- Pre-Conference Class
- SharkFest'19 Europe Agenda
- Instructor Bios
- Session Abstracts & Requirements

SharkFest'19 Europe
November 4th - 8th, 2019

Palacio Estoril
Estoril, Portugal

SharkFest'19 Europe Conference Agenda

Pre-Conference Course and SharkFest'19 Opening Schedule

Next Generation Protocols & Advanced Network Analysis **Pre-Conference Class** **Instructor: Phill Shade**	**Monday**	**4 November, 2019**	
	7:30 - 9:00 am	Check-in and Badge Pick up	Palacio Lobby
	7:30 am	Breakfast	Europa
	9:00 am	Laptop Setup and Class begins (with morning break)	Atlantico
	12:00 pm	Lunch Break	Europa
	1:00 pm	Class Resumes (with afternoon break)	Atlantico
	5:00 pm	Class day ends	Dinner–see area restaurant recommendations
	Tuesday	**5 November, 2019**	
	7:30 am	Breakfast	Europa
	9:00 am	Class begins (with morning break)	Atlantico
	12:00 pm	Lunch Break	Europa
	1:00 pm	Class Resumes (with afternoon break)	Atlantico
	5:00 pm	Class day ends	Attending SharkFest'19 Europe? See Tuesday Opening Schedule below
SharkFest'19 Europe **Opening Schedule**	**Tuesday**	**5 November, 2019**	
	12:00-8:00 pm	***Check-In & Badge Pick-Up for SharkFest'19 Europe***	***Lobby***
	1:00-5:00 pm	***Developer Drop-In Workshop***	***Bridge Room***
	5:00-8:00 pm	***Welcome Dinner & Sponsor Showcase Reception*** ***SharkFest'19 Europe Attendees Only***	***Europa***

SharkFest'19 Europe Conference Agenda

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

Wednesday	6 November, 2019			
7:00-8:30 am	**Breakfast** (Europa)			
7:00am-12:00 pm	**SharkFest Check-in** (Palacio Lobby)			
8:30-9:30 am	***Keynote & Welcome - Gerald Combs & Friends (Atlantico)***			
	Atlantico	**Park Suite**	**Tropical**	
9:30-9:45 am	Break			~~~~Pick up your Packet Challenge Sheet at the Registration Table in the Palacio Lobby~~~~
9:45-11:00 am	01 **Back to the Packet Trenches** Hansang Bae	02 **Troubleshooting WLANs (Part 1): Layer 1 & 2 analysis using multi-channel hardware, Wi-Spy & other tools** Rolf Leutert	03 **Writing a Wireshark dissector: 3 ways to eat bytes** Graham Bloice	
11:00-11:15 am	Break			
11:15 am-12:30 pm	04 **How Long is a Packet?** Stephen Donnelly	05 **Troubleshooting WLANs (Part 2): Understanding the functions of 802.11 management & control frames** Rolf Leutert	06 **Creating dissectors like a pro by generating dissectors** Richard Sharpe	
12:30-1:30 pm	LUNCH & LEARN – Riverbed Performance Engineering Certification Program			
1:30-2:45 pm	07 **Solving (SharkFest) packet challenges using tshark alone** Sake Blok	08 **Audio & Video with Wireshark** Megumi Takeshita	09 **Schrödinger's packets: they lie as long as they don't lie** Uli Heilmeier	
2:45-3:00 pm	Break			
3:00-4:15 pm	10 **Tracing Uncharted Networks** Eddi Blenkers	11 **TCP Split Brain: Compare/contrast TCP effects on client & server with Wireshark (Part 1)** John Pittle	12 **BACnet & Wireshark for beginners** Werner Fischer	
4:15-4:30 pm	Break			
4:30-5:45 pm	13 **Packet-less traffic analysis using Wireshark** Luca Deri & Samuele Sabella	14 **TCP Split Brain: Compare/contrast TCP effects on client & server with Wireshark (Part 2)** John Pittle	15 **My TCP Ain't Your TCP – ain't no TCP?** Simon Lindermann	
6:00-8:30 pm	***Sponsor Technology Showcase Reception, Treasure Hunt & Dinner (Europa)***			

