



SharkFest'23 EUROPE AGENDA

30 October – 3 November, Brussels



**All times are in the Western European Time Zone.
Conference days run from:
9:00 through 18:15, with evening events from 18:30-
20:30**

- **Pre-Conference Classes (9:00-17:00)**
- **SharkFest'23 Europe Session Agenda**
- **Session Abstracts & Instructor Bios**

SharkFest'23 EUROPE Conference Agenda

Pre-Conference Classes

<p>Pre-Conference Class I</p> <p>Next Generation Protocols & Advanced Network Analysis</p> <p>INSTRUCTOR: Phill Shade</p> <p>Ballroom: Salon A</p>	Monday, 30 October	
	8:00-9:00	Check-in & Badge Pick up
	9:00-12:00	Class in session (with morning break)
	12:00-13:00	Lunch
	13:00-17:00	Class in session (with afternoon break)
	Tuesday, 31 October	
	9:00am-12:00	Class in session (with morning break)
	12:00-13:00	Lunch
<p>Pre-Conference Class II</p> <p>Wireshark Filtering Masterclass</p> <p>INSTRUCTOR: Sake Blok</p> <p>Ballroom: Salon B</p>	Monday, 30 October	
	8:00-9:00	Check-in & Badge Pick up
	9:00-12:00	Class in session (with morning breaks)
	12:00-13:00	Lunch
	13:00-17:00pm	Class in session (with afternoon break)
	Tuesday, 31 October	
	8:00-9:00	Check-in & Badge Pick up
	9:00-12:00	Class in session (with morning breaks)
<p>Pre-Conference Class III</p> <p>TCP Analysis Masterclass</p> <p>INSTRUCTOR: Jasper Bongertz</p> <p>Ballroom: Salon B</p>	Tuesday, 31 October	
	8:00-9:00	Check-in & Badge Pick up
	9:00-12:00	Class in session (with morning breaks)
	12:00-13:00	Lunch
	13:00-17:00pm	Class in session (with afternoon break)

SharkFest'23 EUROPE Conference Agenda

SharkFest Opening & Welcome Dinner

		Tuesday, 31 October
SharkFest'23 EUROPE Welcome Dinner & Sponsor Showcase Studio 1 & Foyer	12:00-20:00	SharkFest'23 EUROPE Check-In & Badge Pick-Up
	13:00-17:00	Developer Den Drop-In
	18:00-20:30	<i>SharkFest'23 EUROPE Welcome Dinner & Sponsor Showcase</i> SharkFest'23 EUROPE Attendees Only


SharkFest'23 EUROPE Conference Agenda

Wednesday 1 November		
9:00-10:00	KEYNOTE: "...So That's What We Did" Gerald Combs & Friends Ballroom: Salon A	
10:00-10:15	BREAK	
10:15-11:30	(Beginner/Intermediate) Ballroom: Salon B	(Intermediate/Advanced) Ballroom: Salon A
	01 WebRTC and the Art of Conferencing Matthias Kaiser	02 From Packets to System Calls: Evolving Cloud Visibility to Detect Attacks (part 1 of 2-part workshop) Pablo Musa
11:30-11:45	BREAK	
11:45-13:00	03 Wireshark and AI Roland Knall	04 From Packets to System Calls: Evolving Cloud Visibility to Detect Attacks (part 2 of 2-part workshop) Pablo Musa
13:00-14:00	LUNCH	
14:00-15:15	05 Packet Capture in Public Cloud Stephen Donnelly	06 Analysing WebRTC connectivity issues on the packet level - a field report Robert Hess
15:15-15:30	BREAK	
15:30-16:45	07 Stepping up your packet analysis game by leveraging the Wireshark CLI tools (part 1 of 2-part workshop) Sake Blok	08 Real-world post-quantum TLS Peter Wu
16:45-17:00	BREAK	
17:00-18:15	09 Stepping up your packet analysis game by leveraging the Wireshark CLI tools (part 2 of 2-part workshop) Sake Blok	10 Multicast & Broadcast Reconnaissance - What Can a Hacker Learn From Your Packets? Betty DuBois
18:30-20:30	Sponsor Technology Showcase Reception, Treasure Hunt & Dinner	

