SharkFest'21 Virtual EUROPE

AGENDA

(Draft, subject to change)

All times are in the CEST time zone.
Conference days run from:
9:00am through 18:00

- **Pre-Conference Classes**
- **SharkFest'21 Virtual Session Agenda**
- **Session Abstracts & Instructor Bios**

SharkFest'21 Virtual EUROPE Conference Agenda

Pre-Conference Classes

Monday 14 June 2021	
9:00 – 17:00	**Pre-Conference Class I** **Analyzing Pcaps Faster with Filters** **INSTRUCTOR: Betty DuBois**
Tuesday 15 June 2021	
9:00 – 17:00	**Pre-Conference Class II** **Next Generation Protocols & Advanced Network Analysis** **INSTRUCTOR: Phil Shade**
Wednesday 16 June 2021	
9:00 – 17:00	**Pre-Conference Class III** **SSL/TLS Troubleshooting with Wireshark** **INSTRUCTOR: Sake Blok**

SharkFest'21 Virtual EUROPE Conference Agenda

Thursday, 17 June, 2021		
9:00-10:00	KEYNOTE: "*Latest Wireshark Developments & Road Map*" Gerald Combs & Friends	
10:00-10:15	BREAK	
	Zoom 1	Zoom 2
10:15-11:15	**01**  **Know your preferences** Uli Heilmeier	**02**  **Analysis and Troubleshooting of IPsec VPNs** Jean-Paul Archier
11:15-11:30	Q & A	
11:30-11:45	BREAK	
11:45-12:45	**03**  **Chasing application performance with Wireshark** Matthias Kaiser	**04**  **Automate your Analysis: tshark, the Swiss army knife** André Luyer
12:45-13:00	Q & A	
13:00-13:45	LUNCH	
13:45-14:45	**05**  **Make the bytes speak to you** Roland Knall	**06**  **When It's NOT a "Network Problem" - Identifying Higher-Layer Issues in Packet Data** Wes Morgan
14:45-15:00	Q & A	
15:00-15:15	BREAK	
15:15-16:15	**07**  **Cybersecurity-oriented Network Traffic Analysis** Luca Deri, Matteo Biscosi and Martin Scheu	**08**  **Back to the Packet Trenches** Hansang Bae
16:15-16:30	Q & A	
16:30-16:45	BREAK	
16:45-17:45	**09**  **Intro to QUIC - The TCP Killer?** Chris Greer	**10**  **Introduction to WAN Optimization** John Pittle
17:45-18:00	Q & A	

SharkFest'21 Virtual EUROPE Conference Agenda

Friday, 18 June 2021		
9:00-10:00	**KEYNOTE: "*Scapy Turned 18. Boy They Grow Up Fast, Don't They!*"** **Guillaume Valadon**	
10:00-10:15	**BREAK**	
	Zoom 1	**Zoom 2**
10:15-11:15	**13** **How long is a packet? And does it really matter?** Dr. Stephen Donnelly	**14** **How to analyze SACK and DSACK with Wireshark** Christian Reusch
11:15-11:30	**Q & A**	
11:30-11:45	**BREAK**	
11:45-12:45	**15** **DDoS from the packet level** Eddi Blenkers	**16** **The Packet Doctors are in! Packet trace examinations with the experts** Drs. Bae, Blok, Bongertz & Landström
12:45-13:00	**Q & A**	
13:00-13:45	**LUNCH**	
13:45-14:45	**17** **Network Forensics Analysis** Rami	**18** **Dissecting WiFi6 using Wireshark** Megumi Takeshita
14:45-15:00	**Q & A**	
15:00-15:15	**BREAK**	
15:15-16:15	**19** **Trace Files Case Files** Jasper Bongertz	**20** **More Patterns in TCP Retransmissions** Scott Reid
16:15-16:30	**Q & A**	
16:30-16:45	**BREAK**	
16:45-17:45	**21** **Discovering IPv6 with Wireshark** Rolf Leutert	**22** **imnurnet - Exploiting Your IPv4 Network with IPv6** Jeff Carrell
17:45-18:00	**Q & A**	

SharkFest'21 Virtual EUROPE Conference Agenda

Session Abstracts & Instructor Bios

(DRAFT - UPDATED FREQUENTLY)

THURSDAY, 17 JUNE

9:00-10:00

KEYNOTE: *Latest Wireshark Developments & Road Map*
Gerald Combs & Friends

10:15-11:15

01 Know your preferences

There are more than 1000 preferences in Wireshark. Most of the time the default value is good enough, But to know which preference brings you a better result can improve your analysis work. In this session we will have a look at a variety of preferences for all kinds of protocols, helpers and the UI.

