
# Wireshark in Action:
## Empowering Education and Research

Tom Cordemans
Ville Haapakangas

#sf25eu

# Some info about the speakers

- Ville Haapakangas
- Senior lecturer @tamk
- Cybersecurity specialist
- Wireshark as a tool for education
- My socials: LinkedIn

- Tom Cordemans
- Senior lecturer @Odisee
- Researcher @DistriNet KU Leuven
- Sharing knowledge and expertise
- My socials: LinkedIn

# Agenda



- Introduction
- Join the CTF
- Packets never lie, but AI might!
- Wireshark CTF: Engaging Students Through Active Learning
- Everyone knows how TLS works, right?
- Time for the CTF!
- Q&A

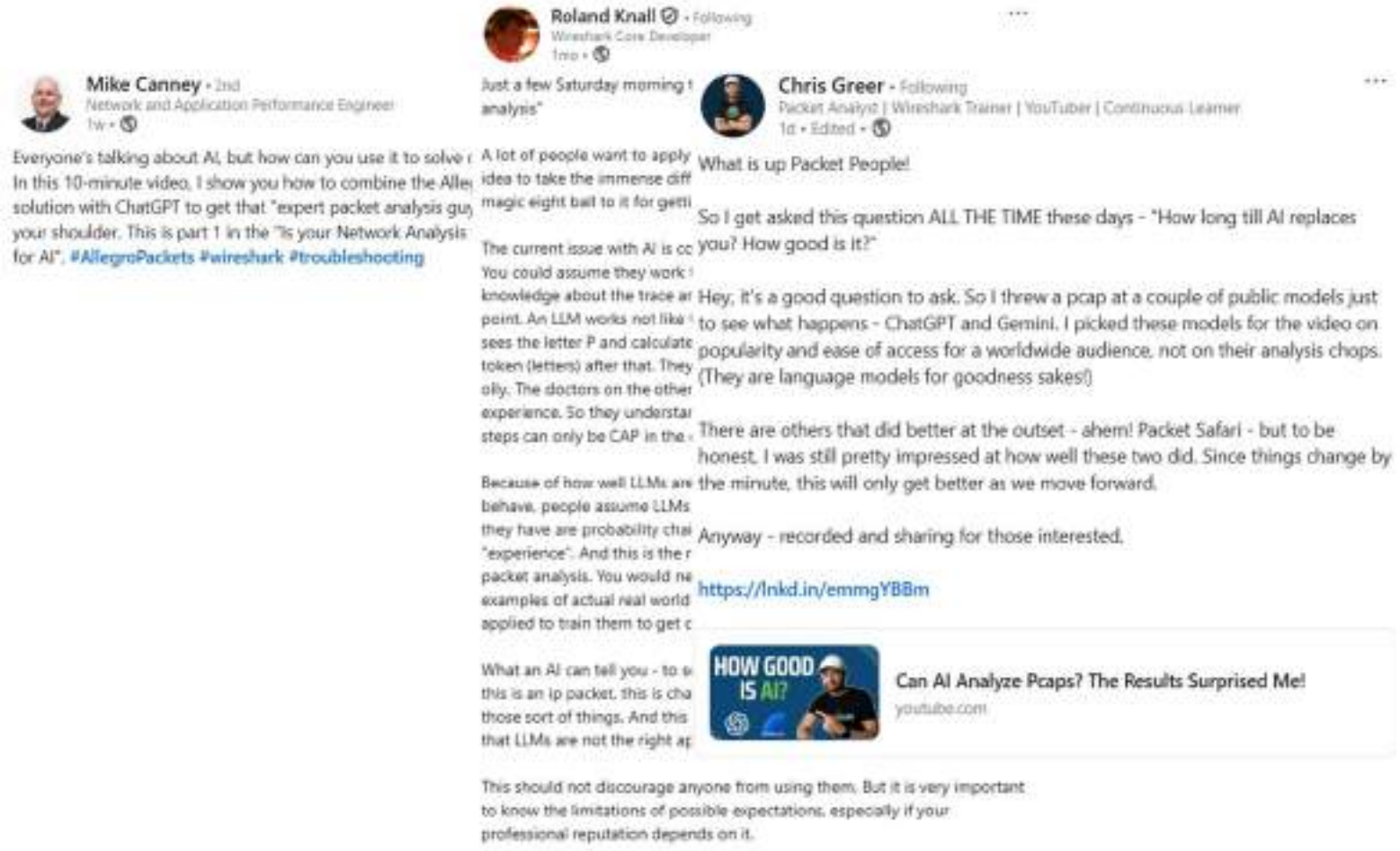
# Join the CTF

- https://synflop.ctfd.io
- Register
- Code: sf25

- [very short intro]

# Packets never lie, but AI might!

- Our students rely extensively and blindly on AI tools.