SharkFest'19 Europe Conference Agenda

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

Thursday	7 November, 2019			
7:00-8:30 am	**Breakfast** (Europa)			
8:30am-9:30am	**SharkBytes*** (Atlantico)			
	Atlantico	**Park Suite**	**Tropical**	
9:30am–9:45 am	Break			
9:45am-11:00 am	16 **War story: troubleshooting issues on encrypted links** Christian Landström	17 **Wireshark as a part of your DevSecOps Cycle** Milorad Imbra	18 **Reliable Packet Capture** Christian Reusch	**Visit the Vendor Showcase in the Europa Room**
11:00–11:15 am	Break			
11:15am–12:30 pm	19 **EXPERT PANEL: Pros & Cons of Building your own Capture Appliance** Moderator: Sake Blok Panel: Jasper Bongertz, Hansang Bae, Luca Deri, Chris Greer	20 **Automate your analysis: tshark, the Swiss army knife** Andre Luyer	21 **Analysis & Troubleshooting of IPsec VPNs** Jean-Paul Archier	
12:30 –1:30 pm	**LUNCH & LEARN – Monitoring & incident Creation with Wireshark & PCAP Trace files**			
1:30–2:45 pm	22 **Using Wireshark to solve real problems for real people: step-by-step case studies in packet analysis** Kary Rogers	23 **Is it the network? (Part 1)** Matthias Kaiser	24 **IPv6 Crash Course: Understanding IPv6 as seen on the wire** Johannes Weber	
2:45-3:00 pm	Break			
3:00–4:15 pm	25 **The Packet Doctors are In!** Drs. Bae, Blok, Bongertz, Landström & Rogers	26 **Is it the network? (Part 2)** Matthias Kaiser	27 **WiFi Security 101 (Part 1)** Thomas D'Otreppe	
4:15–4:30 pm	Break			
4:30–5:45 pm	28 **Case studies of a cloud-based packet analysis and learning platform** Oliver-Tobias Ripka	29 **Troubleshooting Cisco Software-Defined Access architectures with Wireshark** Josh Halley	30 **WiFi Security 101 (Part 2)** Thomas D'Otreppe	
6:00–8:30 pm	***Sponsor Showcase, Group Packet Competition, & Dinner (Europa)***			

* **Submit your SharkByte session idea at https://sharkfest.wireshark.org/sharkbytes-form. 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 at https://sharkfest.wireshark.org/sharkbytes**

SharkFest'19 Europe Conference Agenda

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

Friday 8 November, 2019			
7:00-8:30 am	**Breakfast** (Europa)		
	Atlantico	**Park Suite**	**Tropical**
8:30–10:00 am	31 **Gentlemen's Software Set for Transport Protocols Testing & Learning** Vladimir Gerasimov	32 **Green Locks are not enough: Plaintext information in network protocols** Simone Mainardi	33 **Analysing VoIP Protocols: Discover Wireshark's numerous features to troubleshoot VoIP** Rolf Leutert
10:00 –10:15 am	Break		
10:15–11:45 am	34 **LTE Explained…The Other Protocols** Mark Stout	35 **Debugging TLS issues with Wireshark** Peter Wu	36 **Automating cloud infrastructure for packet capture and analysis** Brad Palm & Ryan Richter
11:45–1:30 pm	***Closing Comments, Packet Challenge Awards & Farewell Reception (Atlantico & Europa)***		

