Zeitschrift: Visionen : Magazin des Vereins der Informatik Studierenden an der ETH Zürich

Herausgeber: Verein der Informatik Studierenden an der ETH Zürich

Band: - (2019)

Heft: 4

Heft

VISIONEN

www.visionen.ethz.ch

Ausgabe 04 / September 2019

First Day Of School

Magazin des Vereins der Informatik Studierenden an der ETH Zürich (VIS)

Editorial

Liebe Leserinnen, Liebe Leser,

einmal mehr darf ich zu euch sagen: Willkommen zurück! Ein neues Semester hat begonnen und solltet ihr dieses Magazin gerade zum ersten Mal lesen und neu in Zürich sein, so wartet auf euch ein Einsteiger-Artikel.

Wollt ihr so kurz nach euren Ferien noch nicht direkt zu 100 Prozent im Studium versinken, dann findet ihr im Programm der VIScon spannende Unterhaltung und Events. Wenn ihr lieber einen Abend zuhause verbringen wollt, dann schaut euch doch den hier beschriebenen Filmklassiker an, lest einen spannenden Ferienbericht oder beschäftigt euch mit einem Rätsel.

Wer mehr Zeit unter Menschen verbringen möchte, dem kann ich den Anschluss an eine der vielen VIS-Kommissionen empfehlen - in dieser Ausgabe findet ihr einen Artikel der CTF Kommission.

Ich wünsche wie immer viel Spass beim Lesen!

Sarah Kamp

Inhalt

First Day Of School

Offizielles

Random

Serien

Innovation ist ein Teil der Zühlke DNA - Deiner auch?

Wir bringen die Ideen unserer Kunden zum Fliegen – mit branchenübergreifender Business- und Technologiekompetenz und ganz viel Erfahrung. So denken wir immer wieder in neuen Bahnen und übernehmen Verantwortung für Produkte, Services und Geschäftsmodelle der digitalen Zukunft.

Als Arbeitgeber unterstützt Zühlke deinen Erfolg. Wir stehen für Teamarbeit und Wertschätzung. Passt das zu dir?
zuehlke-careers.com

zuhlkecareers

Deine Einstiegsmöglichkeiten in Zürich und Bern:

- Junior Software Engineer
- AR/VR Software Engineer
- Embedded Software Engineer

Oder für:

- Bachelor- oder Masterarbeit
- Praktikum

Zürich für Anfänger

SARAH KAMP - SCHREIBT DIESEN ARTIKEL IM AUSLAND

Ein neues Studienjahr hat begonnen und damit sind auch wieder viele Studierende aus dem Ausland hergezogen. Zürich ist zwar keine Millionenmetropole, trotzdem hat die Schweiz, insbesondere Zürich, ein paar Eigenarten, die für manch einen neu sein können. Deswegen haben wir uns in der Redaktion zusammengesetzt und präsentieren nun unsere am eigenen Leib erfahrene Zürich-für-Anfänger-Liste.

Wer unten am Hauptbahnhof ankommt, wird schnell merken, dass die Abkürzung (HB statt Hbf) nicht der einzige Unterschied ist. Generell ist das Tempo hoch und wehe dem, der auf der Rolltreppe links steht statt geht. Nicht etwa, dass man dann angemotzt würde, der Umgang bleibt hier fast immer höflich. Viel eher kommt dann von hinten ein gereiztes «Exgüsi», natürlich dennoch gefolgt von einem «Merci», denn Umgangsformen müssen sein.

Im Allgemeinen ist die Kommunikation natürlich ein schwieriges Thema für Neulinge in der Schweiz. Wer den Schweizer Dialekt erst ein oder zwei Mal gehört hat und sich dachte, den versteht man doch gut, was haben die Leute denn alle damit, der hat vermutlich Hochdeutsch mit Schweizer Akzent gehört und hielt das schon für den Dialekt. In aller Regel ist die erste Reaktion eines Deutschsprachigen auf den Dialekt nämlich «...was?» oder ähnliches. Doch keine Sorge, man gewöhnt sich schnell daran und dann sind nur noch die berüchtigten menschlichen Wasserfälle oder Bewohner ganz bestimmter Kantone (ich nenne hier keine Namen) eine Herausforderung. Bevor man sich versieht, steht man dann vor der Frage ob man sich selbst an einen Schweizer Dialekt heranwagen möchte - und natürlich an welchen.

Ein weiterer Punkt der Redaktion war die Verpflegung. Vor allem Studierende aus den benachbarten deutschsprachigen Ländern mögen es gewohnt sein, sich regelmässig beim Bäcker etwas zu holen, was in der Schweiz definitiv ins Geld geht, und auch die Grösse des Gebäcks ist dann nicht proportional zum Preis grösser, sondern eher kleiner. Das Angebot ist ebenfalls ein anderes, übrigens nicht nur beim Bäcker, sondern auch im normalen Supermarkt. Milchbrot ist hier sehr beliebt, so isst man regelmässig Butterzopf, nicht nur zu Ostern, denn man mag hier sein «süesses Zmorge». Schwarzbrot hingegen ist schwer zu finden, selbst «dunkles» Brot hat hier in aller Regel einen hohen Weizenanteil. Übrigens steht hier jeder früher oder später vor der Entscheidung, ein Migros- oder ein Coop-Kind zu sein, welches in der Schweiz die beiden grössten Supermarktketten sind, deshalb sollte man sich der möglichen Konsequenzen bewusst sein, bevor man zu Beginn die eine oder andere betritt.

Abschliessend bleibt zu sagen, dass man sich schnell und gut in Zürich einleben kann, auch wenn man wohl einige heimische Dinge vermissen wird. Manches wir einem kurios erscheinen, wie die Standardantwort auf die meisten Fragen, «Das kommt auf den Kanton an», oder der Kantönligeist, das wohl einzige was nicht auf den Kanton ankommt. Aber wem das einmal zu viel wird, dem empfehle ich ein Stück Schweizer Schokolade.


vseth
ESF 19
ERSTSEMESTRIGENFEST
CONCRETE
UNGLE
26. SEPTEMBER
20.00–03.00
ETH HÖNGGERBERG
FREE ENTRANCE FOR ERSTIS
FREE SHUTTLEBUS
DIE ULTIMATIVE
2000er
PARTY
BIG CITY LIFE
X-LIGHT & SOUND

The tale of VIScon

JOHAN STETTLER - MEMBER OF THE VISCON COMMITTEE (VC2)

"VISCONNEEECT!!!" - derived from the infamous and over-the-top enthusiastic speech by an investor of a cryptocurrency company, Carlos Matos[1] - is the most suitable word for summarizing the sheer amount of inspiration, innovation and awesomeness that surrounds the whole VIScon event. This battlecry is mostly used by the committee for spreading the hype of the VIScon experience, but the closer we get to the event itself, the more people are affected by it and join the chant. What? You have never heard of the VIScon?!? Well then my dear reader, take a seat and let me tell you a magnificent story. It all began in the dark ages when the innovator Max Schrimpf, also known as head of VIScon OK, thought "this land needs some hype". So he sought out his VIS-brethren and VIS-sistren and together they forged the foundation for the VIScon. That was around the year 1 B.V...

Well, actually, this won't be an epic underground story, where the hero prevails, despite nobody believing in him or all odds standing against him. Quite the contrary: VIScon is a result of the great engagement from its Actives[2], the reputation VIS has among companies and the D-INFK and the resources the VIS has at its disposal. Also how well the VIS committees are working together and people who are supportive and enthusiastic towards any new idea laid the ground for a crazy-sounding idea like VIScon. It is a fascinating story, a remarkable accomplishment and a very good reflection of the association itself.