Instructor: Uli Heilmeier, Lead Architect ICS Security, Syskron GmbH
Uli has been a network protocol enthusiast for years, he believes in RFCs and sharing knowledge. He has been working as a lead architect for ICS security at Syskron GmbH, a company offering services in the field of ICS/OT/industrial-IT.

02 Analysis and troubleshooting of IPsec VPNs

This presentation will explain what we can see when we launch and use VPNs based on IPsec, and how Wireshark can help with troubleshooting such VPNs. We will consider different examples, including: - site to site VPN - remote access VPN - IKEv1 and IKEv2 VPN - VPN with and without NAT We will explain how and when it is sometimes possible to decipher the IPsec exchanges. We will compare the information we can extract with or without deciphering of these exchanges. For most of the examples, we will first present traces of a VPN running smoothly, and then show traces for VPNs with some issues.Packet traces will be provided.

Instructor: Jean-Paul Archier, Consultant and Trainer, JPACONSEIL
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. Recently, a European VOIP Solution Provider asked him to build and dispense Wireshark training sessions for its resellers, focused specifically on SIP troubleshooting. As a certified trainer, he also delivers training about VPNs and network security for WatchGuard resellers and clients.

11:45-12:45

03 Chasing application performance with Wireshark

Slow database applications can be a pain for both, users, and administrators. With Wireshark, packet analysts often check the network first. But what comes next, when the network is fine? This presentation shows techniques for analyzing the performance of poor database applications with Wireshark in order to identify and isolate faults. Using real-life case studies, Matthias will guide you through the process of analyzing server performance and application response times from trace files using Wireshark and other tools, when the application performance is no good. Trace Files are provided to follow along with the analysis.

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.

04 Automate your Analysis: tshark, the Swiss army knife

Many use only the graphical interface of Wireshark, but the command line tools are also very useful. And even the command line options of Wireshark itself. This presentation shows you how to use tshark in scripts to do analysis that would be hard to do manually. For example, isolating the ratio resumed versus full TLS handshakes, generating a list of ciphers used, listing a count of different HTTP responses, plotting the concurrently active TCP streams, etc. By automating your analysis, you can quickly check for 'known problems' and have more time to investigate new issues. At Rabobank, we took this a step further and made it possible for novice users (DevOps team members) to upload their pcap file and get an automated report with checks and advices. At the core of this tool is tshark.

Instructor: André Luyer, Sr. Performance Consultant, Rabobank
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. He found that these skills are also useful for security analysis in the form of DDoS testing. André also delivers an in-house 'Wireshark bootcamp' training course.

13:45-14:45

05 Make the bytes speak to you

In this session, you will take a look at how dissection is organized in Wireshark's engine and how to write your first dissector. Also includes a few pointers on how to organize your protocols, what good practices are and where to go next.

Instructor: Roland Knall, Wireshark Core Developer
Roland is a software enthusiast with more than 20 years of experience in the field of software development and architecture. For the last 10 years his main focus has been Industrial Automation and VoIP, as well as managing software development teams. He has been a Core Developer of Wireshark since 2016 with the main focus on the UI.

06 When it's NOT a "Network Problem" - Identifying Higher-Layer Issues in Packet Data

While most professionals view packet captures as necessary only when investigating potential "network problems", one can often use packet data to draw important inferences and conclusions about conditions at higher layers of the OSI stack. In our time together, we'll walk through multiple examples of problems that were initially diagnosed through packet/protocol analysis, even though their ultimate root causes were found in the upper layers of the stack. We'll also talk about customizing Wireshark's look-and-feel to give you a better perspective on "what's going on up there". You'll leave this session with a better understanding of just how far packet analysis can REALLY take you in problem determination and performance analysis. Also includes a few pointers on how to organize your protocols, what good practices are and where to go next.