SharkFest'19 Europe Bios & Abstracts

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

WEDNESDAY, 6 NOVEMBER

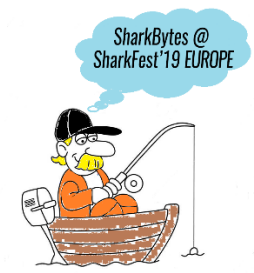
8:30–9:30 am	**Keynote: Gerald Combs & Company**
9:45-11:00 am	
Atlantico	**01 Back to the Packet Trenches** In this session, Hansang provides real-world troubleshooting examples and interacts with attendees in addressing various TCP analysis scenarios. **Instructor: Hansang Bae, Packet Guru** Hansang Bae led the Network/Application Performance Engineering Team with direct responsibility for Packet Capture Infrastructure at Citi until July, 2012 when he joined Riverbed Technology as Director of Cascade Product Architecture. He then took on the role of Chief Scientist and CTO for the company, and, in 2019, stepped into the role of Senior VP of Business Development to help guide Riverbed along a new strategic business path. Now that this business path is secured, Hansang has chosen to pursue new opportunities. With his broad knowledge of protocol analysis in complex enterprise infrastructures, Hansang brings a unique perspective to packet analysis.
Park Suite	**02 Troubleshooting WLANS (Part 1): Layer 1&2 analysis using multi-channel hardware, Wi-Spy & more** The availability of Wireless LANs has become more and more mission-critical for many enterprises, but troubleshooting WLANs is probably the most challenging task for network supporters. Various issues like physical layer interferences with foreign WLANs or other 'non-WLAN' devices like microwave ovens, remote control systems. etc. may significantly influence or reduce the performance of your wireless LAN. This session will demonstrate how to approach WLAN problems on Layer 1&2 using Wireshark, multi-channel hardware, and Wi-Spy. All tools will be live, and Wireshark will be customized with a specific profile to analyze different WLAN problems more efficiently. Moreover, the function of the important 'Radio Tap' pseudo-header and the valuable information available from these fields will be explained. Trace files from real problem situations will be used during the session to illustrate the topics mentioned above. **Instructor: Rolf Leutert, Owner, Leutert NetServices** Leutert NetServices (LNS) is a small team of highly qualified network experts. For more than 20 years, we have offered trainings, troubleshooting, and consulting in protocol analyzing all over Europe. LNS was the first company to offer 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, incorporating real-world scenarios from our many years of troubleshooting experience. Rolf is a SNIFFER Certified Master (SCM) and Wireshark Certified Network Analyst (WCNA).
Tropical	**03 Writing a Wireshark Dissector: 3 Ways to Eat Bytes** The presentation outlines the 3 most popular methods for writing a dissector, using plain text files with WSGD, using a Lua script file and, finally, a C dissector. An introduction to how dissectors fit into the Wireshark system is given, then each method is compared for ease of initial development, facilities offered, and run-time performance. **Instructor: Graham Bloice, Software Developer, Trihedral UK Ltd. & Wireshark Core Developer** Graham is a Software Developer with Trihedral UK Limited where he helps produce their VTScada HMI\Scada toolkit. Graham is also a Wireshark core developer, mainly concentrating on the Windows build machinery and DNP3 dissectors. He uses Wireshark frequently in his day job when analysing telemetry protocols used in the SCADA world, and inter-machine traffic for the company's distributed SCADA product.
11:15 am-12:30 pm	
12:30 – 1:30 pm	**LUNCH & LEARN – Riverbed Performance Engineering Certification Program** **Discover RCPE career-enhancing possibilities with John Pittle**
Atlantico	**04 How long is a packet?** 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.
Park Suite	**05 Troubleshooting WLANs (Part 2): Understanding the functions of 802.11 mgmt & control frames** This session is the continuation of Part 1, and will explain the function of the 802.11 management & control frames (like Beacon, Probe request/response, RTS/CTS and many more). These frames play an important role in the correct function of every WLAN. Profound knowledge of the different processes using these frames for controlling WLAN access is an inevitable requirement for successful troubleshooting. Analyzing roaming problems while capturing frames simultaneously in multiple channels will also be demonstrated. Trace files from real problem situations will be used during the session to illustrate the topics mentioned above. **Instructor: Rolf Leutert, Owner, Leutert NetServices** Leutert NetServices (LNS) is a small team of highly qualified network experts. For more than 20 years, we have offered trainings, troubleshooting, and consulting in protocol analyzing all over Europe. LNS was the first company to offer 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, incorporating real-world scenarios from our many years of troubleshooting experience. Rolf is a SNIFFER Certified Master (SCM) and Wireshark Certified Network Analyst (WCNA).
Tropical	**06 Creating Dissectors Like a Pro by Generating Dissectors** The wireshark dissector generator Richard has been working on for a while now can generate C and Lua dissectors and generates dissectors from a simple description of a protocol. This talk will show you how to quickly generate dissectors for any protocol you need a dissector for and how to make the best use of the dissector generator. **Instructor: Richard Sharpe, Founding Software Engineer, Hammerspace, & Wireshark Core Developer** Richard Sharpe is a software engineer who works on NFS and SMB and is a contributor to Wireshark and Samba. He has worked on a number of Wireshark dissectors and currently works on the Wi-Fi dissector suite a lot.
1:30-2:45 pm	
Atlantico	**07 Solving (SharkFest) packet capture challenges with tshark alone: Get exact answers from trace files in an automated way** Manual analysis of trace files with Wireshark is very valuable. But what if you need to extract information from trace files on a regular basis? How do you get the information out of a trace file with tshark so that it can be repeated in an automated way? In this session, Sake will show you how to extract specific data from a trace file, how to post process the data to get statistics, or present it in a better way. He will also spend some time on how to prevent false positives that would corrupt the results. The session will be presented by live-demoing the techniques on packet capture challenges from past Sharkfests. **(So if you would like to solve this years' capture challenge with tshark, make sure you get inspired during this session!)** **Instructor: Sake Blok, Relational Therapist for Computer Systems** Sake has been analysing 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 analyser 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.