SharkFest'23 EUROPE Conference Agenda

Thursday 2 November		
9:30-10:00	<p>PANEL DISCUSSION: <i>"Tips and Tricks; Ask me Anything"</i></p> <p>Ballroom: Salon A</p>	
10:00-10:15	BREAK	
10:15-11:30	<p>(Beginner/Intermediate) Ballroom: Salon B</p>	<p>(Intermediate/Advanced) Ballroom: Salon A</p>
	<p>11 Sniffing in da cloud: An IaC blueprint Uli Heilmeyer</p>	<p>12 Where does the feed from home cameras go? Traffic analysis and discussions on data privacy and security Andrea Fassina</p>
11:30-11:45	BREAK	
11:45-13:00	<p>13 The Packet Doctors are in! Packet trace examinations with the experts</p>	
13:00-14:00	LUNCH	
14:00-15:15	<p>14 Live capture in containers from the comfort of your desktop Wireshark Harald Albrecht</p>	<p>15 Bake your own Pi: Building a TLS Decrypting Wireless Traffic Sniffer Ross Bagurdes</p>
15:15-15:30	BREAK	
15:30-16:45	<p>16 Wireshark on Rails: A Tale of Trains, Taps and Teamwork Eddi Blenkers and Dirk Haseloff</p>	<p>17 Network Security Monitoring with Wireshark Christian Landström</p>
16:45-17:00	BREAK	
17:00-18:15	<p>18 ChatGPT in Wireshark Megumi Takeshita</p>	<p>19 It's Encrypted - now What? - Evaluating Encrypted Traffic Phill Shade</p>
18:30-20:30	<p>Sponsor Technology Showcase Reception, esPCAPe Group Packet Challenge & Dinner</p>	

SharkFest'23 EUROPE Conference Agenda

Friday 3 November		
9:00-10:00	<p style="text-align: center;">SHARKBYTES</p> <p>SharkBytes consist of “little crunchy bits of wisdom.” Like popular TED talks, SharkBytes aim to inform, inspire, surprise, and delight by delivering a speech on a personal topic in under 5 minutes. Information and a review of past SharkByte presentations can be found https://sharkfest.wireshark.org/sharkbytes Email us your SharkByte session idea: sharkfest@wireshark.org</p> <p style="text-align: center;">Ballroom: Salon A</p>	
10:00-10:15	BREAK	
10:15-11:30	(Beginner/Intermediate) Ballroom: Salon B	(Intermediate/Advanced) Ballroom: Salon A
	<p>20 Empowering Higher Education and Research with Wireshark: Innovative Approaches and Best Practices Ville Haapakangas and Tom Cordemans</p>	<p>21 Unraveling the Packet Mysteries: A Wireshark Journey with Machine Learning! (part 1 of 2-part workshop) Dr. Nathanael Weill</p>
11:30-11:45	BREAK	
11:45-13:00	<p>22 It's Always DNS! Johannes Weber</p>	<p>23 Unraveling the Packet Mysteries: A Wireshark Journey with Machine Learning! (part 2 of 2-part workshop) Dr. Nathanael Weill</p>
13:00-13:45	LUNCH	
13:45-15:00	<p>24 Understanding and troubleshooting IPsec VPNs Jean-Paul Archier</p>	<p>25 Weird captures, what can you do André Luyer</p>
15:00-16:30	 <p>Closing Remarks and Farewell reception</p>	

SharkFest'23 EUROPE Conference Agenda

Session Abstracts & Instructor Bios

(DRAFT - UPDATED FREQUENTLY)

Wednesday 1 November

9:00-10:00

KEYNOTE: "...So That's What We Did"

Gerald Combs & Friends

BREAK (10:00 – 10:15)

10:15-11:30

01 WebRTC and the Art of Conferencing

Web Real-Time Communication (WebRTC) describes a standards-based approach to initiating audio and video communication relationships via IP-based networks, in the simplest case using a browser. WebRTC has become the most significant solution for web-based conferencing in our time. It has been implemented by many conferencing solution manufacturers and providers worldwide.

In this talk Matthias will explain the areas of application of WebRTC in the enterprise and provider environment. Using Wireshark, he will guide you through the underlying processes and protocols for session negotiation, NAT traversal (STUN, TURN and ICE), and media transmission (SRTP).

Sample trace files are provided to follow along.

Instructor: Matthias Kaiser, Senior Trainer and Consultant, ExperTeach GmbH

Matthias started working in network analysis in 1996 as a Sniffer University staff instructor at Network General, where he delivered Sniffer University training and coordinated the European instructor team. In 2004, as a freelance instructor and network consultant, he wrote his own courseware on troubleshooting networks with Wireshark. Since 2009, Matthias has been working for ExperTeach, a German training and consulting company, where he manages and teaches the ExperTeach packet analysis curriculum for business customers. He has trained many individuals on Wireshark and helped them identify network and application-related problems since.

02 From Packets to System Calls: Evolving Cloud Visibility to Detect Attacks (part 1 of 2-part workshop)

Wireshark is the go-to tool for network packet visibility. However, new tools are needed to address the dynamic needs of cloud environments. Syscall analysis offers users next generation visibility for cloud environments. In this session, you'll get a hands-on introduction to an open source visibility tool, built specifically for the cloud: Falco.

Falco provides open source runtime security by monitoring syscalls. It acts like a security camera, monitoring cloud native environments and alerting users of threats, unexpected behavior and intrusions. Expand your knowledge, and learn about this tool created for cloud native by the co-creator of Wireshark.