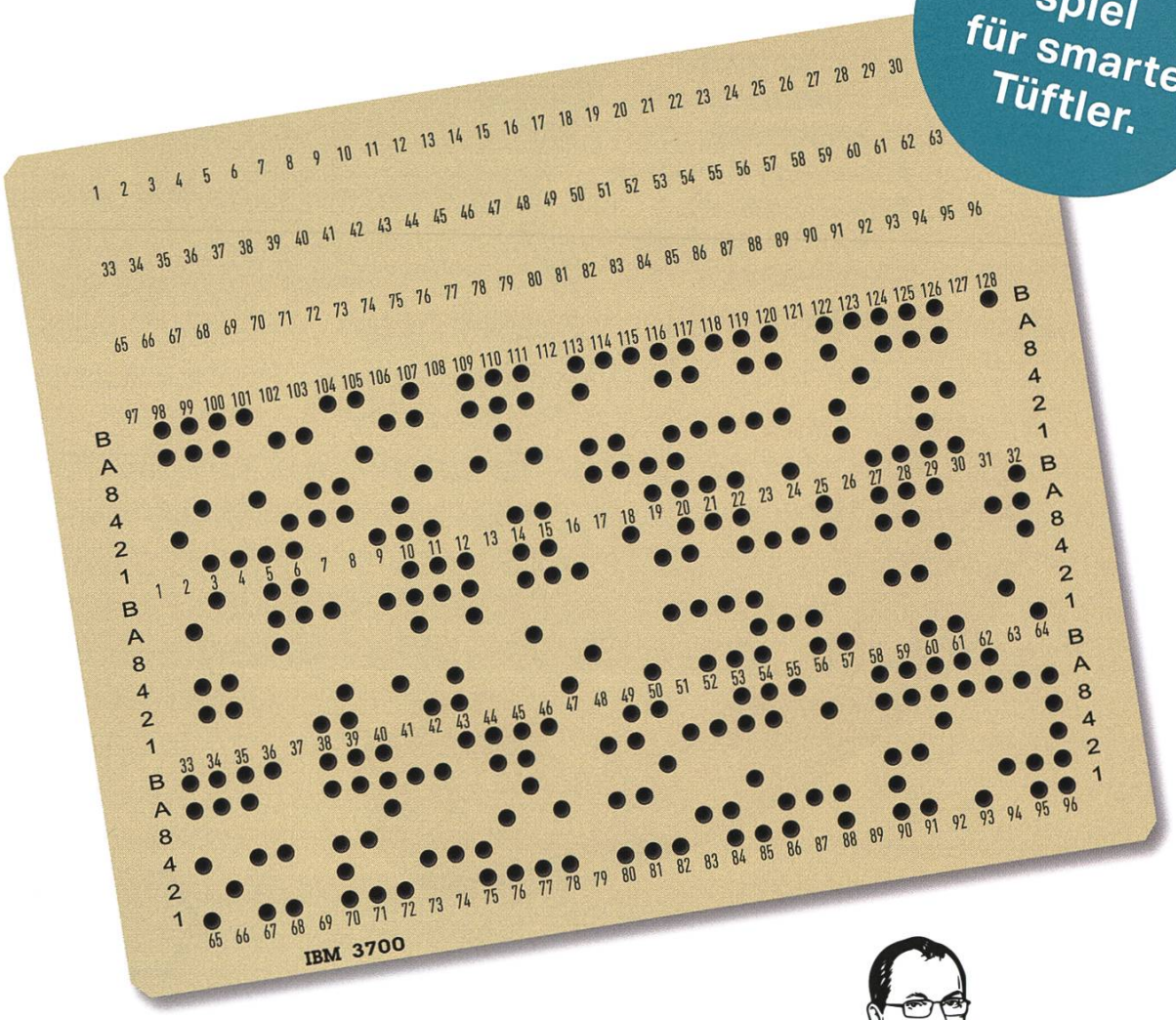
So the great legend of the VIScon begins with the greatness of the VIS. The events of the Great IT Crusade in 2017 by the Computer Infrastructure Team (CIT), taming the gruesome behemoth of VIS's IT infrastructure and its recreation, marked the beginning of a new era, where development, deployment and usage of applications became easier. In order to ensure that their legacy shall not be forgotten and future generations can still profit from this blessing, the whole manifesto was well documented. But to actually bring this new technology to the people and to pass it on, the CIT had the idea to organize a hackathon, where students develop an application using this new environment, while also acquiring lots of coding skills. While this project was in progress, the External Relations Committee (ERK) was flooded with requests from several companies asking for a personal audience with the students of the D-INFK to present their work. Understandably, their main interest in an alliance with our association is to promote their firm to students. But the VIS, thrilled by this idea, had the main goal to create a platform where the main attraction should be the research and challenges of modern computer science.

So, combine these two quests, and bang, the VIScon idea was born on the 11th of January, 2018, year 0 for future calendars. Within two months, the new organizational committee (OK) had to brainstorm and establish the concept in order to present it to the VIS board and get their approval (and by this the money) by the general assembly (MV - you should really go there!) of VIS.

➔

Let's meet.
CU at VIScon!

Gewinn-spiel für smarte Tüftler.



Rätselautor: Erwin Huber, Dipl. Informatikingenieur ETH, seit 1997 bei Ergon Informatik und Miterfinder des Airlock® Secure Access Hub, einem international erfolgreichen IT-Sicherheitsprodukt der Ergon.

Die Knacknuss

Besuche den Airlock Stand am 12. Oktober an der VIScon und teile uns deine Lösung persönlich mit. Erfolgreiche Nussknacker erhalten das patentierte Cardprotector Wallet von SECRID. Wir freuen uns auf dich.

SWISS ARBEIT GEBER AWARD
1. RANG 2018
Kategorie 250 - 999 Mitarbeitende

smart people – smart software

ergon

Teilnahmeberechtigt sind Studierende mit gültigem Ausweis. Die Gewinner können Ihre Lösung am 12. Oktober 2019 persönlich am Airlock Stand an der VIScon mitteilen. Der Rechtsweg ist ausgeschlossen.

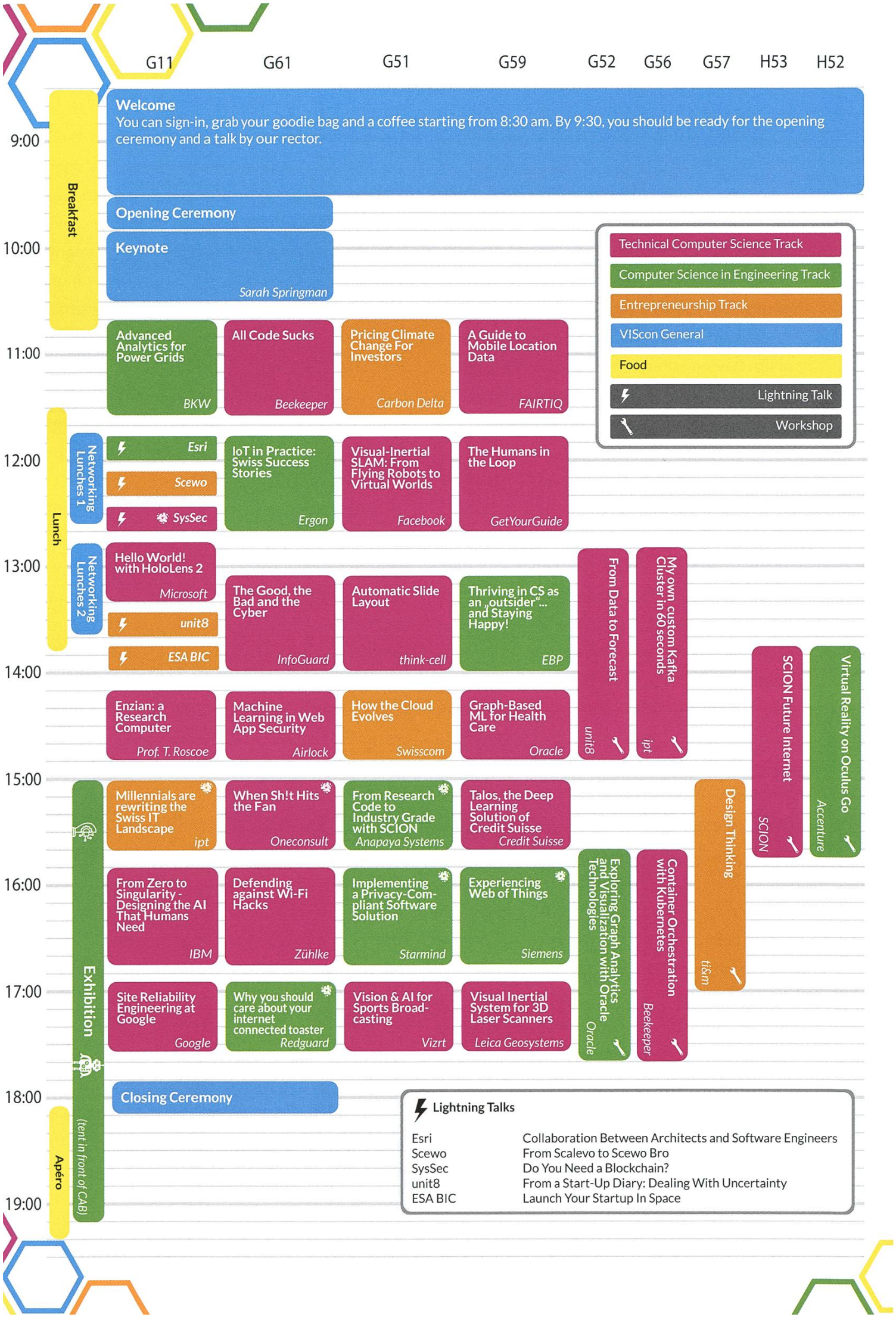
plan, organize, talk

VC2

The VIScon committee organizes a weekend packed with exciting events. On one hand there is the hackathon, where you can focus 42 hours on an idea of your choice, and on the other a symposium takes place with interesting talks and workshops from all around the IT world. Such big events need a lot of motivated volunteers - if you'd like to help make it happen, check out the VC2.