Park Suite	**08 Audio & Video with Wireshark: get sounds and movies from traces of surveillance cameras, drive recorders, chat applications** Wireshark can dissect voice and video protocols such as sip, rtp, rtsp and so on. We can troubleshoot multimedia applications from trace files and utilize Wireshark to retrieve actual sounds and movie files (such as wav, mov, au, mp4) from packets. Megumi shows you many ways to get sounds and movies from traces of surveillance cameras, drive recorders, and chat applications. She will demonstrate techniques and tips to convert files using Wireshark, rtpdump, ffmpeg and other applications..This session is mainly for beginners but please note it contains some long CLI commands of tshark, rtpdump, ffmpeg, etc. with Wireshark GUI for converting trace files in Windows environment. **Instructor: Megumi Takeshita, Packet Otaku and Owner, ikeriri network service** Megumi Takeshita, packet otaku, runs a packet analysis company, ikeriri network service in Japan. Ikeriri offers services such as packet analysis for troubleshooting, debugging, security inspection and security testing. Ikeriri is also a reseller of wired/wireless capture and analysis products for Riverbed, Metageek, Profitap, Dualcomm, and others. Megumi has authored 10+ books about Wireshark and packet analysis in Japanese and she is one of contributors to the Wireshark projects, including Japanese localization
Tropical	**09 Schrödinger's packets: they lie as long as they don't lie** You often hear "Packets never lie". But this phrase itself is a lie. In this session, we will look at all the little lies we face when analysing packets. Be it the capture process, the operating system, Wireshark or other factors. **Instructor: Uli Heilmeier, Lead architect ICS Security, Syskron Security** 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 Security GmbH, a company offering services in the field of ICS/OT/industrial-IT.
3:00-4:15 pm	
Atlantico	**10 Tracing Uncharted Networks: A short intro to systematic network troubleshooting using Wireshark** You have 1 Million packets, 1000 hosts, and a vague problem description. This talk presents analysis techniques to locate problems from OSI layers 1 to 7. **Instructor: Eduard Blenkers, Sr. Network Consultant** Eduard "Eddi" Blenkers has analyzed countless networks and applications - often teaming up with Jasper Bongertz. The majority of analysis projects dumped SMB on his lap. The background in computer and network forensics often helped to link network packets to computer settings or misbehaving applications.
Park Suite	**11 TCP split brain: compare/contrast TCP effects on client and server with Wireshark (Part 1)** In this session, we'll explore the independent, and inter-dependent, TCP behaviors as viewed from both sides of a connection with Wireshark. Observe how each side makes assumptions about the other side based on the traffic it sees and the traffic it doesn't see. **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..
Tropical	**12 BACnet and Wireshark for Beginners** BACnet, the ASHRAE building automation and control networking protocol, is a most exciting one to study. This session is a step forward in providing basic details of the protocol itself, which can leave technical staff in the dark when they haven't a clue what's going on with the bits on the wire and these kind of communications. Troubleshooting these kinds of protocols with Wireshark provides a chance to apply the analyser in a way that allows you to gain a solid and lasting knowledge of packet analysis techniques. **Instructor: Werner Fischer, Principal Networking Consultant, avodaq AG** Werner has been an active and avid SharkFest supporter for many years, serving the community in various locations around the globe - Singapore, Mountain View, CA, and Vienna, AT – by using and teaching the same tool at each stop - Wireshark. That's Werner. Werner is also a long-term Dual-CCIE (R/S, Security) with over 20 years of experience in the networking arena. At avodaq, Werner works as a Principal Networking Consultant on System Architectures. He provides design guidance in key projects and is responsible for transferring new technology of networking solutions to internal and external audiences. Werner holds numerous industry certificates and has been a Sniffer Certified Master since 2003, VMware Certified Professional (4/5/6) and has also attained the Gold Certified Engineer status from the IPv6 Forum. Prior to joining avodaq 10 years ago, Werner worked as a Network Project Engineer for Siemens AG.