Mike Canney • 2nd
Network and Application Performance Engineer
1w •

Everyone's talking about AI, but how can you use it to solve
In this 10-minute video, I show you how to combine the Alle
solution with ChatGPT to get that "expert packet analysis gu
your shoulder. This is part 1 in the "Is your Network Analysis
for AI". #AllegroPackets #wireshark #troubleshooting

Roland Knall • Following
Wireshark Core Developer
1mo •

Just a few Saturday morning
analysis"

A lot of people want to apply
idea to take the immense diff
magic eight ball to it for getti

The current issue with AI is cc
You could assume they work
knowledge about the trace ar
point. An LLM works not like
sees the letter P and calculate
token (letters) after that. They
oily. The doctors on the other
experience. So they understar
steps can only be CAP in the

Because of how well LLMs are
behave, people assume LLMs
they have are probability chai
"experience". And this is the r
packet analysis. You would ne
examples of actual real world
applied to train them to get c

What an AI can tell you - to s
this is an ip packet, this is cha
those sort of things. And this
that LLMs are not the right ap

This should not discourage anyone from using them. But it is very important to know the limitations of possible expectations, especially if your professional reputation depends on it.

Chris Greer • Following
Packet Analyst | Wireshark Trainer | YouTuber | Continuous Learner
1d • Edited •

What is up Packet People!

So I get asked this question ALL THE TIME these days - "How long till AI replaces you? How good is it?"

Hey, it's a good question to ask. So I threw a pcap at a couple of public models just to see what happens - ChatGPT and Gemini. I picked these models for the video on popularity and ease of access for a worldwide audience, not on their analysis chops. (They are language models for goodness sakes!)

There are others that did better at the outset - ahem! Packet Safari - but to be honest, I was still pretty impressed at how well these two did. Since things change by the minute, this will only get better as we move forward.

Anyway - recorded and sharing for those interested.

https://lnkd.in/emmgYBBm



Can AI Analyze Pcaps? The Results Surprised Me!
youtube.com

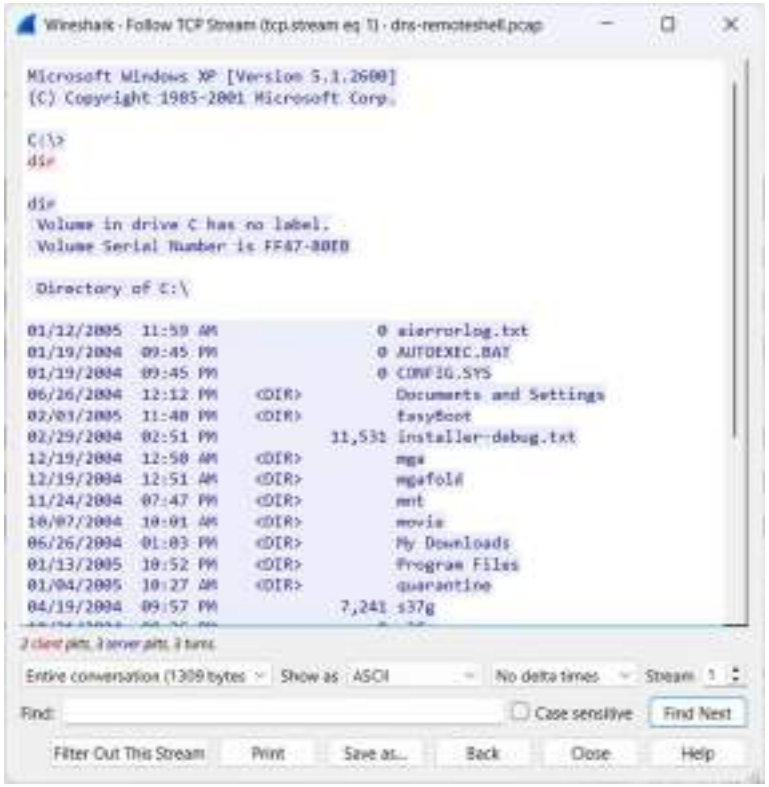
# Packets never lie, but AI might!

- The proof of the pudding is in the eating.
  - ChatGPT5
  - Claude Sonnet 4
  - Claude Sonnet 4.5
  - Google Gemini Flash 2.5
  - Google Gemini 2.5 Pro
  - Microsoft 365 Copilot
  - Packetcopilot Selector
  - PacketSafari Analyser Pro with Copilot

- A set of three PCAP samples
  - DNS-remoteshell.pcap (https://wiki.wireshark.org/SampleCaptures)
  - Demo-WLAN.pcapng
  - FTP.pcapng

# Packets never lie, but AI might!

- dns-remoteshell.pcap (131 frames)
  - 192.168.1.3:1396 <-> 192.168.1.2:53
  - 192.168.1.3:1403 <-> 192.188.1.2:23
  - 192.168.1.3:1404 <-> 192.168.1.2:80