vc2@vis.ethz.ch

v i s vseth Fachverein Verband der Studierenden an der ETH


G11
G61
G51
G59
G52
G56
G57
H53
H52
9:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
Breakfast
Lunch
Exhibition
(tent in front of CAB)
Apéro
Networking Lunches 1
Networking Lunches 2
Welcome
You can sign-in, grab your goodie bag and a coffee starting from 8:30 am. By 9:30, you should be ready for the opening ceremony and a talk by our rector.
Opening Ceremony
Keynote
Sarah Springman
Technical Computer Science Track
Computer Science in Engineering Track
Entrepreneurship Track
VIScon General
Food
Lightning Talk
Workshop
Advanced Analytics for Power Grids
BKW
All Code Sucks
Beekeeper
Pricing Climate Change For Investors
Carbon Delta
A Guide to Mobile Location Data
FAIRTIQ
Esri
Scewo
SysSec
IoT in Practice: Swiss Success Stories
Ergon
Visual-Inertial SLAM: From Flying Robots to Virtual Worlds
Facebook
The Humans in the Loop
GetYourGuide
Hello World! with HoloLens 2
Microsoft
unit8
ESA BIC
The Good, the Bad and the Cyber
InfoGuard
Automatic Slide Layout
think-cell
Thriving in CS as an „outsider“... and Staying Happy!
EBP
From Data to Forecast
unit8
My own custom Kafka Cluster in 60 seconds
ipt
SCION Future Internet
SCION
Virtual Reality on Oculus Go
Accenture
Enzian: a Research Computer
Prof. T. Roscoe
Machine Learning in Web App Security
Airlock
How the Cloud Evolves
Swisscom
Graph-Based ML for Health Care
Oracle
Millennials are rewriting the Swiss IT Landscape
ipt
When Sh!t Hits the Fan
Oneconsult
From Research Code to Industry Grade with SCION
Anapaya Systems
Talos, the Deep Learning Solution of Credit Suisse
Credit Suisse
Design Thinking
ti&m
From Zero to Singularity - Designing the AI That Humans Need
IBM
Defending against Wi-Fi Hacks
Zühlke
Implementing a Privacy-Compliant Software Solution
Starmind
Experiencing Web of Things
Siemens
Exploring Graph Analytics and Visualization with Oracle Technologies
Oracle
Container Orchestration with Kubernetes
Beekeeper
Site Reliability Engineering at Google
Google
Why you should care about your internet connected toaster
Redguard
Vision & AI for Sports Broadcasting
Vizrt
Visual Inertial System for 3D Laser Scanners
Leica Geosystems
Closing Ceremony
Lightning Talks
Esri Collaboration Between Architects and Software Engineers
Scewo From Scalevo to Scewo Bro
SysSec Do You Need a Blockchain?
unit8 From a Start-Up Diary: Dealing With Uncertainty
ESA BIC Launch Your Startup In Space

But that was just the start. The following six months, they had to get all the permissions, finalize all the concepts, find sponsors and helpers, in addition to studying and eventually passing the exams. This was no easy task, given the little time for working out such a huge event from scratch. Thus, there were lots of concerns whether this was actually feasible and the fear of not having enough money due to the lack of sponsors. But as the VIScon is being held for the second time, it is clear that the first one in 2018 was a huge success. Max, who was also the head of the OK last year, commented, in the short interview I held with him, that it was certainly tough. However he is really proud and happy of what the team had accomplished and what the future holds for the VIScon. He hopes for less stress with sponsoring, packed audiences, bigger buildings and much more coffee for future generations. He is certain that the VIScon is on a good path and enjoys it very much (especially hoisting the impressive 60 square meter banner on to the CAB building, his favourite part).

As a fan myself, I might be a bit overexcited, but what really draws me to the story, is the fact that it just happened recently. I enjoy being a part of it when it is still in its early phase and experience VIS-History at first hand. It is one thing one should definitely not miss out, so come to the VIScon, we have a lot to offer.

Hundreds of students from different kingdoms from all around Switzerland pilgrimage to the VIScon to seek wisdom, even as far away as HSG or EPFL (or at least we advertised it there). Sages, sent by well-known houses, with such a great reputation, that they need not be named, share their knowledge and wisdom on modern challenges, research and projects in the arts of magic and witchcraft we know as Computer Science and Engineering. In addition to their talks, the VIScon offers workshops for the ones seeking more practice-oriented magic and also an exhibition where you can marvel at toys brought by the aforementioned houses. In any university, no matter how famous or how high its ranking is, a student only gets to see a small fraction of what computer science has to offer. The VIScon committee wants to give insight on the whole spectrum, beauty and challenges from computer science that no university can do. Therefore, the program is definitely worth checking out.

Very brave nerds attended the trial of champions, a harsh test that requires a tremendous amount of endurance, a good portion of creativity and a passion for coding. Based on ancient traditions, participants are faced with a problem that has to be solved by creating software. It is a 42-hour hackathon, a competition between teams to see who develops the finest and most creative solution to one of the tasks given by the jury. The difficulty levels go from "I can code Hello World" to "My OS is Gentoo", so the competition is for beginners and pros alike. Even I participated last year and the most sophisticated code I had ever written was a Heapsort. I contributed roughly 20 lines of code, but I gained a great insight in actual coding, acquired practical skills and had tons of fun. There was also an entire team with the same skill level as me and they had a blast for the whole weekend. They created their first real application alone and were really proud of their achievement. The challenge really lies in being creative and having endurance because you will have to perform with little to no sleep.

You are still not convinced enough to visit the VIScon? Not by the hackathon nor by the fantastic list of amazing talks and workshops? Then how about all the cool people you can get to know? I am talking about your fellow students that go to the VIScon, just to have a good time, to forge connections and friendships with people from different universities and people have the same interests as you have, to get in touch with your board members, researchers from well-known companies and some of your professors, for all the cool stories that will happen and you will be missing out on if you decide to stay at home, and of course, the free food and drinks! So what are you waiting for? Go online, register for the VIScon and hop on the hype train before all the spots are gone.

Notes:

Coming soon: VIScon reloaded, the return of the Hype. 11.10 - 13.10, save the date!

Also, it would be really cool if you register as a helper. The admission to the Symposium is free for helpers and you get more rewards the more shifts you do (see helper shifts online).

Website: viscon.vis.ethz.ch
Symposium: viscon.vis.ethz.ch/symposium
Hackathon: viscon.vis.ethz.ch/hackathon
Subscribe to the newsletter

Links:

[1] https://www.coinkurier.de/carlos-matos-der-mensch-hinter-der-bitconnect-meme/

[2] Members of committees doing active work for the VIS

A year of backdoors, exploits and pwning

LEONARDO GALLI - STILL AT 0 ZERO-DAYS

I was very eager to join VIS's hacking group flagbot (the CTF Committee). I had no inital experience with CTF and could barely read assembly code. After a few tutorial challenges, I was thrown into cold water as we participated in various online hacking competitions, including DEF CON qualifiers and an attack-and-defense CTF. What follows are highlights of the past year from flagbot.

Baby Steps

It all started with my first CTF meeting: I was eagerly wanting to learn "hacking stuff" and become the very best when I was given my first CTF task: Baby ROP. I had no clue what "CTF" or "ROP" was, so Jonas (the current CTF president) gave a small introduction to CTF: CTF, an abbreviation of *Capture the Flag*, is a sport which consists of solving computer science (hacking) challenges. A competition usually consists of many challenges and for every solved challenge you get a flag as proof of solving it. This flag can be redeemed for points, and the team with the most points wins the competition. These challenges are grouped into five major categories: pwnables, reversing, web, crypto and misc.

Pwnables are challenges where most of the time you are given a small application (e.g. a Linux program) and you have to get remote code execution by finding and exploiting a vulnerability in it. Because you do not necessarily get the original source code, you have to use a disassembler to extract the CPU instructions from it. With the help of a decompiler, we can turn the CPU instructions into a format that (hopefully) resembles the original source code. (Pictured is a challenge open inside IDA, a disassembler and decompiler.)

Reversing challenges are very similar to pwnables, but the focus lies more on understanding what the program *exactly* does. An example is a key generator, where you have to

find a valid key to make the program accept it.

As the name implies, web challenges are mostly web services that are vulnerable to some kind of attack.

Crypto, short for cryptography, mostly consists of finding weaknesses or published research for implementations of certain protocols and then exploiting those.

The last - and often weirdest category - *misc*, focuses on all kind of different things, from scavenger hunts to steganography and more.

With this new knowledge, I finally got to try my hand at hacking a simple application. The first challenge was getting the application to run, all while the "Baby" in the name was mocking me. With some help, I got the application running and I immediately found a way to crash it (which is good). *Hurray!* Following some more trial and error, I triumphiantly got my first exploit working. I was hooked and started solving more and more old challenges, excitedly waiting for the next CTF event.

Can you even cat?

My first CTF was the TUCTF, an online CTF, meaning anyone could participate from anywhere. As always, we met in our CTF room (CAB H52) and started hacking. The CTF had already started a day prior, which meant we had to catch up with teams that started earlier. Most of the binary challenges were quickly pwned, leaving us with the two most dreaded categories: misc and web.