Note: Every participant will need a WiFi Internet enabled laptop with a modern web browser to access their own lab environment and use Falco.

The following topics will be covered:

- An introduction from Gerald Combs covering the evolution from Wireshark to Falco
- Cloud Threat Detection and Runtime Security
- Install and Run Falco
- Falco Architecture
 - Data sources – syscalls and plugins
 - Data Enrichment – adding metadata
 - Falco rules – matching suspicious behavior
- Output channels – Falcosidekick and notifications (e.g. Slack)

Instructor: Pablo Musa, Developer Advocate, Sysdig

Pablo is a tenured speaker and trainer with more than 15 years of experience in the computer software industry. As an expert in the Observability ecosystem, he embraces the cutting-edge world of microservices and cloud-based monitoring and security. Holding a Master of Science (MSc) in

SharkFest'23 EUROPE Conference Agenda

Distributed Systems and Programming Languages, Pablo is a passionate educator who firmly believes in the power of knowledge sharing and its transformative impact on the tech community.

BREAK (11:30 – 11:45)

11:45-13:00

03 Wireshark and AI

AI is the new hot thing in town. In this session we demonstrate, how you can use AI with Wireshark for filtering, asking the right questions or giving the right inputs to gain the most from it. Additionally we demonstrate a fast and easy way to write your own protocol dissector by using the AI

Instructor: Roland Knall, Wireshark Core Developer

Roland has been a software developer for around 25 years, 8 of which he has developed for Wireshark and 6 of those as a Core Developer. He has seen all beginning with web and basic UI development and more recently focusing on embedded systems.

04 From Packets to System Calls: Evolving Cloud Visibility to Detect Attacks (part 2 of 2-part workshop)

Wireshark is the go-to tool for network packet visibility. However, new tools are needed to address the dynamic needs of cloud environments. Syscall analysis offers users next generation visibility for cloud environments. In this session, you'll get a hands-on introduction to an open source visibility tool, built specifically for the cloud: Falco.

Falco provides open source runtime security by monitoring syscalls. It acts like a security camera, monitoring cloud native environments and alerting users of threats, unexpected behavior and intrusions. Expand your knowledge, and learn about this tool created for cloud native by the co-creator of Wireshark.

Note: Every participant will need a WiFi Internet enabled laptop with a modern web browser to access their own lab environment and use Falco.

The following topics will be covered:

- An introduction from Gerald Combs covering the evolution from Wireshark to Falco
- Cloud Threat Detection and Runtime Security
- Install and Run Falco
- Falco Architecture
 - Data sources – syscalls and plugins
 - Data Enrichment – adding metadata
 - Falco rules – matching suspicious behavior
- Output channels – Falcosidekick and notifications (e.g. Slack)

Instructor: Pablo Musa, Developer Advocate, Sysdig

Pablo is a tenured speaker and trainer with more than 15 years of experience in the computer software industry. As an expert in the Observability ecosystem, he embraces the cutting-edge world of microservices and cloud-based monitoring and security. Holding a Master of Science (MSc) in Distributed Systems and Programming Languages, Pablo is a passionate educator who firmly believes in the power of knowledge sharing and its transformative impact on the tech community.

LUNCH (13:00 – 14:00)

14:00-15:15

05 Packet Capture in Public Cloud

Is packet capture still relevant in public cloud environments? Aren't flow logs sufficient, and doesn't the cloud provider secure their network? We will look at the motivations and use cases for packet capture in Cloud, as well as practical techniques for AWS and Azure.

Instructor: Stephen Donnelly, CTO, Endace

Stephen has worked on packet capture and time-stamping systems for 20 years, earning his PhD for "High Precision Timing in Passive Measurements of Data Networks" from the University of Waikato, New Zealand. A founding employee of Endace, Stephen has developed FPGA-based packet capture and timing systems, clock synchronization systems, and high-performance network monitoring virtualization, and collaborated with customers in telcos, finance, test & measurement, enterprise, and government agencies to solve unique problems. Stephen is a contributor to the Wireshark, libpcap, Argus, and Suricata open-source projects.

SharkFest'23 EUROPE Conference Agenda

06 Analysing WebRTC connectivity issues on the packet level - a field report

WebRTC and the required signaling as employed today's Web Conferencing solutions comes with a rather high complexity on the protocol level. Mix this with current network setups especially in large companies, encumbered by the need for remote working and current security threads and you end up with an intimidating debugging challenge if things don't work.

Based on 20 years of analyzing communication products and their protocols I'll present my current approach on drilling down on such problems using packet level analysis paired with the tools that come with WebRTC. I will also present an outlook towards the future of this approach in a world of ever-increasing encryption.

Contents:

- Typical problems when analyzing WebRTC connections.
- Overview of available analysis tools besides Wireshark.
- Where to capture packets - various test setups.
- Considerations when asking customers for packet captures.
- How to capture traffic from mobile apps.
- Anatomy of a specific session in Wireshark.
- Specific techniques used during Wireshark analysis.
- Aligning two captures from different network locations (i.e., VPN router and Internet egress)
- Which traffic is relevant for WebRTC analysis?
- What can be done about encryption?
- Outlook – What's left for packet level analysis when everything is encrypted and tunneled?