# Packets never lie, but AI might!

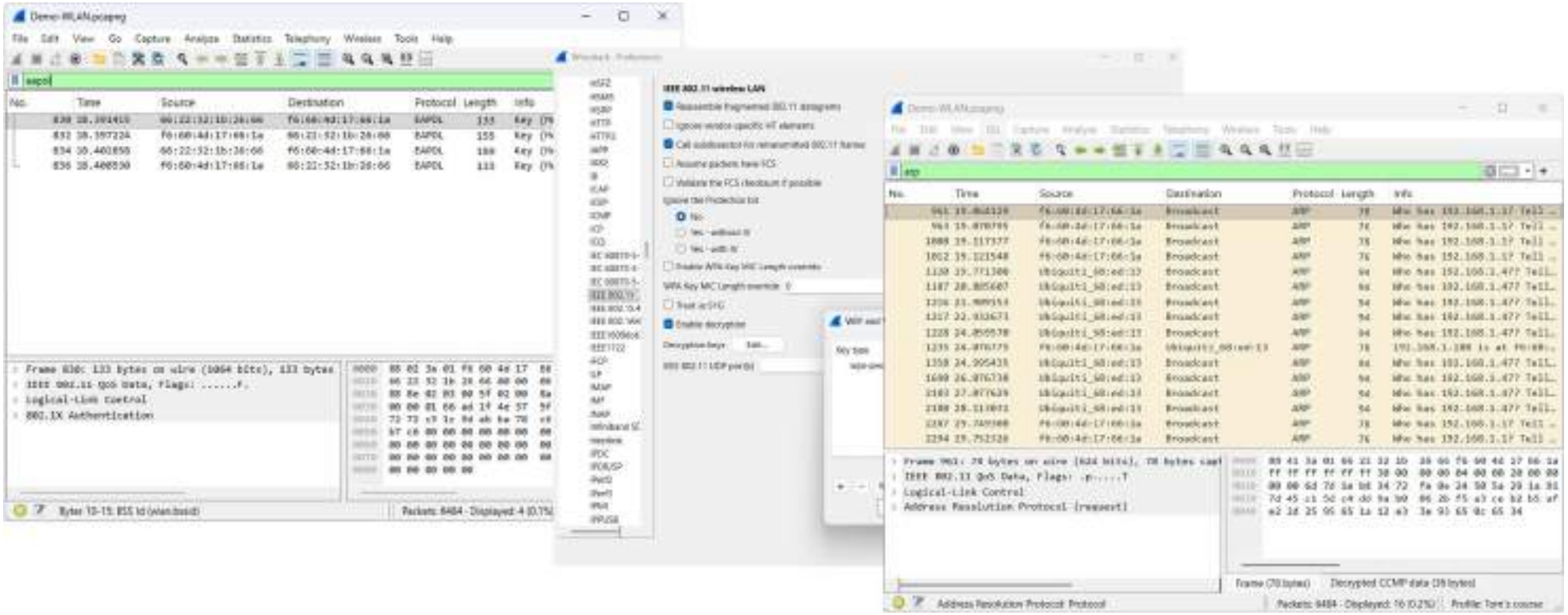
- dns-remoteshell.pcap

Prompt:
There are three remote shells in the PCAP file. Can you identify them?

- ChatGPT5
- Claude Sonnet 4
- Claude Sonnet 4.5
- Google Gemini Flash 2.5
- Google Gemini 2.5 Pro
- Microsoft 365 Copilot *** (Export as JSON)
- Packetcopilot Selector
- PacketSafari Analyser Pro with Copilot

# Packets never lie, but AI might!

- Demo-WLAN.pcapng (6484 frames)