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

4:30-5:45 pm	
Atlantico	**13 Packet-less traffic analysis using Wireshark: How to use Wireshark for monitoring users, applications, and containers** For years, traffic monitoring has been packet-centric, with the industry putting a lot of effort into accelerating packet capture and analysis. Recently, the need to analyse users, applications, and software container interactions, has shown that the packet paradigm must now be complemented with additional information to provide network administrators the visibility they require. The introduction of technologies such as eBPF (extended Berkeley Packet Filter) and XDP (eXpress Data Path) enable traffic to be monitored in container-ised environments, and to gather metrics previously computed on packets (e.g. TCP retransmissions), without using packets at all. This talk will give an overview of the above technologies such as eBPF (extended Berkeley Packet Filter) and XDP (eXpress Data Path) enable traffic to be monitored in container-ised environments, and to gather metrics previously computed on packets (e.g. TCP retransmissions), without using packets at all. This talk will give an overview of the above technologies, and present some open-source tools the authors developed to enable Wireshark to effectively analyse in container-ised environments, as well as provide new traffic metrics unavailable when processing only packets. **Instructors: Luca Deri, Leader, ntop Project, & Samuele Sabella, CS Student, University of Pisa** Luca is the leader of the ntop project (http://www.ntop.org/) 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. Samuele is an undergraduate student at the Computer Science department of the University of Pisa, actually enrolled in the master's degree program. His interests are network monitoring and machine learning, the main topic of his study plan.
Park Suite	**14 TCP split brain: compare/contrast TCP effects on client and server with Wireshark (Part 2)** In this session, we'll explore the independent, and inter-dependent, TCP behaviors as viewed from both sides of a connection with Wireshark. Observe how each side makes assumptions about the other side based on the traffic it sees and the traffic it doesn't see. **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.
Tropical	**15 My TCP ain't your TCP ain't no TCP? How new implementations speed up the internet & make engineers drink** From the first specs to modern implementations, TCP stack behaviours have changed quite a bit and are still subject to major changes when new versions of operating systems are released. Big IT players push self-developed solutions. Estab-lished, long-standardized protocols are having a hard time gaining proper attention, with some working on totally different OSI layers. In this session, we are going to think outside the box and explore a few alternatives to our well known and beloved TCP and the implications for our daily operations. **Instructor: Simon Lindermann, Network Engineer, Miele** Since successfully completing his IT Specialist apprenticeship, Simon has been working as a Network Engineer for a German household appliance manufacturer. While working on projects in various global locations, he discovered his passion for network analysis so, along with his job at Miele, Simon started doing freelance troubleshooting work following the slogan "Only packets tell the truth!"



Submit a SharkByte!

THURSDAY, 7 NOVEMBER	
8:30–9:30 am	**SharkBytes (Atlantico)**
9:45-11:00 am	
Atlantico	**16 War story: troubleshooting issues on encrypted links** In this session, we will re-perform a real analysis job and analyze severe connectivity issues between two sites where the WAN link is fully encrypted. With four capture points in parallel, we will see what happened on the wire, how to deal with customers, vendors and service providers playing the blame game, and learn how to analyze unknown protocols. **Instructor: Christian Landström Senior Consultant, Airbus DS CyberSecurity** Christian Landström works as an Incident Response and Security Audit Expert at Airbus Defence and Space CyberSecurity. Working in IT since 2004, with a strong focus on network communications and IT security, he graduated with a degree in Computer Science in 2008 and joined Synerity Systems and afterwards moved with the whole Synerity team to work for Fast Lane GmbH. There, Christian created and delivered various network analysis trainings and worked as a Senior Consultant for network analysis and IT security. In 2013, he started working for Airbus Defence and Space CyberSecurity focusing on IT security, Incident Response and Network Forensics. He shares his passion for network analysis with Jasper and Eddi from the original Synerity Team at Sharkfest conferences and on the blog.packet-foo.com.
Park Suite	**17 Wireshark as a Part of your DevSecOps Cycle: How to include automated security and integration testing into your CI/CD practice using Wireshark** Modern SaaS solutions usually have a large number of integration points with other SaaS/PaaS which are crucial for their functioning. Enterprise integrations also include numerous distributed elements. Message queues, for example, can connect so many diverse systems using different protocols and architectures, that troubleshooting and testing it all can become a nightmare. This talk will present how to include automated security and integration testing with Wireshark into your CI/CD tooling. It will start with a SaaS system integrated with popular services like Auth0 and Stripe and move to a simple architecture constructed around RabbitMQ and give examples of automated Wireshark tests, including how they are integrated into Jenkins. **Instructor: Milorad Imbra, CTO, LinkMyCoach** Milorad is a Software Architect specializing in distributed systems, integrations, cloud services, and API design. He has worked on many enterprise integration projects, as well as on SaaS applications with startups. Using Wireshark regularly for troubleshooting integrations, Milorad thinks that Wireshark goes well with RabbitMQ, Elasticsearch and Jenkins.
Tropical	**18 Reliable Packet Capture** This session will cover mainly the topic of capturing data in ethernet networks. - It will show how network traffic can be captured in ethernet networks. - It will provide hints about cost-effective capture setups. - It will show what is needed for precise and reliable capture file. - It will show which parameters you must be consider for a reliable capture. - It will present some best practice capture strategies. - It will show pros and cons for different capture points (localhost/virtual mac) **Instructor: Christian Reusch, Network Architect, CRNetPACKETS** 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 packet analysis skills for more than 5 years for 2nd and 3rd level network support in the financial sector. Christian has also worked as a network analysis and performance freelancer.