Instructor: Robert Hess

Starting with a small Web conferencing startup in Germany in 1999 and still with the same people after a long chain of acquisitions and mergers. These days I help transitioning the venerable GoToMeeting to the modern WebRTC based GoTo.

My day job is helping our developers as well as our customers to analyse and understand intricate network problems in the context of various communication protocols and complex corporate networks. As such I'm proficient in network analysis tools like Wireshark as well as in log analysis tools like Splunk. In my spare time, I read, do the odd triathlon together with my colleagues and fancy ice bathing.

BREAK (15:15 – 15:30)

15:30 - 16:45

07 Stepping up your packet analysis game by leveraging the Wireshark CLI tools (2-part workshop)

In this 2-slot HANDS-ON workshop you will add the Wireshark CLI tools to your toolbox in order to increase efficiency in analysing packet capture data. Preprocessing pcap files on the command-line (directly or with scripting) will greatly enhance the speed by which you can analyse the packets you need in Wireshark.

You will also practice with extracting data from pcap files that is hard to do with Wireshark. Being able to report on just any combination of fields in statistical overviews could help in pinpointing the root cause of an issue or enhance your understanding of the data flows in your environment.

Instructor: Sake Blok, Relational Therapist for Computer Systems

Sake has been analyzing packets for over 15 years. While working for a reseller of networking equipment, he discovered many bugs in devices from multiple vendors and presented his findings to the vendors to fix the issues. He also discovered many configuration issues that have led to functional problems or performance issues in applications running over the network. These issues were then resolved based on the reports presented to his customers. In 2009, Sake started the company SYN-bit to provide network analysis services to enterprises across Europe. During his work, Sake started developing functionality for Wireshark that he missed while working with the analyzer in his day-to-day job. He also enhanced multiple protocol dissectors to suit his analysis needs. In 2007, Sake joined the Wireshark Core Development team.

08 Real-world post-quantum TLS

Quantum computers are coming which may break the security of existing TLS communications. Therefore we need post-quantum (PQ) cryptography to secure the new world. In this session, we will go over the basic flow of a TLS session, and compare various configurations (TLS 1.2, TLS 1.3, TLS 1.3 with PQ). We will also discuss how we can use Wireshark to study real-world traffic on the public Internet. Since TLS is encrypted, we will also go over methods to enable TLS decryption.

SharkFest'23 EUROPE Conference Agenda

Instructor: Peter Wu

Peter Wu is part of the Research Team at Cloudflare, working on various TLS and cryptography-related projects. He is a contributor to many open source projects, including Wireshark, where he started in 2013 with TLS decryption improvements in order to assist in analyzing encrypted application traffic. Peter added TLS 1.3, QUIC, and WireGuard decryption support to Wireshark and aims to help everyone understand their traces.

BREAK (16:45 – 17:00)

17:00-18:15

09 Stepping up your packet analysis game by leveraging the Wireshark CLI tools (2-part workshop)

In this 2-slot HANDS-ON workshop you will add the Wireshark CLI tools to your toolbox in order to increase efficiency in analysing packet capture data. Preprocessing pcap files on the command-line (directly or switch scripting) will greatly enhance the speed by which you can analyse the packets you need in Wireshark.

You will also practice with extracting data from pcap files that is hard to do with Wireshark. Being able to report on just any combination of fields in statistical overviews could help in pinpointing the root cause of an issue or enhance your understanding of the data flows in your environment.

Instructor: Sake Blok, Relational Therapist for Computer Systems

Sake has been analyzing packets for over 15 years. While working for a reseller of networking equipment, he discovered many bugs in devices from multiple vendors and presented his findings to the vendors to fix the issues. He also discovered many configuration issues that have led to functional problems or performance issues in applications running over the network. These issues were then resolved based on the reports presented to his customers. In 2009, Sake started the company SYN-bit to provide network analysis services to enterprises across Europe. During his work, Sake started developing functionality for Wireshark that he missed while working with the analyzer in his day-to-day job. He also enhanced multiple protocol dissectors to suit his analysis needs. In 2007, Sake joined the Wireshark Core Development team.

10 Multicast & Broadcast Reconnaissance - What Can a Hacker Learn From Your Packets?

Multicast and broadcast packets are one of the last vestiges of cleartext traffic on our networks. If a hacker breaks into your environment, what sensitive data can they collect to pivot to your most valuable assets?

This presentation will cover a variety of discovery (Layers 2, 3, & 7), routing, and configuration protocols. Bring your laptop so you can follow along. Pcaps will be provided via [CloudShark Enterprise Hosted](#). Links will be sent in advance to give you a chance to download the files before the session.