The two remaining misc challenges were both related to DOS (Microsoft Disk Operating System) which made them super annoying to solve: They where both text-based adventures where you had to solve some kind of puzzle to get the flag. After a lot of trial and error, we managed to find the flag for the - supposedly - harder one by just sending random Unix commands. We then further broke it in an unintended way by sending a Ctrl-C (an interrupt signal), making the program spew error messages we weren't supposed to see, and using this knowledge, we even managed to get code execution.

Back to the 'easier' one, where we got the following hint: `what do witches usually have?` Because witches usually have cats, we tried all possible variations of `cat flag` (which on linux prints the file `flag`). At the end, it turned out to be `cat flag.txt`. How I hate random blackbox challenges.

We quickly solved all the remaining web challenges but one (which also turned out to be a random blackbox challenge).

Nonetheless, it was a lot of fun and, even though we started a day late, we came in on place 37 out of 764.

3 bytes and even less hours of sleep

The next CTF was Insomni'hack in Geneva, where we had to travel to. Up until this year, the CTF committee did not have a travel budget, as we can usually play online. So our journey began with requesting for a travel budget at the VIS general assembly.

So we travelled to Geneva, did some ightseeing and went to the convention center, where the CTF was held. The CTF was played over night, from 18:00 to 04:00, so we brought tons of caffeinated drinks to keep urselves awake.

During the CTF, I tried to solve the challenge called '3bytes'. Opening the 3bytes binary with my favourite decompiler, it turned out to not contain much code. True to its name, the binary allowed you to write three arbitrary bytes wherever you chose. It even helpfully included ➔

the location of the libc as well as a Docker container for the challenge. However, all addresses were randomized, so we couldn't, for instance, overwrite the address of `exit()` with something we controlled. We were pretty clueless and came back constantly during the CTF trying new approaches, stepping through everything in the libc and researching similar challenges, but we found nothing. That is, until the very end of the CTF, when Yves managed to find a similar challenge that was 6 months old. But it was too late, since modifying the exploit was not trivial and ould have taken a lot of time. Still I had a lot of fun and I tried solving some web challenges as well. Meanwhile, our other teammates managed to solve one challenge by just

sending random shell commands. Furthermore, we managed to be the first team to solve the exploit quest challenge, a fun scavenger hunt around the convention center.

In the end, we beat all other schools that participated (including the EPFL team ;)) and placed 9th. (Pictured is the exhausted flagbot team at the award ceremony at 4am). Given that some of the best teams around the world were participating, we were pretty satisfied with that outcome. Even more so when we received our prizes for being the best school team. However, all of it came in a big cheap cardboard box with no carrying handles. Since we were close to the airport, we borrowed a luggage cart and used that to carry it around (see Jonas exhausted after 10 hours of CTF and now having to carry a

big cardboard box). Of course not everything was perfect, our train back (at 5 am) was cancelled and we had to wait even longer to be able to finally try to get some sleep.

Russia still uses Windows XP?

After coming home from Geneva and finally getting some sleep, I was sure of one thing: I needed more practice. While solving challenges of old CTFs is always a good exercise, participating in more CTFs would help even more, especially with time management, something often underrated for CTFs.

So we started by participating in a Russian CTF called TyumenCTF. Even though we were ➔

AdNovum

Go2market App

Ready for a challenge? Sign up now!

16. Oktober 2019

17.30 Welcome

17.45 Workshop: Conceptualize an App

19.00 Apéro: Bier & Snacks mit AdNovum Team

Wo? AdNovum Informatik AG, Röntgenstrasse 16, Zürich

Mach bei diesem praxisorientierten Case mit, löse knifflige Architektur-fragen im Team und analysiere die Anforderungen an die App für Financial Services! Im Anschluss offeriert dir AdNovum kulinarische Leckereien und erfrischendes Bier.

Melde dich an unter vis.ethz.ch

adnovum.ch

VIS

warned at the registration that the CTF would be Windows XP-themed, I was not prepared for their website: a completely normal-looking - besides the weird folders - looking XP desktop.

Luckily for us, though, the challenges were still all Linux-based and most pwnables even came with the source code! Although I worked remotely, I was still able to solve some challenges and help our team secure the 6th place.

Lots of MOVs and a first place

Between TyumenCTF and other events we also participated in SwampCTF. We didn't really start solving challenges after a good few hours past the start and hence had a lot of catching up to do. But once we tasted flags, we powered through a lot of the challenges.

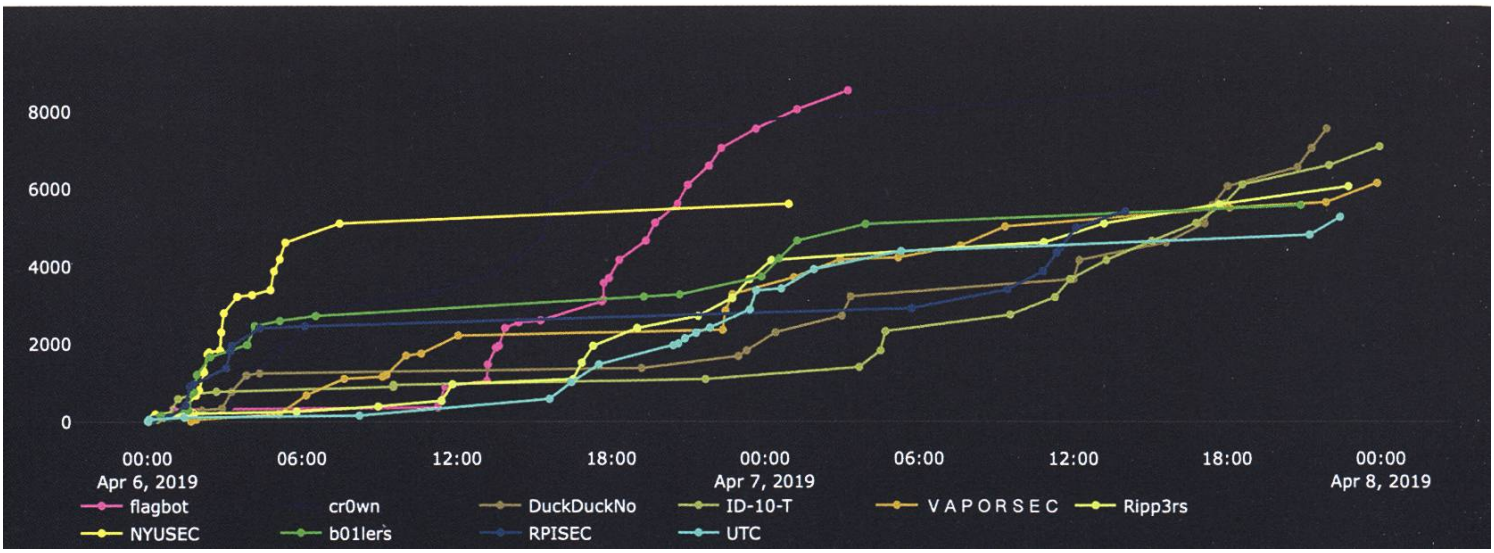
An interesting challenge was called "future fun". It was a 10Mb binary that needed some input and was tagged as reversing. I opened it in IDA, not expecting much and was greeted by a very long loading time. Once IDA had finally loaded the binary, it complained a lot about missing stuff. I looked closely at the disassembly and only saw `MOV` instructions. At that point I gave up, but my teammates mentioned a compiler called `movfuscator`: A compiler that outputs only MOV instructions, as MOV is Touring complete.

Things started to slow down though (pictured), when we completed almost all challenges. It was also getting late, so most of us decided to go home and try our luck the next day. But then suddenly we only had one challenge left and - even though we were first place now - I knew we had to try to solve it as fast as possible. We worked hard and eventually - at 3 AM - we got the final flag of the CTF and won!

This was an amazing experience and would not have been possible without my incredible teammates. I learned a lot during this CTF and I hope we will win again next year :)

Stealing exploits is fun, COBOL is not...

To end the year on a high note we participated in the FaustCTF, an attack-and-defense CTF: Every team gets a server with vulnerable applications. The goal is to patch your own server, while simultaneously exploiting the applications running on the servers of all the other



teams. This time, researching beforehand payed off immensely. We found a tool named flower, that can ingest network traffic dumps and not only filter out traffic stealing our flags, but also create exploit scripts we can use from that traffic.

Backing up a bit, we arrived at CAB and eagerly awaited the download and decryption of our VM so we can start exploiting and patching. We hosted our sever on Google cloud and the first complication was getting the application code onto our local machines. After that hurdle was overcome, we could finally start finding exploits. A harmless looking web service named punchy caught my eye. It was written in Python, but also contained native libraries that were called. Upon opening the native libraries in IDA, I was confused. It seemed like the native libraries were writing code to a file, then calling COBOL to compile said file and then executing the compiled binary. I feared I would have to learn COBOL to be able to make an exploit. But after looking at the web interface, it turned out it was even worse: The only thing one could do, was upload punch cards with COBOL code that was then processed by the service and converted to code. I still had hope that there was another exploit somewhere, but when checking flower for what traffic the game server sent (to store the flag), it was clear I had to somehow write COBOL code onto punch cards.

