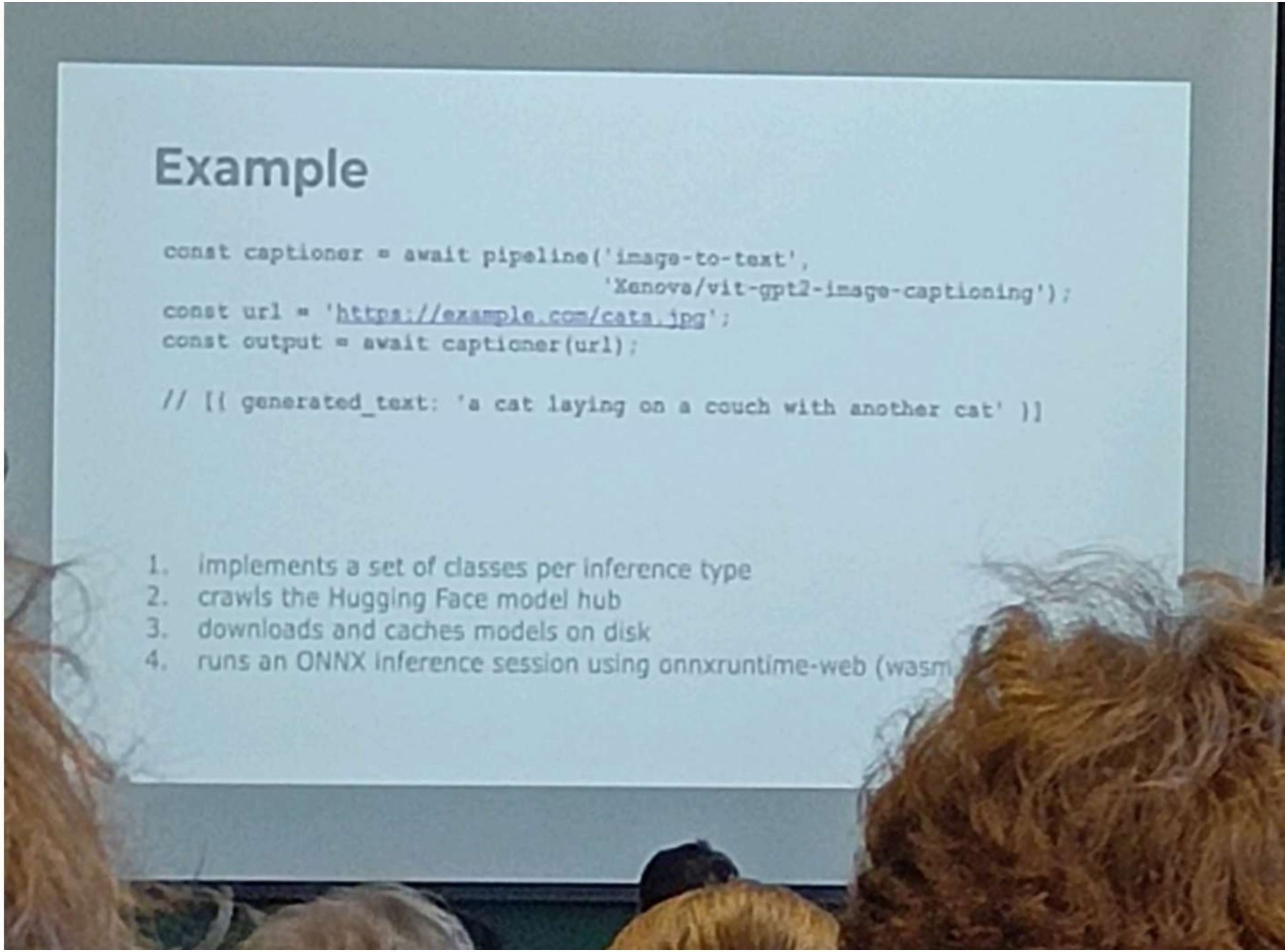
FOSDEM 2025 - Community Insights: Best Practices for Open Datasets for LLM training


genda
01 The current landscape of datasets for AI training
02 What is an open and fair dataset for AI?
03 Challenges in building open datasets for AI
04 A roadmap for building open datasets for AI
05 Policy & Tech investment recommendations

14h25 UB5.230 Mozilla B.P. llm training
Currently Dataset for training are no more released
Issue with copyright

Definition of open data / public domain
Even public domain content is not always easily digitalised
Research on going

FOSDEM 2025 - The Firefox AI Platform


Example
const captioner = await pipeline('image-to-text',
'Xenova/vit-gpt2-image-captioning');
const url = 'https://example.com/cats.jpg';
const output = await captioner(url);
// [{ generated_text: 'a cat laying on a couch with another cat' }]
1. implements a set of classes per inference type
2. crawls the Hugging Face model hub
3. downloads and caches models on disk
4. runs an ONNX inference session using onnxruntime-web (wasm

14h45 firefox AI runtime

- Translation since 2019 (based on bergamot)

New goals

- Image to text
- OCR (kind of)
- Text to speech and vice versa
- Etc

Bergamot won't be enough
Transformers.js (firefox 133+)
We extensions AI API (134)
https://firefox-source-docs.mozilla.org/toolkit/components/ml/ Firefox AI Runtime

FOSDEM 2025 - The most fun you'll ever have dealing with Firefox crashes

15h00 firefox crashes
Capture crashes happening on end users with or without the users explicit the crash report sending
What happens? Immediate reload can be done and so invisible crash for the end user, prompt them to send report? Create confusion
Telemetry?

FOSDEM 2025 - What’s the (floating) Point of all these data types? A (not so) brief overview of the history and usage of datatypes within the wide world of computation


"What the heck is floating point?"
A data format for representing integers and non integers in a standard* way


For the gamers in the 2000's:
Packed RGB Floats

15h30 UB5.132 Datatype history kind of 'floating point'
Floating point: short version
Sign + Magnitude 3 Precision (fraction in magnitude)14 +3.14 (short ominous short explanation)
Medium version
Fixed point:
Base 10 how ?
Started from base 2
Binary floating point: (IEEE754 standard)
8087 support FP32 FP64 FP80
> Standard
Special type: (RGB) always positive
For memory optimization: 32bits
IEEE 754 2008 > FP16 32 64 128 256
FMA: fused multiply add, avoiding rounding too much
Brain float, FP8, …
Truncate format from FP32 to FP16, when the precision is less needed for optimisation
TF32 combine BF and FP ?