Instructor: Betty DuBois, Mystery Solver, Packet Detectives

[Betty DuBois](#) unlocks the power of packets to resolve NetOps and SecOps issues. Founder of Packet Detectives, an application & network performance consulting and training firm the Washington, D.C area. She has been solving packet mysteries since 1997.

Experienced with a range of hardware and software packet capture solutions, she captures the right data, in the right place, and at the right time to find the real culprit.

Using packets to solve crimes against networks and applications is her passion. Teaching others to do the same is her calling.

18:30-20:30

Sponsor Technology Showcase Reception, Treasure Hunt & Dinner

SharkFest'23 EUROPE Conference Agenda

THURSDAY 2 NOVEMBER

9:00-10:00

PANEL DISCUSSION: *"Tips and Tricks; Ask me Anything"* Various Presenters

BREAK (10:00 – 10.15)

10:15-11:30

11 Sniffing in da cloud: An IaC blueprint

How to do an ad hoc capture in a 1k AWS accounts environment? In this session we will have a close look at how Infrastructure as Code with Terraform can be used to deploy and destroy a ad hoc capture infrastructure. We will discuss what works well and where the limitations are.

Instructors: Uli Heilmeier, DevSecOps Engineer

Uli has been a network protocol enthusiast for years, and he believes in RFCs and sharing knowledge. He has been working as a DevSecOps engineer at Vitesco Technologies.

12 Where does the feed from home cameras go? Traffic analysis and discussions on data privacy and security

An analysis of the EZVIZ/Hikvision wireless security camera reveals that the video feed of Italian users is always sent, via the Thrift protocol, to remote cloud servers outside of Italy owned by cloud providers subject to Chinese government laws which may include access to the decrypted content without the user' knowledge. This issue likely extends to other camera manufacturers, indicating a broader industry problem. The packet analysis has shown the network architecture, based on Kubernetes, of such device connecting to multiple endpoints via the SSDP, DHCP, NTP, UDP, TCP and HTTP protocols, to name a few. The public IP address of the device is also leaked to an external server. Unexpectedly there was also a RDP connection (X11) which could allow external third party to access the local wifi network. The transmission of video data involves international servers, raising privacy and security concerns. Critical vulnerabilities were found in the tested model, which have since been fixed by the device manufacturer. Addressing data localization, vulnerability disclosure, and overall security practices is crucial in the home security camera industry to protect user privacy and security. The iVMS backend cloud software of Hikvision, used in public monitoring, offers functionalities such as face detection, so transparency about server locations and type and data handling is essential for users putting these products in their home.

Instructors: Andrea Fassina, Cybersecurity Expert, Italian National Cybersecurity Agency

Andrea is a highly experienced professional with a diverse background in the field of technology. Andrea contributes to enhancing the Italy's cybersecurity efforts. Prior to this, he was a team leader of the Playback and Living Room devices team at DAZN in London. At Sky, he played a significant role in the Streaming and Cloud Computing team. As a Developer Evangelist at Bitmovin, Andrea successfully launched the developer network (bitmovin.dev) and conducted video courses worldwide on encoding, player, and analytics. Additionally, he organized the Milan Video Tech meetup and worked on various video apps proof-of-concepts.

Andrea has worked with multiple clients, specializing in device security, DRM, data analysis, web scraping, system architecture and network analysis. He likes working in Python with third-party APIs. He is a proud owner of a flipper Zero. He also holds a master degree in Electronic Engineering from the University of York.

BREAK (11:30 – 11:45)

11:45-13:00

13 The Packet Doctors are in! Packet trace examinations with the experts

The experts on this panel have been asked to look at a trace file and help find a reason for certain behaviors by attendees at many SharkFests. Based on this, they've decided to create a public forum for examining individual trace files with a broader audience for a collective learning experience. Trace files will be gathered from attendees prior to SharkFest and only given to the panel members during the session so that the "not-knowing what to expect and whether it can be solved" experience of working through an unknown trace file can be preserved. Come to this session and learn to ask the right questions and look at packets in different ways.

PLEASE SEND PERPLEXING TRACE FILES FOR ANALYSIS BY THE PANEL TO jasper@packet-foo.com PRIOR TO SHARKFEST!

SharkFest'23 EUROPE Conference Agenda

LUNCH (13:00 – 14:00)

14:00-15:15

14 Live capture in containers from the comfort of your desktop Wireshark

Edgeshark is an OpenSource project by Siemens that makes the virtual communication of and inside (Linux) containers easily accessible. It visualizes virtual container network topologies and configuration of communication. Users then can click on a "fin" button and get transferred to a new Wireshark live capture session.

The project consists of two services that are deployed to container hosts (such as Docker), as well as a Wireshark extcap plugin. The discovery service is container and pod-aware and provides information about virtual network stacks (network namespaces) and their interconnections, open sockets, forwarded ports, and more. The capture service streams pcapng data via websockets to Wireshark clients.