# Packets never lie, but AI might!

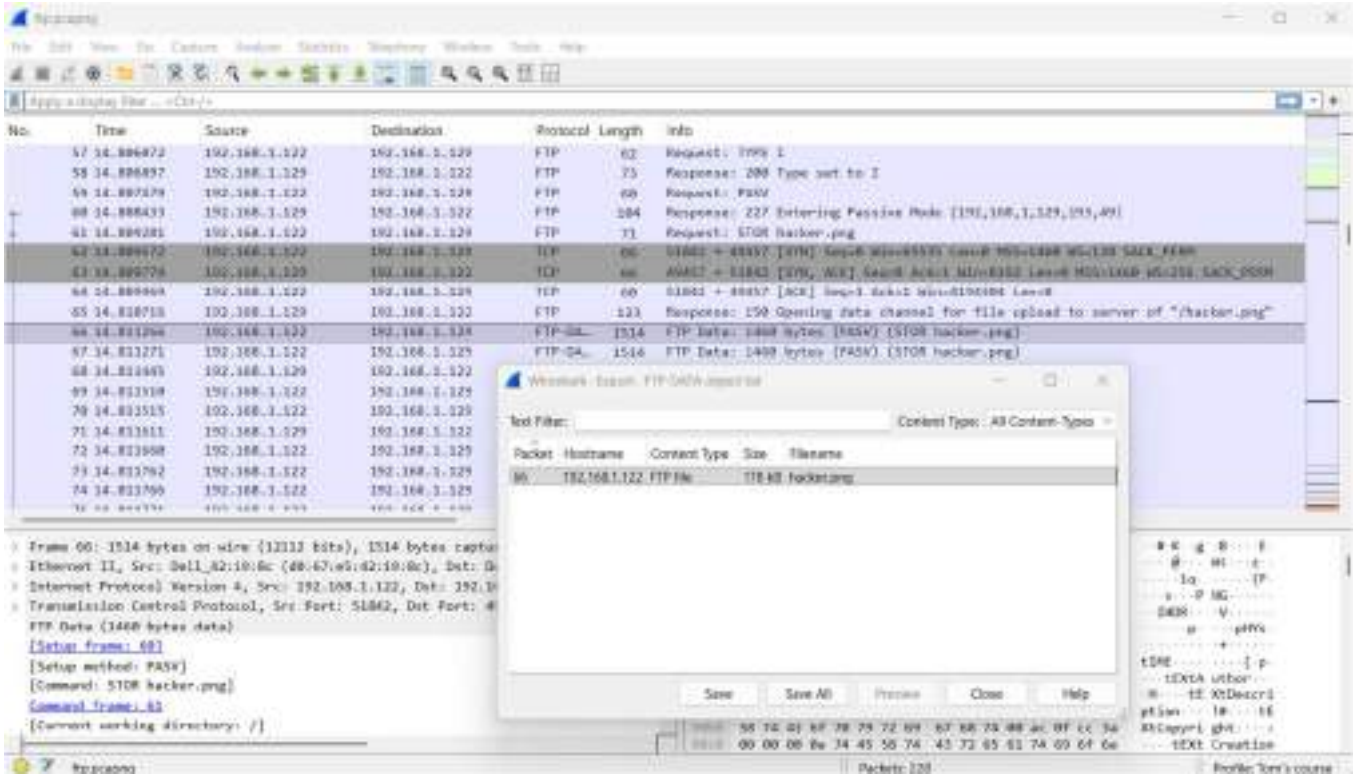
- Demo-WLAN.pcapng

Prompt:
Will we be able do decrypt the WLAN traffic of the SSID Demo-WLAN if we know the shared secret? (Yes/No and why?)

- ChatGPT5
- Claude Sonnet 4 (Could not upload the file)
- Claude Sonnet 4.5 (Could not upload the file)
- Google Gemini Flash 2.5
- Google Gemini 2.5 Pro
- Microsoft 365 Copilot *** (Export as JSON)
- Packetcopilot Selector
- PacketSafari Analyser Pro with Copilot (Limit of 250 frames)

# Packets never lie, but AI might!

- ftp.pcapng (228 frames)



# Packets never lie, but AI might!

- ftp.pcapng

Prompt:
Can you extract the file hacker.png out of the PCAP file?

- ChatGPT5 (Close but no cigar)
- Claude Sonnet 4 (Could not upload the file)
- Claude Sonnet 4.5 (Could not upload the file)
- Google Gemini Flash 2.5 (Error)
- Google Gemini 2.5 Pro (Error)
- Microsoft 365 Copilot *** (Export as JSON)
- Packetcopilot Selector (Lacks the option but gives a how-to)
- PacketSafari Analyser Pro with Copilot (Lacks the option … )

# Packets never lie, but AI might!



- Conclusions
  - We're getting closer, but we're not there yet
  - Solid expertise of network protocols remains essential

- Considerations
  - Sharing network traffic with third parties?
  - Develop your AI skills! (Go beyond prompting)
  - The cost of AI hallucinations: reduced effectiveness


# Adapting pedagogy to new learner generations:

*If we teach today's students as we taught yesterday's, we rob them of tomorrow.* Attributed to John Dewey (1859-1952)

| "Traditional" | -> | Modern learners expect: |
|---|---|---|
| Linear learning | -> | Multimodal learning |
| Print based, books | -> | Digital, interactive |
| Repetition, memorization, knowledge | -> | Discovery, problem-solving, gamification |
| Teacher-centered | -> | Collaborative |
| Passive content | -> | Active and personalized paths |
| Standard pace | -> | Adaptive progression |
| Focus on theory | -> | Practical, hands-on |

21st Century Skills

- Critical Thinking
- Creativity
- Collaboration
- Communication
- Information Literacy
- Media Literacy
- Technology Literacy
- Flexibility and Adaptability
- Initiative and Self-direction
- Social and Cross-cultural Skills
- Productivity and Accountability
- Leadership and Responsibility
- Problem Solving
- Global Awareness
- Innovation


**Gamification** ≠ game or playing a game

- Using game elements to **engage** and **activate** students
  - Motivation through rewards & progress tracking
  - Challenges, levels, and feedback loops
  - Points, competitions, prizes
- Fosters *engagement* and persistence
- Encourages *collaboration* and healthy competition
- Immediate reinforcement of learning outcomes
- Builds 21st-century skills such as *problem-solving*, *creativity*, and learner *autonomy*


## What is **CTF** (Capture the Flag)?

- A competition format where participants solve challenges to capture *flags* and earn points.
- **Gamification**!

## Pedagogical Challenge:

How to emphasize *learning through problem-solving* rather than just measure existing knowledge?

- Activities must be intentionally designed to support this goal!
- Not only a competition!