11:15 am–12:30 pm	
Atlantico	**19 PANEL: The Pros & Cons of Building Your Own Capture Appliance** In this expert panel session, the following basic technological foundation topics will be reviewed before entering into a moderated discussion with audience participation. - Packet indexing - Data compression - Data format: pcap / vs. not pcap (custom format) - Storage types: rotating drives vs SSD vs NVME - The purpose of a FPGA based capture card (with a special focus on timestamping) - Network link types (fiber SX, LX, copper) and link speeds - TAP and SPAN connection requirements Moderated Panel/Open Discussion Topics - Purpose of a capture appliance (also: why not just a laptop?) - Network load and speeds as well as copper/fiber requirements - Portable/small/lightweight vs. fixed/rack mounted/heavy - RAM & CPU sizing - Ease of use / Operating System selection - Data transfer of the captured data / copy time delay via USB/Network/swappable removable disk - Wiping the device for the next job - Data encryption for sensitive data capture jobs - And the classic: Windows? Mac? Linux? VMS? :-) **Moderator: Sake Blok** **Expert Panel: Jasper Bongertz, Hansang Bae, Luca Deri, Chris Greer**
Park Suite	**20 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.
Tropical	**21 Analysis & 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 For each of them, 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, Owner, 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.

12:30–1:30 pm LUNCH & LEARN: MONITORING & INCIDENT CREATION WITH WIRESHARK & PCAP FILES

As the only open trace analysis tool in the industry, Wireshark's data analysis is too precious to not process in an enterprise management system

Spend your lunch hour with Andreas Diedrich and learn how his development IPAC-TM:

- Monitors data over long time periods based on pcap files
- Provides profile- and scenario-based packet analysis for parallel analysis tasks with tshark
- Creates incidents for processing by an external management system

1:30–2:45 pm

Atlantico

22 Using Wireshark to Solve Real Problems for Real People: Step-by-Step Real-World Case Studies in Packet Analysis

Stop banging your head on your desk trying to find root cause and solve performance problems. The answers are in the packets and this session will show you step-by-step in Wireshark how to solve real world case studies that had stumped others. Be the hero!

Instructor: Kary Rogers, Director, Staff Engineering, Riverbed Technology

Kary first learned the value of packet analysis helping customers solve difficult issues in Riverbed TAC, and has since moved onto a management role for the company. Not wanting to lose the skills he fought hard to learn, he started a packet analysis website, PacketBomb.com, where he posts tutorials and case studies for the hapless network engineer struggling to prove that it's not the network.

Park Suite

23 Is it the network? (Part 1): Troubleshooting network-related problems like packet loss and others

When network or application-related problems occur, the network is often blamed as being responsible for outages or bad performance. Quite often, staff responsible for network infrastructure need to prove whether the network is to blame or not. This presentation offers an introduction on how to differentiate network-related problems from application-related ones, and shows methods of identifying and isolating network problems. Using two real-life case studies, Matthias will guide attendees through the process of troubleshooting when a network shows packet loss and other network-related problems. Trace Files are provided to follow along with the analysis.

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

Matthias started his career in network analysis in 1996 when he joined Network General as one of the European Sniffer University staff instructors. In various position, he delivered Sniffer University training and coordinated the European instructor team with experts like Rolf, Eddi and Jasper. In 2004, working as a freelance instructor and network consultant, he started working with Wireshark and 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 has also helped various customers identify network and application-related problems.