The extcap plugin connects Wireshark with containers and thus makes it "container-aware", adding useful meta data to captures about the container and system captured from.

Instructor: Harald Albrecht

Received a PhD from the Chair of Process Control Engineering at RWTH Aachen University. With Siemens Digital Industries now for more than 17 years in the field of systems communication and control networks. Father of Edgeshark.

15 Bake your own Pi: Building a TLS Decrypting Wireless Traffic Sniffer

Ever struggled with capturing traffic from your mobile device or felt stumped by encrypted applications? Dive into this comprehensive session to build your very own wired or wireless traffic sniffer using a Raspberry Pi.

In this engaging workshop, you'll explore:

- Selecting the ideal Raspberry Pi hardware and components.
- Choosing the best Raspbian OS versions.
- Building proper interface and routing configurations.
- Setting up a wireless AP.
- Generating and installing certificates.
- Setting up a TLS proxy to export session keys.
- Connecting devices to capture their traffic.
- Limitations of the device and configuration.
- Addressing critical security and privacy considerations associated with the device.

Walk away with the confidence and knowledge to construct a wireless capture device, granting you the power to decrypt and troubleshoot applications with ease(results may vary)

Instructor: Ross Bagurdes, Network Engineer & Educator, Bagurdes Technology

Ross has had a diverse career in engineering, beginning as a structural engineer, then project engineer for a gas utility, Ross was always quickly assigned the de-facto network administrator, typically after no one else was brave enough to break, and later fix, the network. Ross eventually ended up working as a network engineer designing and implementing enterprise networks for a major university hospital. Here he worked with Extreme Networks, HP, Cisco, Tipping Point, among other network technology, as well as honed his Wireshark and protocol analysis skills. Ross spent 7 years teaching data networking at Madison College, and in 2017 started authoring and producing IT training videos in Wireshark/Protocol Analysis, Cisco, and general networking topics for www.Pluralsight.com. In his free time, you'll find Ross and his dog at the beach swimming and surfing, traveling, hiking, or snowboarding somewhere in the western US.

BREAK (15:15 – 15:30)

15:30-16:45

16 Wireshark on Rails: A Tale of Trains, Taps and Teamwork

A modern passenger train is a rolling data center that happens to transport passenger. We used Wireshark to improve our understanding of the on-board systems and their communication. Using Wireshark in a train is much different to a network analysis in a data center or office network. Challenges begin with the location: A maintenance area for trains in a beautiful, but remote area. Careful planning, covering special cables, food and more, was rewarded with remarkable trace files.

Instructor: Eddi Blenkers, IT Security Analyst, BLT and Dirk Haseloff, ICT-Architekt, BLA

Eddi Blenkers is a member of the BLS IT security team. In 20+ years of IT security he uses Wireshark (or Ethereal, back in the days) to analyze network traffic. Understanding the regular data flow helps to spot irregularities, which might be indicators for an ongoing attack or just a simple

SharkFest'23 EUROPE Conference Agenda

misconfiguration that floods a log file. Being a rookie in the world of trains and IOT, he teams up with Dirk Haseloff to learn the specific requirements for the trains onboard-systems.

Dirk Haseloff is BLS' ICT architect responsible for the passenger information systems. Working with the manufacturer, he looks after the plethora of onboard-devices, including speakers, displays, cameras and a vast number of other devices. He uses Wireshark for troubleshooting and network planning.

17 Network Security Monitoring with Wireshark

While there are many dedicated solutions regarding network security monitoring out there, analyzing raw packet data for signs of malicious activity still is a valuable technique to either verify the solutions effectiveness or to provide network security monitoring at very low costs just relying on (automated) analysis of perimeter network traffic. In this session we will have a look at typical indicators of compromise for corporate infrastructures from a PCAP perspective, as well as to go through best practice approaches on spotting anomalies and behaviour changes within network traffic patterns which may indicate various types of attacks. Based on Incident response experience from the past 10+ years we will take a look at typical attacker patterns visible throughout network traffic, do some statistical analysis of network baselining approaches and give you many real-world examples from IR cases to build a foundation for you on what to look for in terms of detecting compromise of your infrastructure, etc.

Instructor: Christian Landström, CSIRT Lead DACH, NVISO Security

Christian Landström is the CSIRT Lead DACH for NVISO Security. In his previous roles he worked as Head of Managed Security Services at GDATA Advanced Analytics between 2019 and 2023 and as Incident Response and security audit expert for Airbus Cybersecurity from 2013 until 2019. He shares his passion about network analysis together with Jasper and Eddi with whom he started working in the field of network security and cyber security back in 2006 and since then has been an integral part of the SharkFest Community for over 10 years now.