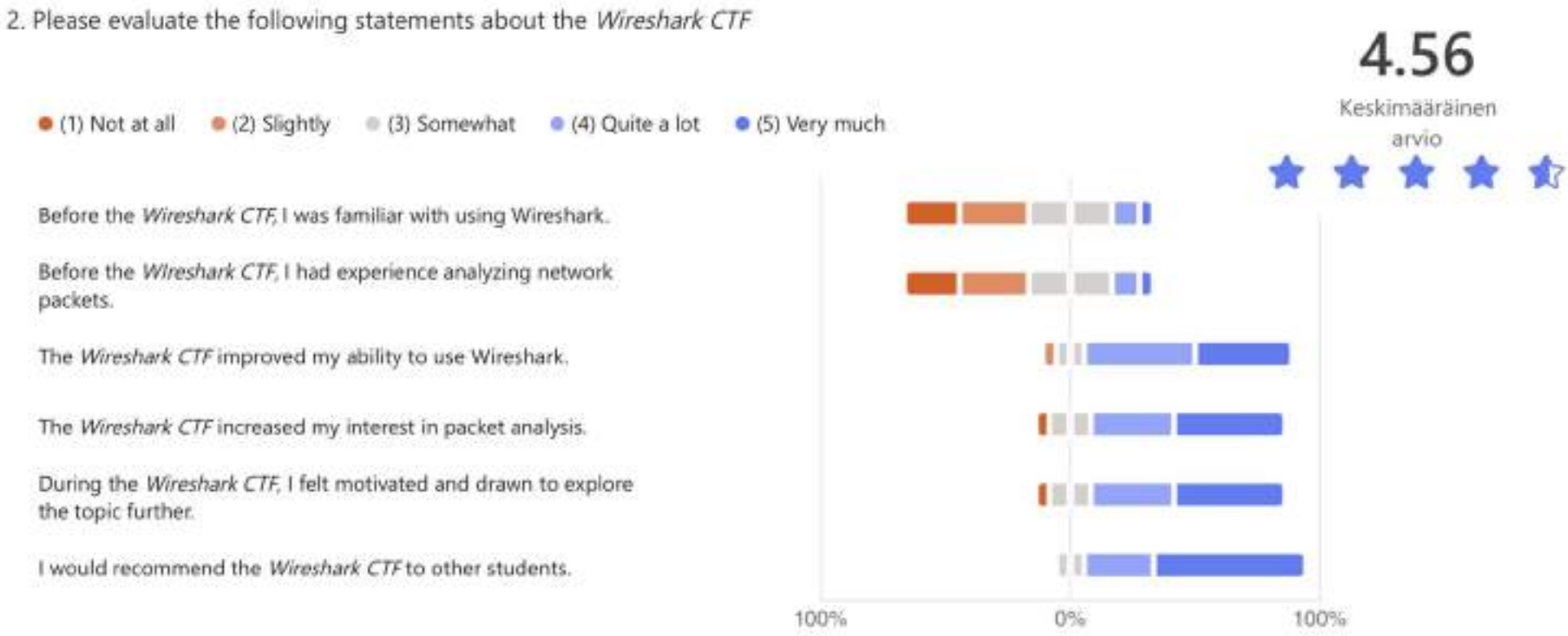

## Wireshark CTF

- Main objectives:
  - Understand how some common protocols work
  - Learn to use Wireshark (at least the basics)
  - Develop packet analysis skills
- Concept and testing: 2020–2023
- Pilot phase: 2024
- Ongoing re-design and evaluation


## Wireshark CTF, Current Implementation (2025)

- Integrated into the Ethical Hacking Blended Intensive Learning Programme at Kauno Kollegija
- 6 hours of lessons and demos, followed by self-studies and a 3.5-hour CTF final
- Over 120 challenges covering protocol analysis, troubleshooting, cybersecurity
- Platform: CTFd (self-hosted and cloud)

# Student Feedback - Strong Engagement and Learning Gains



# Student Feedback - Strong Engagement and Learning Gains


I liked the gamification of the learning process, i felt energized by the other students also trying to find the solution to the different challenges. I don't have enough knowledge to suggest improvements, i have learned a lot and loved the course till the end.

The answers needed to be specific in some cases, its easy to make mistakes, for example, the flag input for filters I liked the challenges, they were nice

liked the challenges since they are quite good. also hints were mostly helpfull.

## Lessons learned

- **Worth the effort – definitely!** The CTF method delivers strong engagement and learning impact.
- **Engagement:** Hard to predict time requirements, students often go beyond expectations.
- **Wording matters**: Nearly any task description can be misinterpreted. Clarity is essential but difficult.
- **Flags**: Must be unambiguous yet designing them clearly is not easy.
- **Cheating**: Always a risk, especially with AI tools. Incentives and scoring need careful planning.
- **CTF or gamification overload**: Not every topic fits this method. Choose contexts where problem-solving truly adds value.