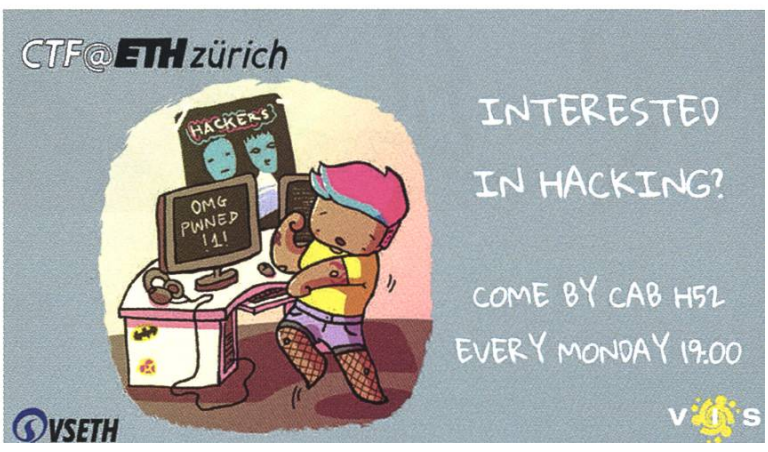
While I struggled with punchy, we were already under attack on a different service. Although we already knew how to pwn it, our exploit was somehow failing. Thanks to flower however, we were able to just copy the exploit that exploited us and use it as our own. This pattern was visible throughout the whole CTF. Once other people got their punch cards to work, I gave up and just used flower to copy their images. We even managed to copy an exploit, for which we still have no idea how it works. Even better, one of our applications - which nobody took a look at - was getting exploited. But somehow we were gaining points for that service, instead of loosing them? Turns out, one team decided to have some fun and started exploiting that service on all teams servers. Instead of using the exploit normally, they submitted flags for other teams, meaning we were gaining points instead.

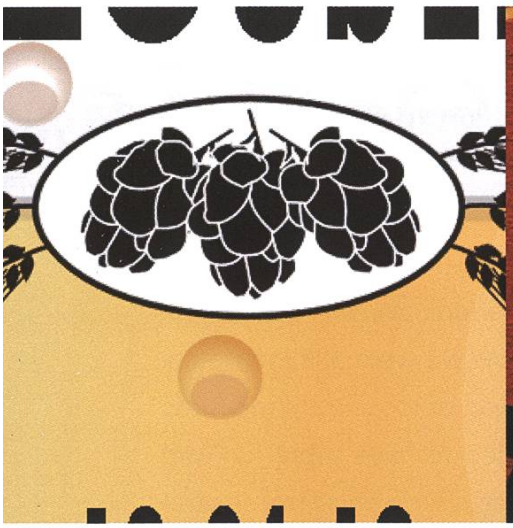
Two hours before the CTF was over, we noticed some suspicious sh sessions (a shell). To combat attackers, [redacted] decided to kill all sh sessions. However, not only did he run that in the host on Google cloud (instead of the VM being attacked), he also ran it in a loop. Immediately all of us were kicked out and we had to hard reset the server. Nevertheless, we still managed to secure a good place.

All in all, while it was a very hectic CTF, I had a lot of fun and flower was unbeatable.

We want you for flagbot!

If any of this sounded interesting to you, we are always looking for new members. We have meetings on Monday from 19:00 at CAB H52 and everyone is welcome. Just drop by and someone will help you get started.



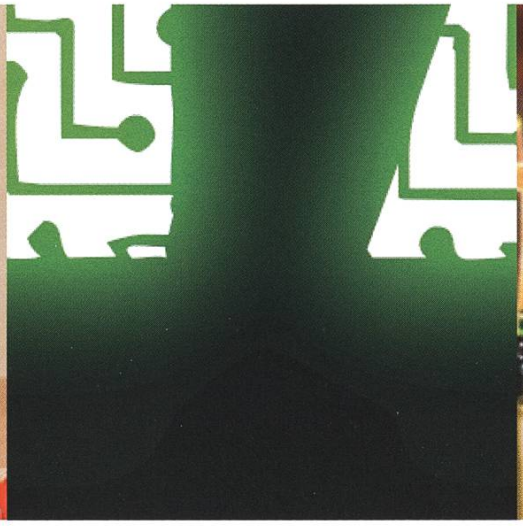


Event 1

Event 2

Event 3

Event 4



Event 5

Event 6

Event 7

Event 8

Event 9

Poster-Riddle

JOHAN STETTLER - MEME NOVICE LEVEL 7

I really like reading the Visionen. The articles are really interesting, sometimes heartwarming and sometimes the distraction I need when I am sunk in a tedious study session. But my absolute favourite part about such magazines are the riddlesections. I just love them, whether it is a Pokemon riddle, a puzzle or a funny crossword. They are especially good when they involve some sort of personal connection, for example, when the riddle is about my favourite TV-show, or about people I know. Naturally, I wanted to create a riddle by myself just for you, the VIS reader.

The Design-Committee has very talented people and we all appreciate their fantastic work. They always make wonderful posters for every event the VIS has and now, I want to know, how many you can recognize. You are faced with a snippet of a DesKo poster and you have to guess the event it was made for. Have fun and shout out for the DesKo team!

Von Mäusenieren und unbesuchbaren Walen

TOBIAS SCHEITHAUSER - SUCHTE IN DEN USA NACH ALTEN ZELLEN IN JUNGEN NIEREN

Seit mehreren Stunden sind wir jetzt im Auto auf der Straße und sehen gerade noch die letzten Sonnenstrahlen. Immer wieder entdecken wir tote Tiere am Rand der Straße im Scheinwerferlicht. "Roadkill". Was in meiner Vorstellung ein überfahrener Igel oder ein Frosch ist, sind hier deutlich größere Tiere. So richtig erkennen kann ich nicht, was es ist, nur dass es schrecklich viel ist.

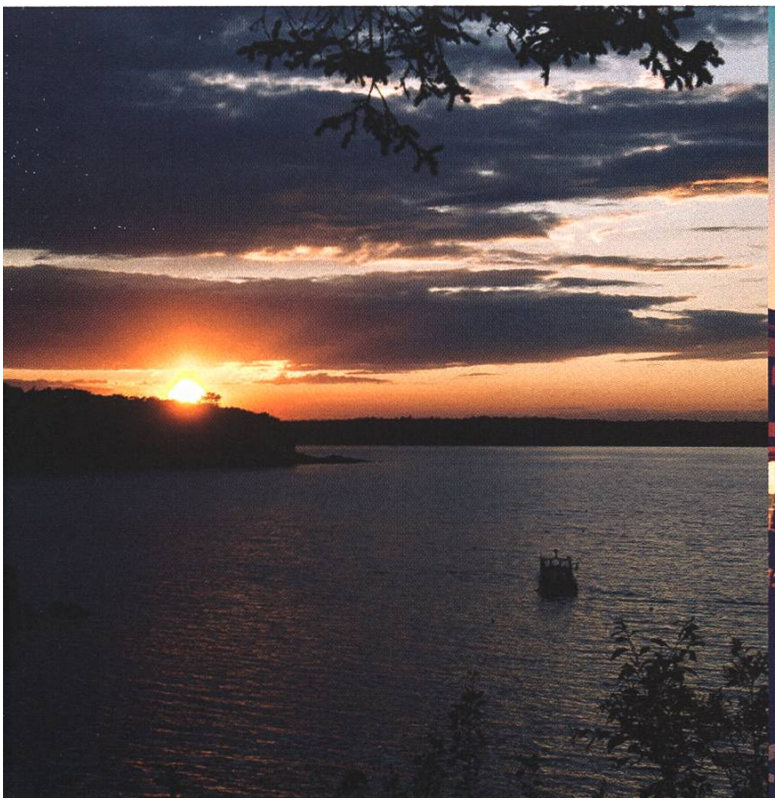
Müde bin ich auch noch. Losgefahren in Zürich um 7 Uhr morgens, bin ich jetzt seit 20 Stunden unterwegs und das Navi zeigt an, dass wir noch zwei weitere Stunden brauchen werden, bis wir auf Mount Desert Island ankommen. Der Name klingt genauso abgelegen, wie es der Ort ist. Für mich als jemanden, der immer in einer Großstadt gelebt hat, werden die kommenden sechs Wochen ein ganz anderes Erlebnis sein. Ich bin zum ersten Mal in meinem Leben in den USA. Nachdem wir an einer scheinbar unendlichen Menge an kleinen Freikirchen, und noch mehr Hotels und Motels vorbeigefahren sind, kommen wir schließlich an.