Tropical

24 IPv6 Crash Course: Understanding IPv6 as seen on the wire

While it is quite obvious that the IP addresses have changed, it is not that easy to understand all those new control protocols such as ICMPv6 with its Router Advertisements, Neighbor Solicitations, and so on. How does a router propagate itself? How does a new IPv6 client get an IPv6 address? How does he know about the DNS server? How does the data link layer address resolution (ARP in v4) occur? How does a residential Internet connection get its IPv6 prefix via DHCPv6? This presentation guides you through pcaps and how to interpret and filter for relevant IPv6 messages with Wireshark.

Instructor: Johannes Weber, Security Consultant, TÜV Rheinland i-sec GmbH

Johannes is a network security consultant at TÜV Rheinland i-sec GmbH. He has a master's degree in IT-Security (thesis: IPv6 Security) and blogs regularly at https://weberblog.net, covering IPv6, DNSSEC, NTP, Wireshark and other topics. At customer sites Johannes works with next-generation firewalls, mail- and DNS-appliances, as well as classical routers/switches.

3:00–4:15 pm

Atlantico

25 The Packet Doctors are In! Packet Trace Diagnoses 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 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 BRING PERPLEXING TRACE FILES FOR SURGICAL ANALYSIS BY THE PANEL!**

Surgical Team: Drs. Bae, Blok, Bongertz, Landström & Rogers

Park Suite	**26 Is it the network? (Part 2): Troubleshooting networks when the network is OK** So you are in charge of analyzing the network and identifying problems with Wireshark? And you found the network in superb condition? So, how can we check server performance and overall application performance? This presentation demonstrates what needs to be done when the network is performing well and the users are still not happy. Using two more real-life case studies, Matthias guides you through the analysis and fault isolation process checking server performance and overall application performance when it wasn't the network. But whodunit? Trace Files are provided to follow along with the analysis. **Instructor: Mathias Kaiser, Senior Trainer and Consultant, ExperTeach GmbH** Matthias started his career in network analysis in 1996 when he joined Network General as one of the European Sniffer University staff instructors. In various position, he delivered Sniffer University training and coordinated the European instructor team with experts like Rolf, Eddi and Jasper. In 2004, working as a freelance instructor and network consultant, he started working with Wireshark and 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 has also helped various customers identify network and application-related problems.
Tropical	**27 WiFi Security 101 (Part 1)** Brought to you by the developer of the leading Wi-Fi attack suite - Aircrack-ng, this 2-part workshop covers the basics of Wi-Fi security through hands-on exercises. We'll begin with a brief presentation of the main standard and amendments, the different types of networks, as well as the common frames encountered on Wi-Fi networks. A short hardware section will explain how to pick the right hardware. We'll then go over different types of encryption used, and learn how to attack WPA/2 PSK as well as WPA/2 Enterprise networks, finishing up with a short introduction to GPUs to speed up the cracking process, if time permits. **NOTE! Students must bring the following equipment to participate in the class (available from amazon.fr/.co.uk/.com):** **- TP-Link MR3020** **- Alfa AWUS036NHA** **Your laptop must also have the latest VMware Workstation/Fusion (15+) installed and should have 8Gb+ RAM.** Time being short, a basic knowledge of networking and Linux command line is strongly advised. Resources: https://kali.training and https://linuxjourney.com **Instructor: Thomas d'Otreppe, Author, Aircrack-ng** Thomas d'Otreppe is a wireless security researcher and author of Aircrack-ng, the most popular and complete suite of tools for WiFi network security assessments. He is an active open source developer and also created OpenWIPS-ng, and WiFiBeat. He maintains (WPE) patches for hostAPd and Freeradius to test WPA Enterprise networks security and contributes to other open sources projects. Thomas is a contributor to the WiFi stack and toolset in Backtrack Linux, which has now become Kali Linux, the de facto top choice Linux distribution for penetration testing and vulnerability assessment. He is also the author of a pro-active wireless security course, "Offensive-Security Wireless Attacks (aka WiFu)" which has been delivered to large numbers of IT Security professionals worldwide. Thomas speaks and teaches in the Americas and Europe. He is a well-known speaker at DefCon, BlackHat, DerbyCon, SharkFest, Mundo Hacker Day, BruCON and other conferences.
4:30–5:45 pm	
Atlantico	**28 Case Studies of a cloud-based packet analysis and learning platform** Wave Packet Analyzer, a cloud-based packet indexer and analyzer, was first demo'ed at Sharkfest EU 2018. Since then it has come a long way and is ready to be released for testing., The first presentation focused on the technical implementation of a scalable, flexible data ingestion pipeline, presentation features and the technical details to overcome in development. The second edition of this talk will dive deeper into use cases of the platform and open it for alpha testing to a limited group. **Instructor: Oliver-Tobias Ripka, Consultant and Trainer, Ripka-Security Consulting** Oliver-Tobias Ripka is a network security expert with focus on offensive security and network analysis at Ripka - Security Consulting. During his international studies in Germany, France, and Portugal, he focused on machine learning and databases and worked on testing global climate models at the Max Plank Institute. After his studies, he worked on Linux kernel programming and embedded devices for telemetry applications at Intelligent Sensing Anywhere. In 2010, Oliver became a Consultant and Trainer for Fast Lane within the Synerity team, where he developed hacking trainings, and performed pentesting and incident response. In 2013, he joined Airbus Defence and Space CyberSecurity as a network defender and pentester. Since 2015 he has been working freelance as a cybersecurity consultant and trainer.
Park Suite	**29 Troubleshooting Cisco Software-Defined Access Architectures with Wireshark** With modern network infrastructures taking away from classic layer 2 topologies and mechanisms such as spanning tree, new troubleshooting methodologies are needed focusing on protocols such as LISP and VXLAN. This session