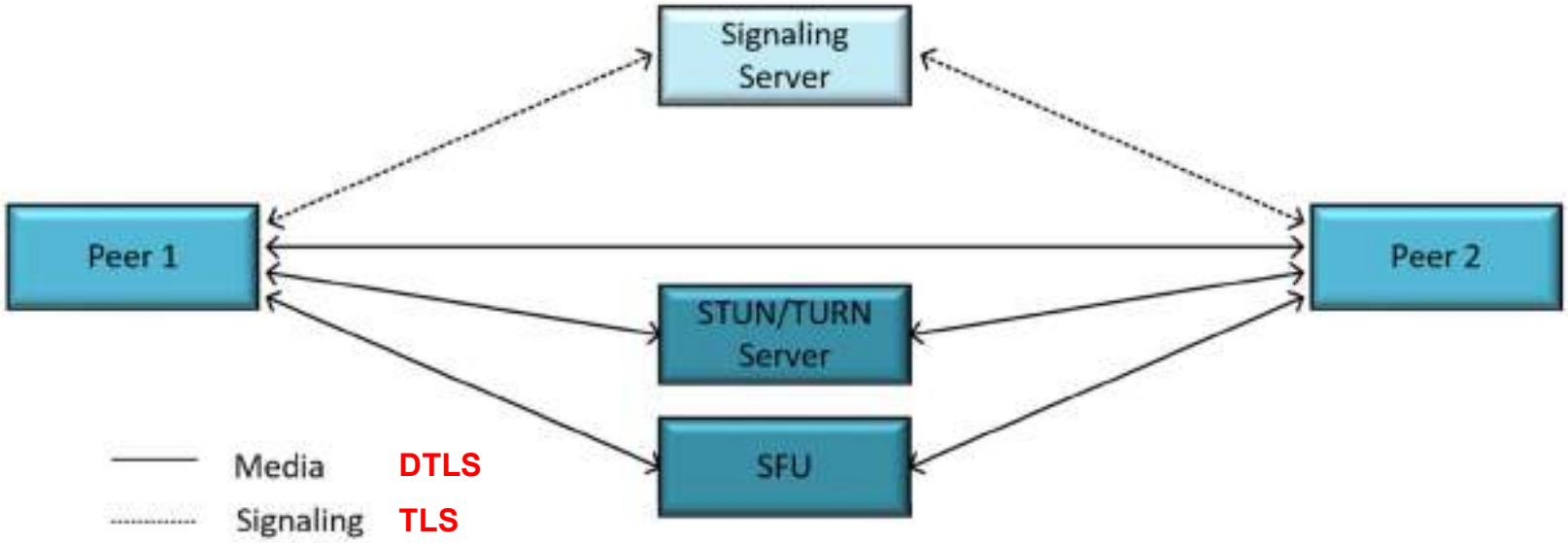
## What's Next for Wireshark CTF

- In the pipeline:
  - Bluetooth, Modbus, Zigbee, Wi-Fi
  - More cybersecurity related challenges
- Planned additions (collaboration welcome):
  - **Protocols**: IPv6, WebRTC, QUIC, extended TCP scenarios
  - **Wireshark features**: IO Graphs, Flow Graph, protocol-specific statistics, Profiles, tshark, and more
  - Add more advanced challenges

- **All ideas and contributions are warmly welcome!**

# Everyone knows how TLS works, right?

- Security analysis of Real-time communication (RTC) stacks in web apps and IoT devices



# Everyone knows how TLS works, right?

SharkFest'25 EUROPE

- TLS 1.2

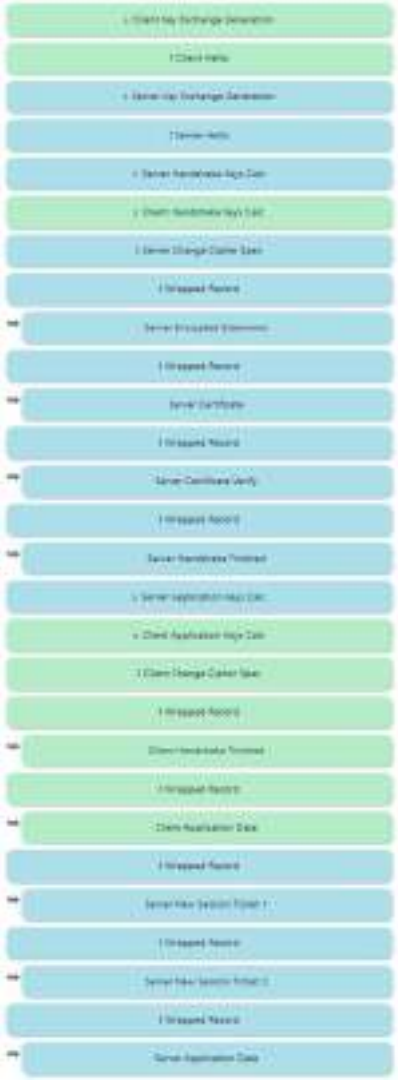

Source: https://tls12.xargs.org/

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TCP | 86 | 57164 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM |
| 2 | 0.002903 | 2a02:26f0:3900::172… | 2001:6a8:1d40:c632:… | TCP | 86 | 443 → 57164 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1344 SACK_PERM WS=128 |
| 3 | 0.002990 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TCP | 74 | 57164 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 4 | 0.002992 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TLSv1.2 | 276 | Client Hello (SNI=www.example.com) |
| 5 | 0.020000 | 2a02:26f0:3900::172… | 2001:6a8:1d40:c632:… | TLSv1.2 | 1454 | Server Hello |
| 6 | 0.020010 | 2a02:26f0:3900::172… | 2001:6a8:1d40:c632:… | TLSv1.2 | 1454 | Certificate, Certificate Status |
| 7 | 0.020012 | 2a02:26f0:3900::172… | 2001:6a8:1d40:c632:… | TLSv1.2 | 233 | Server Key Exchange, Server Hello Done |
| 8 | 0.020014 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TCP | 74 | 57164 → 443 [ACK] Seq=203 Ack=2761 Win=65280 Len=0 |
| 9 | 0.024252 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TLSv1.2 | 200 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 10 | 0.024261 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TLSv1.2 | 173 | Application Data |
| 11 | 0.024264 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TLSv1.2 | 528 | Application Data |