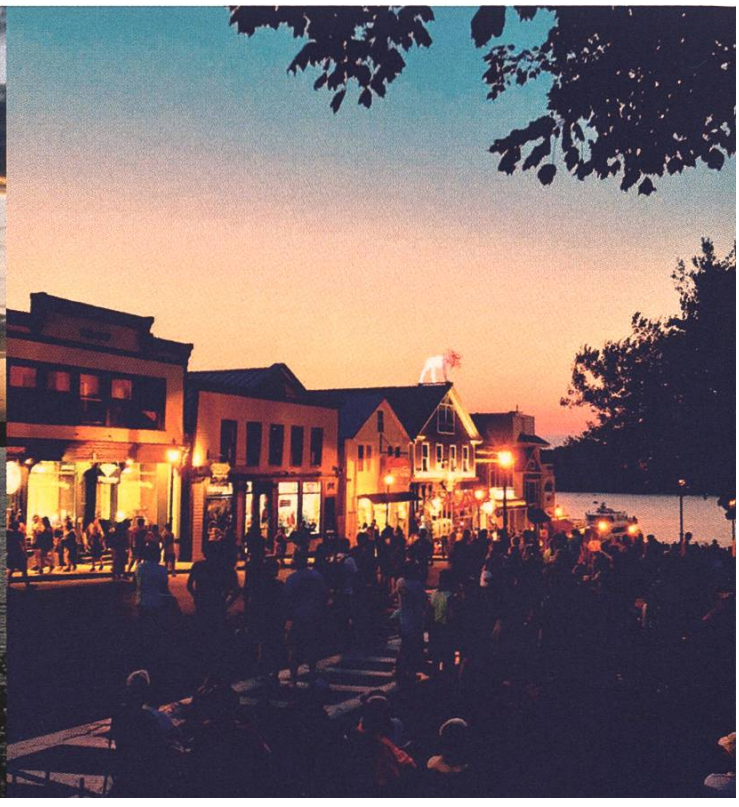
Hier in Maine, dem östlichsten Bundesstaat der USA, findet man nach einer kurzen Suche auf der Karte, die, nach Long Island, mit 280km² zweitgrößte Insel vor der Ostküste der USA. Mount Desert Island. Bekannt ist die Insel für den Acadia Nationalpark und den Cadillac Mountain, den Ort in den Vereinigten Staaten, den die Strahlen der aufgehenden Sonne als Erstes treffen[1]. Auf dieser Insel befinden sich auch zwei biomedizinische Forschungslabore, das Jackson Laboratory[2] und das Mount Desert Island Biological Laboratory (MDIBL)[3]. Gelegen direkt am Wasser, aufgeteilt in viele kleinere Holzhütten, ein modernes Schulungsgebäude und ein großes Hauptgebäude, ist das MDIBL der Ort, and dem ich im Sommer für sechs Wochen ein Praktikum machen durfte. Als Teil einer deutschen Gruppe von Nephrologen hatte ich so die Möglichkeit der Lernphase zu entkommen und im "Visiting Scientist Program" dort praktisch zu arbeiten und zu forschen.

Während meines Praktikums habe ich mich mit sogenannten seneszenten Zellen in Nieren beschäftigt. Das sind Zellen, die sich nicht mehr teilen, was hauptsächlich durch Alterung auftritt. In der Niere hat dieses Phänomen eine besondere Bedeutung, da mit der zellulären Seneszenz die Effizienz und Regenerations- →

fähigkeit der Niere nachlässt. Bei Transplantationen kann es zu stressinduzierter Seneszenz kommen, die die Verheilung und damit auch den Erfolg der Transplantation zusätzlich beeinflussen kann. Meine Aufgabe war es nun aus Datensätzen, die bereits in aufwändiger Laborarbeit mit Mäusen erstellt wurden, unter Zuhilfenahme öffentlicher Daten neue Erkenntnisse über die Expression bestimmter Gene zu gewinnen. Zudem stellte sich die Frage, ob sich diese Genexpressionsmuster aus Modellversuchen auch in normaler Alterung wiederfinden. Mithilfe von R und weiterer open-source Software konnte ich manche Fragen beantworten, doch es kamen jederzeit neue auf, sodass ich auch jetzt noch weiterhin an dem Projekt arbeiten werde.

Natürlich war auch etwas Zeit übrig, den Naionalpark mit dem Rad, Kajak und beim Wandern zu erkunden. Dafür musste dann nur das Wetter mitspielen, was nicht zwingend der Fall war. So habe ich teils gefroren oder wurde vom Regen pflotschnass, während man in Europa fast geschmolzen ist. Dreimal haben wir versucht zu einer Whale-watching-tour zu kommen, doch bis zur Abreise war uns dies nicht vergönnt. Durch die interessante Arbeit und die wunderschöne Natur blieb natürlich eines auf der Strecke: das Lernen für die Klausuren. Nach sechs Wochen Pause bin ich nun also eifrig am Lernen und muss feststellen, dass man in solch einer Zeit auch einiges wieder vergessen kann, wenn man sich nicht damit beschäftigt. Insgesamt sehe ich das Praktikum als wundervolle Erfahrung an und kann jedem nur empfehlen, eine solche Chance wahrzunehmen, wenn sie sich bietet. Gerade im Sommer gibt es dafür eigentlich genügend Zeit und der Austausch mit anderen Menschen aus der ganzen Welt und der nicht nur fachliche Erfahrungsgewinn sind den (nur wenigen) ➔





„Unsere Softwarelösungen setzen neue Standards in der Sensorik."

Eduard Rudi,
Software Engineer

„Become part of the Sensirion success story". Wollen Sie Ihrer Karriere den entscheidenden Kick geben und sich neuen Herausforderung stellen? Dann heissen wir Sie herzlich willkommen bei Sensirion.

Sensirion steht für Hightech, Innovation und Spitzenleistungen. Wir sind der international führende Hersteller von hochwertigen Sensor- und Softwarelösungen zur Messung und Steuerung von Feuchte, Gas- und Flüssigkeitsdurchflüssen. Unsere Sensoren werden weltweit millionenfach in der Automobilindustrie, der Medizintechnik und der Konsumgüterindustrie eingesetzt und tragen zur stetigen Verbesserung von Gesundheit, Komfort und Energieeffizienz bei. Mit unserer Sensorik liefern wir damit einen aktiven Beitrag an eine smarte und moderne Welt.

Schreiben Sie Ihre eigenen Kapitel der Sensirion Erfolgsgeschichte und übernehmen Sie Verantwortung in internationalen Projekten. Stimmen Sie sich auf www.sensirion.com/jobs auf eine vielversprechende Zukunft ein.

www.sensirion.com/jobs

SENSIRION
THE SENSOR COMPANY

zusätzlichen Stress beim Lernen definitiv Wert! Bedanken möchte ich mich bei Prof. Dr. Dr. Anette Melk aus der Abteilung für Päd. Nieren-, Leber- und Stoffwechselerkrankungen der Medizinischen Hochschule Hannover, die mir das Praktikum ermöglichte und in mir die Begeisterung für dieses Thema weckte. 

Links:

[1] https://de.wikipedia.org/wiki/Mount_Desert_Island

[2] https://www.jax.org

[3] https://mdibl.org

[4] https://www.ncbi.nlm.nih.gov

[5] https://galaxyproject.org

[6] https://usegalaxy.eu

[7] http://www.webgestalt.org

[8] https://training.galaxyproject.org

[9] https://www.biostars.org

[10] schetobi@student.ethz.ch

P.S.

Jeden Tag war ich davon begeistert, wie einfach es auch für Leute sein kann, die noch nie mit solchen Daten gearbeitet haben, in das Thema einzusteigen. Die Webseite des National Center for Biotechnology Information (NCBI)[4] bietet wohl die größte Sammlung von (Roh-)Daten. Diese können dann sehr einfach in das Online-Tool Galaxy ([5], [6]) geladen und dort analysiert werden. Zum Schluss bietet eine Reihe weiterer Webseiten Tools an, die dabei helfen Erkenntnisse aus den Daten in die Biologie einzuordnen; ein Beispiel hierfür ist WebGestalt[7]. Gute Tutorials für Galaxy finden sich im Galaxy Training Network[8] und bei Fragen bietet das Biostars Forum[9] eine gute Plattform für Fragen von Einsteigern und Experten auf dem Gebiet. Falls ich euer Interesse geweckt habe, könnt ihr mich gerne ansprechen oder anschreiben[10]. Ich würde mich auch sehr freuen davon zu hören, wenn ich jemanden von euch dazu gebracht habe, sich einen Datensatz oder eine Fragestellung mal anzusehen.

Bildnachweis dieser Ausgabe

Sofern nicht anders vermekt, wurden die Bilder und Grafiken dieser Ausgabe durch die jeweiligen Autoren oder den VIS zur Verfügung gestellt.

Cover:

- https://www.pexels.com/photo/boy-looking-on-a-tidied-desk-2781814/

PRAKTIKUM

SYSTEMSOFTWARE-ENTWICKLUNG

PDF-TOOLS.COM
Premium PDF Technology

PERSPEKTIVE

informieren -
kontaktieren

www.pdf-tools.com/eth

FÜR DENKER, MACHER, INNOVATOREN UND TEAMWORKER

PDF Tools AG bietet Studenten (ETH, Uni) mit der Fachrichtung Elektrotechnik oder Informatik die Gelegenheit ein Praktikum „mittendrin" zu absolvieren.