BREAK (16:45 – 17:00)

17:00-18:15

18 ChatGPT in Wireshark

ChatGPT is trending in the IT world. Machine learning is one of the most evolved topics. Convolution / Recurrent neural networks with supervised learnings are already used for many AI-based systems such as Gmail Smart Reply. ChatGPT is one of the deep learning systems, the interesting point is we do not need difficult theory and complicated API library, we just need the natural query text (and URL) in any language!! How about applying ChatGPT with Wireshark?

This session uses ChatGPT for Wireshark/tshark, we use ChatGPT for packet manipulation, display filtering, capture filtering, creating graphs/charts, and analysing trace file with Wireshark.

ChatGPT is not a perfect packet doctor, but it works as a nice trace assistant if you indicate it correctly. Use Wireshark with ChatGPT and get better trace file analysis!!

Instructor: Megumi Takeshita, Packet Otaku and Owner, Ikeriri Network Service

Megumi Takeshita, or Packet Otaku, runs a packet analysis company, Ikeriri Network Service, in Japan. Ikeriri offers services such as packet analysis for troubleshooting, debugging and security inspection. Ikeriri is also a reseller of wired/wireless capture and analysis devices and software for Riverbed, Metageek, Profitap, Dualcomm, and others. Megumi has authored 10+ books about Wireshark and packet analysis in Japanese and she is an avid contributor to the Wireshark project.

19 It's Encrypted - now What? - Evaluating Encrypted Traffic

The realities of modern traffic analysis require interpreting encrypted network traffic correctly. Former Blackhat Phill Shade maintains that a detailed knowledge of how key protocols such as HTTP can provide valuable insights into what is happening in a suspect traffic capture. This workshop will provide an introduction to techniques for the evaluation of encrypted traffic using open-source tools such as Wireshark.

Instructor: Phill Shade, Owner, Merlion's Keep Consulting

Phill "Sherlock" Shade is a Senior Network / Forensics Investigator and founder of Merlion's Keep Consulting, specializing in all aspects of Network and Forensics Analysis. He is an internationally recognized Network Security and Forensics expert, drawing from his over 30 years of hands-on, real world experience. A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at Cyber Warfare Forum Initiative, he is a frequent consultant for numerous international security, technology and government agencies.

18:30-20:30

Sponsor Technology Showcase, esPCAPe Group Packet Challenge, Reception & Dinner

SharkFest'23 EUROPE Conference Agenda

FRIDAY 3 NOVEMBER

9:00-10:00

SharkBytes

BREAK (10:00 – 10:15)

10:15-11:30

20 Empowering Higher Education and Research with Wireshark: Innovative Approaches and Best Practices

This inspirational and interactive session will feature two senior lecturers from different European Universities of Applied Sciences, who will share their insights and best practices on leveraging Wireshark in both educational and research contexts.

Recognizing that today's students rely less on textbooks and more on dynamic learning experiences, educators must adapt and develop innovative methods to effectively engage students and help them achieve their aims. Furthermore, applied research is a fundamental cornerstone of higher education in applied sciences universities.

To this end, the presenters will offer a concise view of a few methods in which Wireshark has been successfully incorporated within their daily job.

The objective of this session is to provide participants with ideas on harnessing Wireshark's capabilities for their own activities while showcasing its usage in higher education and research.

Wireshark has become an omnipresent tool in the realms of IT, OT, IoT, and cybersecurity.

The primary focus of this presentation is to become more efficient in packet analysis. Based on our personal experiences as lecturers and researchers, we will discuss practical examples that highlight the tool's versatility and value.

This session is interactive and includes hands-on tasks with trace files. Trace files will be provided to the participants.

Instructors: Ville Haapakangas and Tom Cordemans

Ville Haapakangas

Senior Lecturer of Computer Networks and Cybersecurity at Tampere University of Applied Sciences (Tampere, Finland)

Working as a specialist in several cybersecurity related research projects

A speaker at Sharkfest22EU and a participant of SharkFest EU for a few years now

Tom Cordemans:

A daily user of Wireshark in IT, IoT and OT environments

ICT Technologist at DistriNet Research Unit @KU Leuven (Belgium)

Senior Lecturer at Odisee University of Applied Sciences (Belgium)

21 Unraveling the Packet Mysteries: A Wireshark Journey with Machine Learning! (part 1 of 2-part workshop)

Dive into the intricate world of packets and navigate through PCAP files with the compass of unsupervised machine learning (ML). Our goal? To uncover patterns, group similar packets, and spotlight those elusive edge behaviors.

What's on the Agenda?

1. **Tshark Deep Dive:** We'll harness the power of tshark, the renowned command-line tool, to extract the nitty-gritty from our PCAP files. If tshark's new to you, prepare to be amazed!
2. **Feature Engineering Workshop:** Let's sculpt the ideal perspective for our packets. By cherry-picking and transforming key attributes, we'll encapsulate the very soul of each network packet.
3. **Magic of Unsupervised ML:** With unsupervised models as our guide, we'll let the data weave its own narrative. Witness as patterns crystallize and packets find their kindred.