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TCP | 86 | 57164 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM |
| 2 | 0.002903 | 2a02:26f0:3900::172… | 2001:6a8:1d40:c632:… | TCP | 86 | 443 → 57164 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1344 SACK_PERM WS=128 |
| 3 | 0.002990 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TCP | 74 | 57164 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 4 | 0.002992 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TLSv1.2 | 276 | Client Hello (SNI=www.example.com) |
| 5 | 0.020000 | 2a02:26f0:3900::172… | 2001:6a8:1d40:c632:… | TLSv1.2 | 1454 | Server Hello |
| 6 | 0.020010 | 2a02:26f0:3900::172… | 2001:6a8:1d40:c632:… | TLSv1.2 | 1454 | Certificate, Certificate Status |
| 7 | 0.020012 | 2a02:26f0:3900::172… | 2001:6a8:1d40:c632:… | TLSv1.2 | 233 | Server Key Exchange, Server Hello Done |
| 8 | 0.020014 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TCP | 74 | 57164 → 443 [ACK] Seq=203 Ack=2761 Win=65280 Len=0 |
| 9 | 0.024252 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | TLSv1.2 | 200 | Client Key Exchange, Change Cipher Spec, Finished |
| 10 | 0.024261 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | HTTP2 | 173 | Magic, SETTINGS[0], WINDOW_UPDATE[0] |
| 11 | 0.024264 | 2001:6a8:1d40:c632:… | 2a02:26f0:3900::172… | HTTP2 | 528 | HEADERS[1]: GET /favicon.ico |

# Everyone knows how TLS works, right?

- TLS 1.3



Source: https://tls13.xargs.org/

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TCP | 86 | 64398 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM |
| 2 | 0.001111 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TCP | 86 | 443 → 64398 [SYN, ACK] Seq=0 Ack=1 Win=65000 Len=0 MSS=1344 SACK_PERM WS=128 |
| 3 | 0.003561 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TCP | 74 | 64398 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 4 | 0.005604 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TCP | 1418 | 64398 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1344 [TCP PDU reassembled in 5] |
| 5 | 0.005608 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TLSv1.3 | 510 | Client Hello (SNI=www.example.com) |
| 6 | 0.007540 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TCP | 74 | 443 → 64398 [ACK] Seq=1 Ack=1345 Win=32768 Len=0 |
| 7 | 0.007559 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TCP | 74 | 443 → 64398 [ACK] Seq=1 Ack=1790 Win=32256 Len=0 |
| 8 | 0.021787 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TLSv1.3 | 1454 | Server Hello, Change Cipher Spec, Application Data |
| 9 | 0.021788 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TCP | 1454 | 443 → 64398 [PSH, ACK] Seq=1381 Ack=1790 Win=72448 Len=1380 [TCP PDU reassembled in 10] |
| 10 | 0.021808 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TLSv1.3 | 364 | Application Data, Application Data, Application Data |
| 11 | 0.021812 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TCP | 74 | 64398 → 443 [ACK] Seq=1790 Ack=3851 Win=65280 Len=0 |
| 12 | 0.027193 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TLSv1.3 | 154 | Change Cipher Spec, Application Data |
| 13 | 0.027197 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TLSv1.3 | 166 | Application Data |
| 14 | 0.027199 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TLSv1.3 | 521 | Application Data |

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TCP | 86 | 64398 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM |
| 2 | 0.001111 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TCP | 86 | 443 → 64398 [SYN, ACK] Seq=0 Ack=1 Win=65000 Len=0 MSS=1344 SACK_PERM WS=128 |
| 3 | 0.003561 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TCP | 74 | 64398 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 4 | 0.005604 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TCP | 1418 | 64398 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1344 [TCP PDU reassembled in 5] |
| 5 | 0.005608 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TLSv1.3 | 510 | Client Hello (SNI=www.example.com) |
| 6 | 0.007540 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TCP | 74 | 443 → 64398 [ACK] Seq=1 Ack=1345 Win=32768 Len=0 |
| 7 | 0.007559 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TCP | 74 | 443 → 64398 [ACK] Seq=1 Ack=1790 Win=32256 Len=0 |
| 8 | 0.021787 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TLSv1.3 | 1454 | Server Hello, Change Cipher Spec, Encrypted Extensions |
| 9 | 0.021788 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TCP | 1454 | 443 → 64398 [PSH, ACK] Seq=1381 Ack=1790 Win=72448 Len=1380 [TCP PDU reassembled in 10] |
| 10 | 0.021808 | 2a02:26f0:3900::172... | 2001:6a8:1640:c632:... | TLSv1.3 | 364 | Certificate, Certificate Verify, Finished |
| 11 | 0.021812 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TCP | 74 | 64398 → 443 [ACK] Seq=1790 Ack=3851 Win=65280 Len=0 |
| 12 | 0.027193 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | TLSv1.3 | 154 | Change Cipher Spec, Finished |
| 13 | 0.027197 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | HTTP2 | 166 | Magic, SETTINGS[0], WINDOW_UPDATE[0] |
| 14 | 0.027199 | 2001:6a8:1640:c632:... | 2a02:26f0:3900::172... | HTTP2 | 521 | HEADERS[1]: GET /favicon.ico |