PDF Tools AG • Kasernenstrasse 1 • 8184 Bachenbülach • praktikum@pdf-tools.com • www.pdf-tools.com

Filmklassiker #2 - 2001: A Space Odyssey

MARCEL - WILL TÄGLICH ZU "ALSO SPRACH ZARATHUSTRA" AUFWACHEN

Nachdem ich das letzte Mal auf einen der beliebtesten Klassiker von F. Coppola eingegangen bin, will ich mit einem Film weiterfahren, der mir erstmals klar gemacht hat, dass es auch Filme gibt, die sich stark von den üblichen Blockbustern unterscheiden.

Ich spreche natürlich von "2001: A Space Odyssey", der 1968 erschienen ist. Der Regisseur von 2001, Stanley Kubrick, ist ein absoluter Meister seines Faches; er war bekannt für seinen übertriebenen Perfektionismus - und dies merkt man seinen Werken auch an. In seinem Horror-Klassiker The Shining (1980) liess er gewisse Szenen über 200 Mal filmen, bis er mit dem Resultat zufrieden war! Sein Stil zeichnet sich oftmals durch wahnsinnig symmetrische Szenenbilder aus, seine früheren Werke (Dr. Strangelove (1964), Lolita (1962)) triefen ausserdem vor Ironie. Genau wie F. Coppola gehörte er zu der New-Hollywood-Bewegung, der viele Junge angehörten, die von den ewig gleichen Produktionen der grossen Filmstudios gelangweilt waren.

Worum geht es? Es ist fast nicht möglich, die Handlung vollständig und einfach zu erklären. Der Film spielt in 3 Teilen - er beginnt beim "Dawning of Man", also einige Jahre vor der Steinzeit, und endet in einer nahen Zukunft (der Film spielt, wie im Titel schon klar wird, im Jahr 2001). In allen Teilen geht es um grosse Entwicklungen der Menschheit: Das Finden von (primitiven) Werkzeugen und Waffen ermöglicht es mehrere Tausend Jahre später, Expeditionen auf den Mond zu unternehmen und einige Jahrzehnte später, noch weiter in das Sonnensystem vorzustossen. Ein fremdartiges, ausserirdisches Objekt scheint dabei grossen Einfluss auf die Menschheit zu haben - in verschiedener Art und zu verschiedenen Zeitpunkten.

Es geht unter anderem primär um die Entwicklung der Menschheit. Müsste man ein zentrales Thema bestimmen, wäre es wohl die Evolution. Weiter kommt auch ein Konflikt mit einer AI vor; spannenderweise werden Parallelen gezogen, von der ausser Kontrolle geratenen künstlichen Intelligenz zu Darwins Theorien. Alles in allem kann es gut sein, dass man der Handlung nicht viel abgewinnt, ohne intensiv zu recherchieren - es wurden ganze Doktorarbeiten geschrieben, die sich mit dem Film befassen. Man wird jedoch schnell im Internet fündig, wenn man sich näher mit möglichen Interpretationen auseinandersetzen will.

Doch auch wenn man wenig Interesse an den philosophischen Fragen hat oder Sci-Fi nicht wirklich mag - alleine wegen des technischen Aspekts ist der Film ein Muss. Das sehr breite Bildformat weiss Stanley Kubrick gut zu nutzen - er erschuf Szenen, die man fast schon als Fotographien an Kunstausstellungen sehen könnte. Im letzen Teil kommen spektakuläre visuelle Effekte vor, und das ganz ohne CGI. Einer der besten Cuts der Filmgeschichte ist der Übergang vom ersten zum zweiten Teil, der einen staunend vor dem Bildschirm sitzen lässt. Nicht

zuletzt ist auch die Verwendung von der Musik und diversen Klängen erwähnenswert. Auch wenn man nicht darauf achtet, so hat alleine die Abwesenheit von Ton in gewissen Szenen einen extrem bedrückenden Effekt.

Zugegeben, "2001: A Space Odyssey" mag nicht der zugänglichste Film sein; ich hätte hier andere Werke Kubricks nennen können, die etwas 'normaler' sind. Aber, wie ich bereits erwähnt habe, hatte ich einen Aha-Moment als ich ihn das erste mal gesehen habe - was mich veranlasst hat, mehr über Filmkunst wissen zu wollen. Ich glaube aber, das wichtigste ist, dass man nicht mit einem entspannten Popcorn-Streifen rechnet - man sollte in der richtigen Stimmung sein, auch etwas handlungsärmere Strecken durchzustehen und sich auf die philosophischen Themen einzulassen. Meiner Meinung nach lohnt sich das aber auf jeden Fall.

Da ich ein absoluter Fan von Kubrick bin, würde ich fast ausnahmslos alle seine Werke empfehlen; ich hätte beinahe über "A Clockwork Orange" (1971) geschrieben (mein persönlicher Favorit, der aber ziemlich brutal ist). Der bereits erwähnte "Dr. Strangelove" ist eine Komödie über den kalten Krieg. Kubricks wohl bekanntester Film ist "Full Metal Jacket" (1987), ein Antikriegsfilm über den Vietnamkrieg (und insbesondere im ersten Teil über die brutale Ausbildung zum Soldaten). Der Drill Instructor (gespielt von Ronald Lee Ermey) hat seine Rolle fast vollständig improvisiert und spielt sagenhaft. Und für alle Horrorfans lohnt sich auch "The Shining", in dem Jack Nicholson's Figur zur Bedrohung für seine Familie wird, als dieser eine Stelle als Hausmeister in einem abgelegenen Hotel annimmt. Ein Ausschnitt in "Ready Player One" (2018) von Spielberg ist eine Hommage an eine bekannten Szene daraus.

Sollte dir 2001 gefallen haben, wirst du wahrscheinlich auch andere Sci-Fi Klassiker mögen, unter anderem "Blade Runner" (1982) mit Harrison Ford. Auch der originale "Alien" (1979) von Ridley Scott, so wie dessen Fortsetzung "Aliens" (1986) sind für Thriller/Horrorfans sehenswert. Leider kennt man von "Planet of the Apes" (1968) nur noch den Reboot, dabei legte der erste Teil das Fundament für 3 Fortsetzungen und die neuen Filme. Sehr unterhaltsame und spannende Filme sind "Back To The Future" (1985) und "Terminator" (1984) sowie dessen Fortsetzung "Terminator 2" (1991). Schliesslich gab es auch in den letzten Jahren unzählige Beispiele guter Sci-Fi; viel zu wenig bekannt ist dabei leider unter anderem "Children Of Men" (2006), der definitiv viel mehr Beachtung verdient (alleine wegen seines wahnsinnigen Endes). 

Never Heard of It #23

BALZ GUENAT - THE RETURN OF THE MASTER

Nicole has kindly invited me for a short comeback to this column and I gladly accepted. I could not miss the opportunity to present to you...

King Gizzard & The Lizard Wizard - Infest The Rats' Nest

Infest The Rats' Nest is already the second album *King Ichor & The War Boar* have released this year after *Fishing For Fishies* and while these albums contain some similar themes, they deliver them with vastly different sounds.

The opening track *Planet B* sets both the tone and theme of this album that is a warning and a call to action.

"Open your eyes and see / There is no Planet B" are the words sung over unapologetic thrash metal guitars and drums.

The first song is the starting gun for the race towards the apocalypse that is the rest of the album.

Across nine tracks and 34 minutes, *King Nightmare & The Bear Lair* give the thrash treatment to the issues that endanger humanity's current lavish lifestyle:

Overuse of Earth's resources, financial disparity, the meat production industry, antibiotic resistance, climate change, and finally our naive hope for space colonialization to save use from ourselves.

But don't mistake *Infest The Rats' Nest* for a boring lecture or political piece!

This album is not *An Inconvenient Truth*.