Instructor: Wes Morgan
Wes has been around computing and networks for 40+ years, with most of that time spent as either a systems administrator or software support engineer. Along the way, he became a full-stack troubleshooter, tracking down environmental glitches in customer environments around the world. He has seen almost every form of "blame the network" that mankind has invented. Wireshark has been a part of his everyday toolkit since the days of Ethereal 0.4 (or thereabouts).

15:15-16:15

07 Cybersecurity-oriented Network Traffic Analysis

In recent years we have observed an escalation of cybersecurity attacks, which are becoming more sophisticated and harder to detect as they use more advanced evasion techniques and encrypted communications. Wireshark is an advanced packet sniffer able to dissect both encrypted and clear-text traffic, and thus a good source of indicators that can be used to identify security threats.
The first part of the talk introduces various concepts and techniques that can be used on security-oriented traffic analysis, shows relevant algorithms useful to fingerprint traffic and identify potential threats and traffic anomalies. In the second part, we will show how Wireshark can be profitably used for generating traffic metrics and security information that can be combined with techniques presented earlier in the talk, to spot network threats. Finally we will demonstrate how the lessons learnt can be applied in real traffic scenarios using publicly available traffic traces of network attacks.

Instructors: Luca Deri, Leader, ntop Project, Matteo Biscosi, Software Engineer, ntop Project and Martin Scheu
Luca is the leader of the ntop (http://www.ntop.org) project aimed at developing an open-source monitoring platform for high-speed traffic analysis. He shares his time between ntop and the University of Pisa, where he is a lecturer in the Computer Science department.

Matteo is a Software developer who graduated in October of 2020 from the University of Pisa with a thesis about high-speed network traffic analysis. He currently works for ntop.org as software engineer.

Martin works at SWITCH CERT in Switzerland. Fascinated by packets on the wire, he is helping SMEs to get started with ICS/OT network monitoring.

08 Back to the packet trenches
In the session, Hansang provides real-world troubleshooting examples and interacts with attendees in addressing various TCP analysis scenarios.

Instructor: Hansang Bae, Field CTO, Netspoke
Hansang Bae led the Network/Application Performance Engineering Team with direct responsibility for Packet Capture Infrastructure at Citi until July, 2012. Since then he has been the CTO for Riverbed and currently works as Field CTO of Netskope. With his broad knowledge of protocol analysis in a complex enterprise infrastructure, Hansang brings a unique perspective to packet analysis.

16:45-17:45

09 Intro to QUIC - The TCP Killer?

It's 2021 - QUIC has formally arrived as an RFC, but it has been here for years. You capture traffic to Google, YouTube, Facebook, Cloudflare, and many other services and no longer see TCP as the primary transport protocol. Yes, QUIC over UDP is here, and it is growing. Some even tout it as a "TCP Killer". No matter what our role within IT, QUIC is a protocol we should familiarize ourselves with. Let's take a dive into QUIC and learn about this rapidly-expanding transport protocol.

Instructor: Chris Greer, Network Analyst, Packet Pioneer
Chris Greer is a Network Analyst for Packet Pioneer. He has worked with companies around the world, helping them to solve pesky network problems at the packet level, primarily with Wireshark and other open-source tools. Chris has a passion for helping others to learn about packet analysis and teaches Wireshark Courses to private companies as well as public audiences. You can follow him on his YouTube channel at - https://www.youtube.com/user/packetpioner

10 Introduction to WAN optimization

WAN Optimization technologies are present in many customer network environments, and have recently evolved to become even more important for Cloud, SaaS, and WFH distributed users. In this introductory session we will explore the key features, benefits, and design patterns of WAN Optimization from a network traffic perspective. We will use Wiresahark to explore sample traffic captures that highlight the expected behavior and measure the performance benefits of WAN Optimization.

Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.
As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.

SharkFest'21 Virtual EUROPE Conference Agenda

FRIDAY, 18 JUNE

9:00-10:00

KEYNOTE: "*Scapy Turned 18. Boy They Grow Up Fast, Don't They!*"
Guillaume Valadon

9:00-10:00

Keynote: Scapy Turned 18. Boy They Grow Up Fast, Don't They

Scapy (https://www.scapy.net), a program written in Python simplifying the handling of network packets, is 18 years old in 2021. Through this keynote, and on the occasion of the first commit made by Philippe Biondi on Wednesday March 26, 2003, the maintainers want to share the highlights of the project. The presentation will be an opportunity to discuss this free software which has grown a lot and whose community continues to amaze us. Beyond a retrospective of the little-known historical aspects of Scapy, different projects and scenarios of its use will be detailed.

Instructor: Guillaume Valadon
Guillaume Valadon holds a PhD in IPv6 networking. He likes looking at data and crafting packets. In his spare time, he co-maintains Scapy and learns reversing embedded devices. Also, he still remembers what AT+MS=V34 means! Guillaume regularly gives technical presentations, classes and live demonstrations, and write research papers for conferences and magazines.

10:15-11:15

13 How long is a packet? And does it really matter?
This will be an introductory level talk about Ethernet and IP networking focusing on packet length, bandwidth, and debugging issues. Can you trust Wireshark and your packet capture system? We consider what factors can affect reported packet length. How do we define, measure, and report bandwidth. What is the Bandwidth Delay Product, and do you still need to tune systems for it. What are some of the networking problems that can be caused by packet length issues, and how can you spot them.

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.

14 How to analyze SACK and DSACK with Wireshark

In this session, an overview about the different kind of SACK and DSACK types is given. And it will be demonstrated how Wireshark can be used / customized to support the analysis SACK and DSACK packets.

Instructor: Christian Reusch
Christian has been analyzing networks with Wireshark/Ethereal since 2000, has a great passion for packet analysis, and now maintains a private network blog CRnetPackets.com. For his day job, he works as a Network Engineer for interlocking systems at Siemens AG. Before his current job, he employed his considerable packet analysis skills for more than 5 years for 2nd and 3rd level network support in the financial service sector. Christian has also worked as a network analysis and performance freelancer.

11:45-12:45

15 DDoS from the packet level

DDoS attacks are a seemingly omnipresent nuisance. This presentation covers different attack methods like reflection attacks or SYN floods from a Wireshark-perspective.

A few protocols have remarkable properties that make them prime candidates for DDoS attacks. Using Wireshark we investigate the most popular protocols. We also look at the source of DDoS attacks and possible misconfigurations in a network that can lead to a self-inflicted DDoS. The last part covers methods to block incoming DDoS attacks and a few hints to make sure that your systems are no unwitting contributors to an attack.

Instructor: Eddi Blenkers
Eduard "Eddi" Blenkers has analyzed countless networks and applications - often teaming up with Jasper Bongertz. He is currently working as a ICT Security Specialist, identifying and eliminating attack vectors to networks and systems.

16 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!

13:45-14:45

17 Network Forensics Analysis

Advanced Persistent Threat (APT) groups do not like to have the evidence of their crime into their targets, usually, they would develop or use file-less malware to not leave any fingerprints traces proof their crime and unleashed their operations. Network forensics analysis became an essential skills to uncover APTs operation and identify what has happened by utilizing Wireshark and other open-source tools to analyze network packet captures (PCAP). In this lecture, we will introduce couple of APT attack scenarios and walk-through how to analyze them.

Instructor: Rami
Rami has experience across different information security and cybersecurity fields for over 12 years. Worked as Incident Response Expert in the past for four years to handle different cyber incident and events. Provided DFIR and Cyber Range training for different regions in the world (Europe, Asia, Middle East and US). Dealt with different sophisticated APT cyber incident cases that ranging from cyber espionage until data destruction.