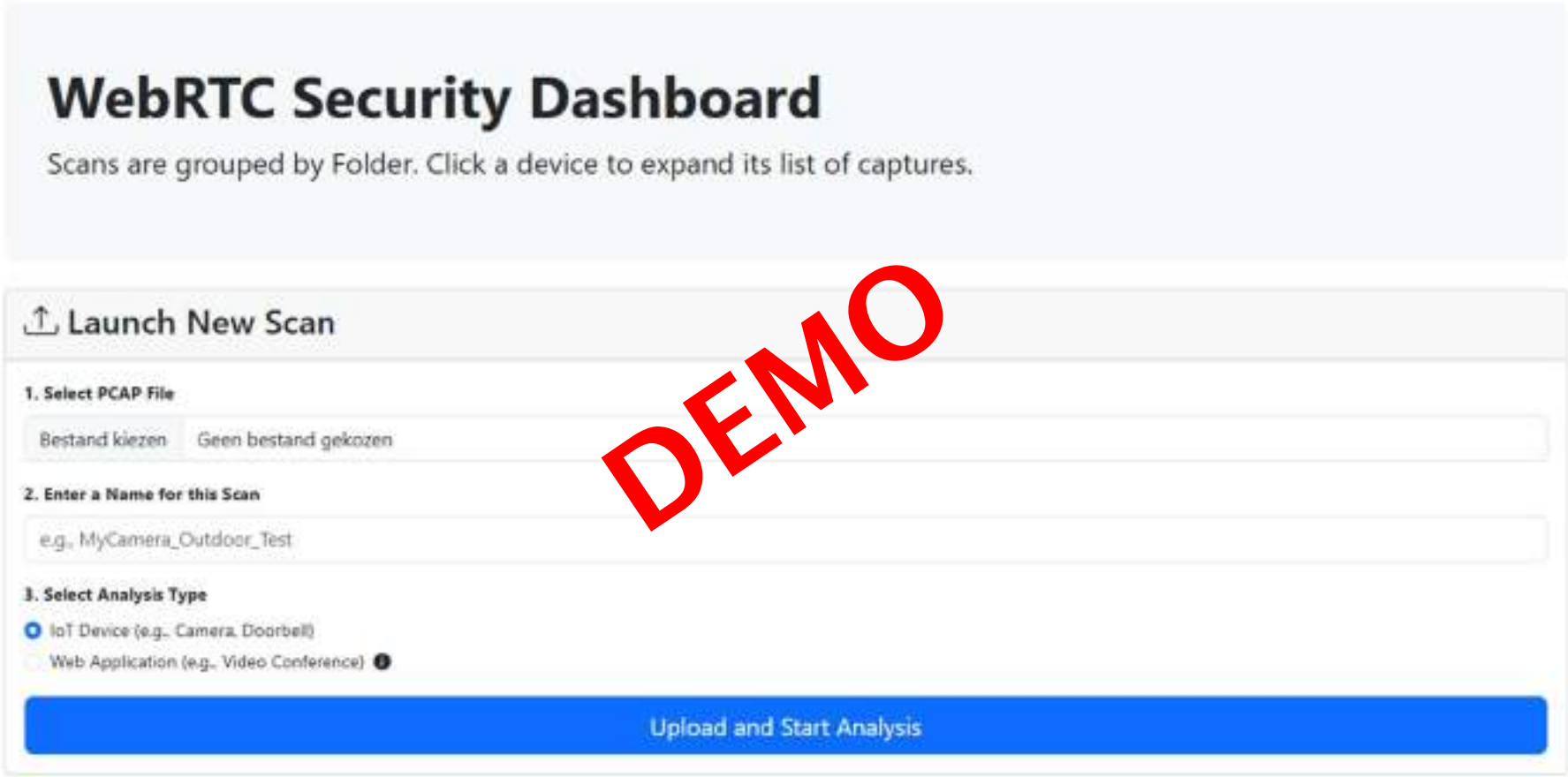
# Everyone knows how TLS works, right?

- Security analysis
  - STUN
  - TURN
  - DTLS (Media)
    - Weak cipher suites
    - Certificate health
      - Self-Signed
      - Outdated
  - TLS (Signaling)
    - Weak cipher suites
    - Certificate health
      - Self-Signed
      - Outdated

**Potential research approaches:**

- **Manually examine all PCAP files**
- **Developing a LUA script**
- **Utilization of TShark**
- **Building a framework with Scapy and PyShark**

# Everyone knows how TLS works, right?



# CTF contest!

- Time for the CTF contest
- https://synflop.ctfd.io
- Registering code: sf25

- Challenges:
  - Tom & Ville
  - Protocol analysis: 300 Well-known: DHCP
  - Cyberthreat: 900 The Great Data Escape

# Feedback QR code

#sf25eu