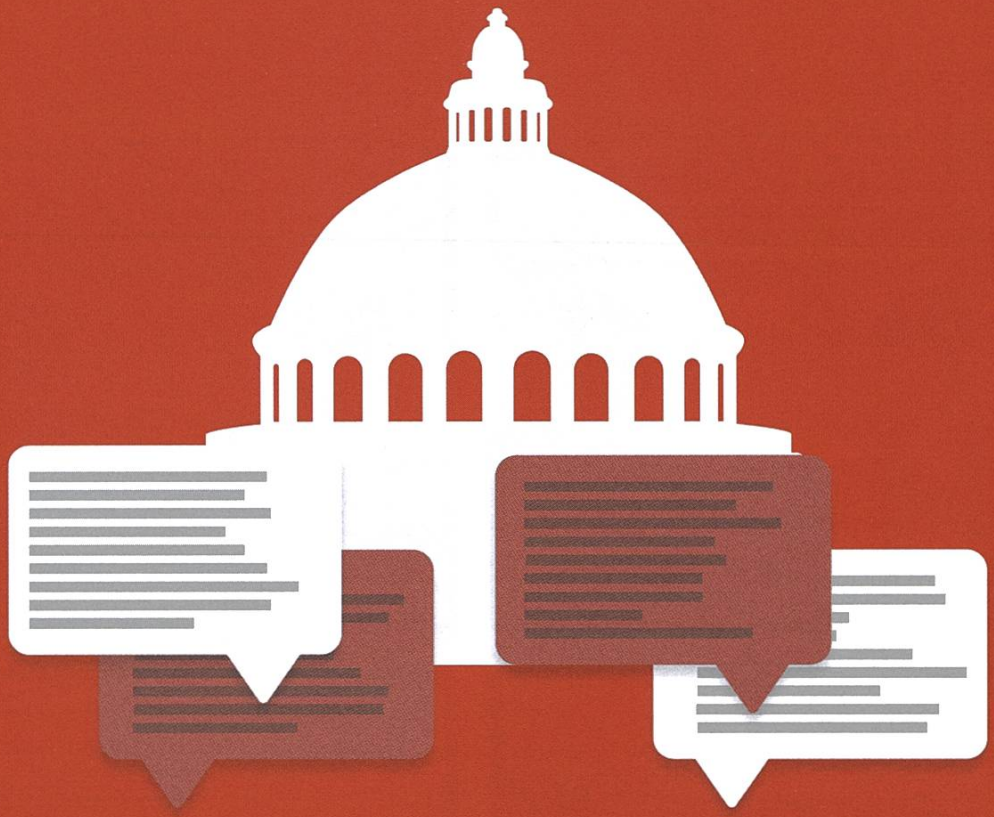
This album is *Mad Max*!

A blazing trip to hell!

As we burn through Earth's pantry and slowly make it hell for ourselves, we go down the track list towards the final track *Hell* with *King Egress & The Chess Mess* singing about humanity's descent into the hell that is the venusian atmosphere.

I think we would all do good to not only listen, but *listen* to this thunderstorm of an album by *King Rick & The Chick Flik*.

represent, discuss, change



HoPo

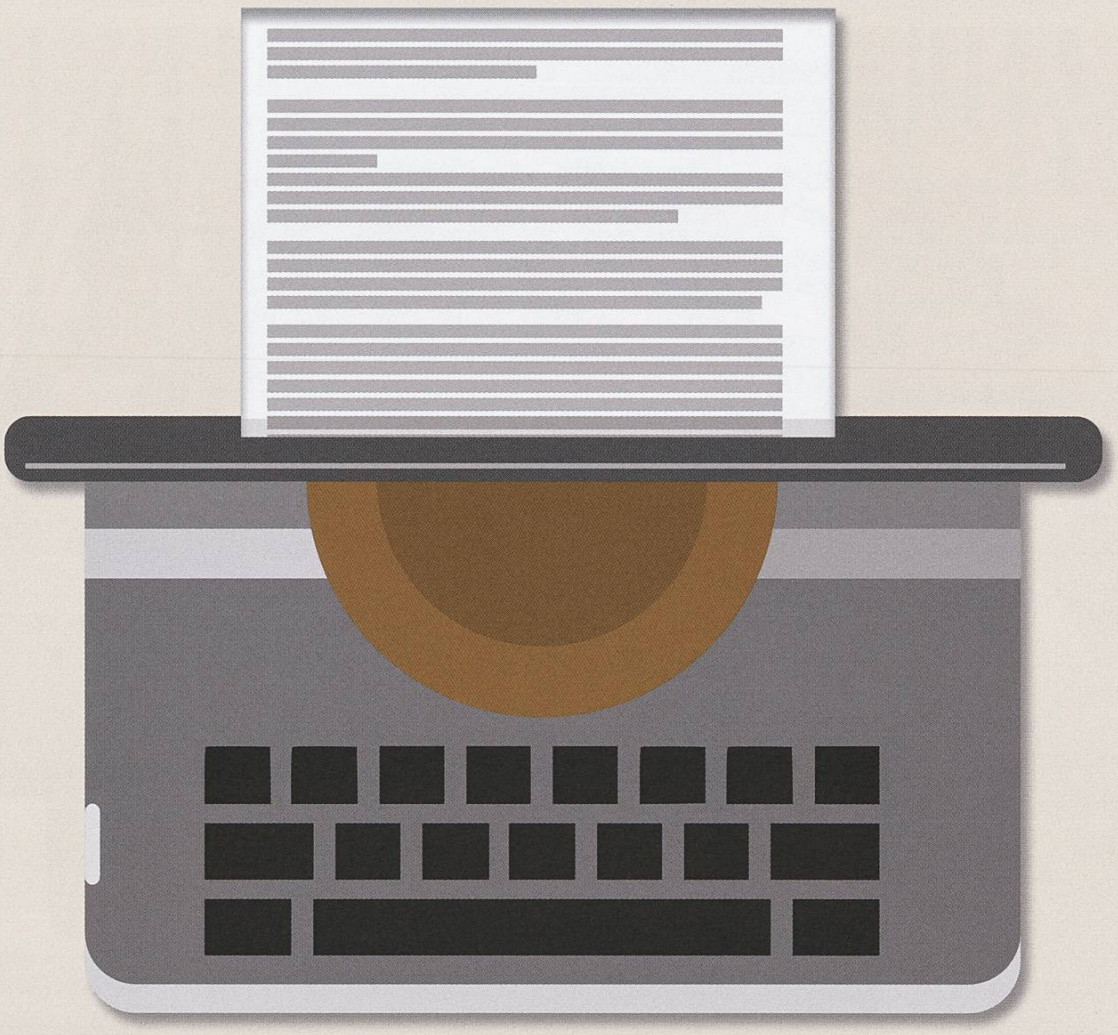
University Politics sound boring? Not at all! Our HoPo committee is always trying to improve the studies for our students and as being part of different departmental committees that can have a real influence on our students lives. If you like to help others, discuss the latest changes and change something yourself, HoPo gladly welcomes you on board.

hopo@vis.ethz.ch

v s v eth Fachverein Verband der Studierenden an der ETH


"By pushing the Hubble Telescope to its limits and thanks to Deep Learning techniques, we were able to detect water vapour by its spectrographic signature"
"This would suggest that the exoplanet K2-18b could theoretically support life"
Amazing, these scientists... it's so impressive...
And we're just sitting here, what are we doing to advance science or the pursuit of knowledge?
Are you kidding?!
Yesterday I published a script that automatically hides those annoying cookie banners!
True!
CommitStrip.com

edit, layout, publish



VISIONEN

Three times per semester a new issue of the VISIONEN, our VIS magazine, can be found in your mailboxes. Behind them is a motivated team of writers, proofreaders and layouters, whom are always looking for inspiration for the next big article. If your creativity is rather bound to words, and you have something to say to your fellow students, join the editorial staff and get your ideas out in the world.

visionen@vis.ethz.ch

v i s v eth Fachverein Verband der Studierenden an der ETH

VISionäre

VISionäre v.l.n.r.

- Philip Toma, Jonathan Thomm, Julian Croci, Pascal Wacker
- Noah Delius, Clemens Bachmann, Matthias Möhr, Nicolas Winkler
- Andreas Brombach, Frédéric Vogel, Sarah Kamp, Tobias Petter, Alexander Breuss

Impressum

VISIONEN

Magazin des Vereins der Informatik Studierenden an der ETH Zürich (VIS)

Ausgabe September 2019

Periodizität 6x jährlich
Auflage 2200

Chefredaktion
Sarah Kamp
chefredaktor@vis.ethz.ch

Cover
Layout-Team

Layout
Tobias Petter
Nicolas Winkler
Konstantin Wohlwend
layout@vis.ethz.ch

Anschrift Redaktion & Verlag
Verein Informatik Studierender (VIS)
CAB E31
Universitätsstr. 6
ETH Zentrum
CH–8092 Zürich

Inserate (4-farbig)

½ Seite	CHF 1000.–
1/1 Seite	CHF 1800.–
2/2 Doppelseite	CHF 4000.–
1/1 Seite, Umschlagsseite (U2)	CHF 3000.–
½ Seite, Rückumschlag (U4)	CHF 3000.–

Andere Formate auf Anfrage.

Redaktion
Clemens Bachmann
Alexander Breuss
Julian Croci
Sarah Kamp
Fiona Muntwyler
Julia Badertscher
Pascal Wacker
Nicole Wenzinger
redaktion@vis.ethz.ch

und freie Mitarbeiterinnen und Mitarbeiter

Inserate
Frédéric Vogel
inserate@vis.ethz.ch

Druck
Sprüngli Druck AG
5612 Villmergen
http://www.spruenglidruck.ch/

AZB
PP/Journal
CH – 8092 Zürich

Falls unzustellbar, bitte zurück an:
Verein der Informatik Studierenden
CAB E31
Universitätsstr. 6
ETH Zentrum
CH-8092 Zürich