18 Dissecting WiFi6 using WIreshark

It's time to capture WiFi6 and dissect IEEE802.11ax using Wireshark!! new method to capture traffic and filter, profile and so on. Wireless protocol evolves year by year, now new HE (High-Efficiency) ages comes to us, the instructor will show you IEEE802.11ax protocols and the difference with former WiFi, And she will demonstrate the way to capture WiFi6 with new software/hardware. The session will also include a WiFi6 specified profile including display filter/ filter button, coloring rule and so on.

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.

15:15-16:15 pm

19 Trace File Case Files

Working with packet capture (=trace) files usually means trying to find something quite specific. This can be indicators for connection problems, or verifying that there are data elements present/not present that you expect to troubleshoot how a protocol behaves. Sometimes it's also about

finding security issues, or patterns of an attack. In this talk we will walk through a couple of problem situations to see how they can be addressed, and maybe show a few tricks that you hadn't seen before.

Instructor: Jasper Bongertz, Network Security, Airbus CyberSecurity
Jasper Bongertz is a network security expert with focus on network forensics and incident response at Airbus CyberSecurity. He started working freelance in 1992 while he was studying computer science at the Technical University of Aachen. In 2009, Jasper became a Senior Consultant and trainer for Fast Lane, where he created a large training portfolio with a special focus on Wireshark and network hacking. In 2013, he joined Airbus CyberSecurity, focusing on IT security, Incident Response and Network Forensics, and moving on to become the Principal Network Security Specialist at G Data Advanced Analytics in August of 2019. Jasper is the creator of the packet analysis tool "TraceWrangler", which can be used to convert, edit and sanitize PCAP files. His blog regarding network analysis, network forensics and general security topics can be found at blog.packet-foo.com.

20 More Patterns in TCP Retransmissions

Picking up where we left off from a SharkFest presentation a few years ago, we'll use Wireshark to get a better understanding of the retransmission process. All retransmissions are not the same. Are they due to packet loss out on the WAN? A bad TCP parameter setting? A faulty NIC driver? In this session we'll take a look at some differences found in retransmitted data and see if we can determine their causes based on some distinct structures or "patterns" in the retransmissions.

Instructor: Scott Reid
Scott Reid is a member of the Systems and Infrastructure Analysis Group at a large Healthcare organization in Sweden. He has been using Wireshark and its predecessor, Ethereal for over ten years working with large medical imaging and laboratory systems.

At this position Wireshark is used on a daily basis for a range of functions - from benchmarking to development and pre-production testing to troubleshooting. A variety of protocols and technologies are examined and evaluated. Wireshark is often used while giving presentations to demonstrate the details and particulars of a case.

16:45-17:45

21 Discovering IPv6 with Wirehshark

This session will show you the key differences of IPv6 vs IPv4 by providing you with the necessary theory and using Wireshark to demonstrate the most important IPv6 processes.

Instructor: Rolf Leutert, Leutert NetServices
Leutert NetServices (LNS) is a small team of highly qualified network experts. For more than 30 years, we are offering trainings, troubleshooting and consulting in protocol analysing all over Europe.
LNS was the first company offering Network General's Sniffer trainings and, in 2006, the first to offer Wireshark trainings in Europe. LNS has trained thousands of students all over Europe in renowned companies from A(TT) to Z(urich Insurance). The trainings are very practice-oriented from many years of our troubleshooting experience. Rolf Leutert is SNIFFER Certified Master (SCM) and Wireshark Certified Network Analyst (WCNA).

22 imnurnet - Exploiting Your IPv4 Network with IPv6.

In networking, IP as we call it is generally Internet Protocol version 4 (IPv4). Internet Protocol version 6 (IPv6) is the replacement for IP running in today's networks. 22 years after the initial release of IPv6 we observe that many networks are not formally implementing IPv6, however, most modern desktop/server OS's have had IPv6 enabled for 8+ years. That means many IT departments and technologists don't understand that IPv6 is in fact all over their networks nor what the potential implications are. This session will cover a few IPv6 basics and then dive into a real-world demonstration accessing a live network and the recon/exploit of an "IPv4 only" network using IPv6.

Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enteprise
Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.

SharkFest'21 Virtual EUROPE Conference Agenda