SharkFest'23 EUROPE Conference Agenda

What Will You Take Away?

- Tshark Tactics: Delve into PCAP analysis like a pro.
- Feature Engineering Insights: Shape the perfect representation for your network packets.
- ML Know-How: Leverage unsupervised models to classify and group the vast expanse of PCAP data.

Instructor: Dr. Nathanael Weill, Director of Data Science, B-Yond

Dr. Nathanael Weill, as the Director of Data Science at B-Yond adeptly combines complex data into innovative solutions. He is also currently a lecturer and member of the advisory board of the data science certificate at McGill School of Continuing Studies. Dr. Weill's unique blend of business acumen and technical prowess enables the creation of cutting-edge algorithms, infusing innovation and excellence into every project.

BREAK (11:30 – 11:45)

11:45-13:00

22 It's Always DNS!

We all know what DNS is, right? But when we need to troubleshoot DNS, it's getting much more complicated than initially thought.

This session dives deeper into the Domain Name System, covering recursive vs. iterative DNS queries, resource records types, TTL & caching, DNS errors, a little DNSSEC, flags, and of course: Wireshark with its useful display filters, custom columns, coloring rules, and so on. And we will explore some other tools to analyze and troubleshoot DNS even further.

Instructor: Johannes Weber, Network Security Consultant, SVA System Vertrieb Alexander GmbH

Johannes works as a network security consultant at SVA System Vertrieb Alexander GmbH. He has a master's degree in IT-Security (thesis: IPv6 Security) and blogs regularly at <https://netsec.blog/>, covering IPv6, VPNs, DNSSEC, NTP, Wireshark, and other topics. At customer sites, Johannes implements next-generation firewalls, mail and DNS appliances, as well as classical routers/switches.

23 Unraveling the Packet Mysteries: A Wireshark Journey with Machine Learning! (part 2 of 2-part workshop)

Dive into the intricate world of packets and navigate through PCAP files with the compass of unsupervised machine learning (ML). Our goal? To uncover patterns, group similar packets, and spotlight those elusive edge behaviors.

What's on the Agenda?

1. Tshark Deep Dive: We'll harness the power of tshark, the renowned command-line tool, to extract the nitty-gritty from our PCAP files. If tshark's new to you, prepare to be amazed!
2. Feature Engineering Workshop: Let's sculpt the ideal perspective for our packets. By cherry-picking and transforming key attributes, we'll encapsulate the very soul of each network packet.
3. Magic of Unsupervised ML: With unsupervised models as our guide, we'll let the data weave its own narrative. Witness as patterns crystallize and packets find their kindred.

What Will You Take Away?

- Tshark Tactics: Delve into PCAP analysis like a pro.
- Feature Engineering Insights: Shape the perfect representation for your network packets.
- ML Know-How: Leverage unsupervised models to classify and group the vast expanse of PCAP data.

Instructor: Dr. Nathanael Weill, Director of Data Science, B-Yond

Dr. Nathanael Weill, as the Director of Data Science at B-Yond adeptly combines complex data into innovative solutions. He is also currently a lecturer and member of the advisory board of the data science certificate at McGill School of Continuing Studies. Dr. Weill's unique blend of business acumen and technical prowess enables the creation of cutting-edge algorithms, infusing innovation and excellence into every project.

LUNCH (13:00 – 13:45)

13:45 – 15:00

24 Understanding and troubleshooting IPsec VPNs

With this session we intend to demonstrate how Wireshark can be used to analyze IPsec VPNs in site to site and remote access contexts. We will also present some dysfunctioning cases where Wireshark can be of some help.

SharkFest'23 EUROPE Conference Agenda

Instructor: Jean-Paul Archier

Jean-Paul has been working as a System and Network Engineer for more than 30 years. Since 2010, he has run his own company and is mainly focused on network training and consultancy. He is the author of several books for the French publisher ENI: VPN, IPv6, Cisco ASA, Postfix. He regularly gives training sessions on Wireshark and other network-related topics. As a certified trainer, he also delivers training about VPNs and network security for WatchGuard resellers and clients.

25 Weird captures, what can you do

Have you created a network capture on a virtual machine itself, as a first step, to get an idea of what happened? And saw some strange things when analyzing in Wireshark? Like negative delta times, out-of-order packets or ACKed unseen segments while it was captured on the endpoint itself.

This session is about why this can happen and what you can do to make capturing this way more reliable. With examples based on Linux.

Instructor: André Luyer

André is a senior Performance Consultant and troubleshooter at Rabobank, and has been analyzing packets for over 25 years. He started his career as a troubleshooter for network issues, both hard- and software, and later specialized in performance testing, which requires a combination of in-depth knowledge of networking protocols and coding skills. André also delivers an in-house 'Wireshark bootcamp' training course and contributed to the Wireshark project.

15:00 – 16:30

Closing Remarks & Farewell Reception