	takes a deep dive into how the call flows of the packets traverse SDA networks and how you can best leverage Wireshark to troubleshoot these scenarios. **Instructor:Josh Halley, Solutions Architect, Cisco Systems** Solution Architect working for Cisco Systems as part of the professional services organisation. I began working with Cisco in 1998 in Melbourne, Australia. Over the years I have worked and focused on various different technologies including SP, Mobility and Wi-Fi.
Tropical	**30 WiFi Security 101 (Part 2)** Brought to you by the developer of the leading Wi-Fi attack suite - Aircrack-ng, this 2-part workshop covers the basics of Wi-Fi security through hands-on exercises. We'll begin with a brief presentation of the main standard and amendments, the different types of networks, as well as the common frames encountered on Wi-Fi networks. A short hardware section will explain how to pick the right hardware. We'll then go over different types of encryption used, and learn how to attack WPA/2 PSK as well as WPA/2 Enterprise networks, finishing up with a short introduction to GPUs to speed up the cracking process, if time permits. **NOTE! Students must bring the following equipment to participate in the class (available from amazon.fr/.co.uk/.com):** **- TP-Link MR3020** **- Alfa AWUS036NHA** **Your laptop must also have the latest VMware Workstation/Fusion (15+) installed and should have 8Gb+ RAM.** Time being short, a basic knowledge of networking and Linux command line is strongly advised. Resources: https://kali.training and https://linuxjourney.com **Instructor: Thomas d'Otreppe, Author, Aircrack-ng** Thomas d'Otreppe is a wireless security researcher and author of Aircrack-ng, the most popular and complete suite of tools for WiFi network security assessments. He is an active open source developer and also created OpenWIPS-ng, and WiFiBeat. He maintains (WPE) patches for hostAPd and Freeradius to test WPA Enterprise networks security and contributes to other open sources projects. Thomas is a contributor to the WiFi stack and toolset in Backtrack Linux, which has now become Kali Linux, the de facto top choice Linux distribution for penetration testing and vulnerability assessment. He is also the author of a pro-active wireless security course, "Offensive-Security Wireless Attacks (aka WiFu)" which has been delivered to large numbers of IT Security professionals worldwide. Thomas speaks and teaches in the Americas and Europe. He is a well-known speaker at DefCon, BlackHat, DerbyCon, SharkFest, Mundo Hacker Day, BruCON and other conferences.

FRIDAY, 8 November

8:30–10:00 am

Atlantico

31 Gentlemen's Software Set for Transport Protocols Testing & Learning

In the session we'll learn how to effectively use different software tools to test TCP/UDP behavior in various network conditions. This can be helpful in many cases: application behavior testing, and OS TCP stack testing, for example.

We'll learn:
- Tools for introducing delays, packet loss, reordering (NEWT, netem and others).
- Tools for throughput / TCP internals testing (iperf3, flowgrind, ntttcp and others).

We'll investigate their advantages and drawbacks and how to get and interpret results correctly from output and Wireshark captures.

Instructor: Vladimir Gerasimov, Network Engineer, Packettrain.NET

Vladimir Gerasimov currently works as a Network Engineer for Unitop LTD - a company building networks and IP video surveillance systems for customers. He has been working in IT for more than 12 years, and 7 years ago he shifted to Network Protocol Analysis with the main focus on TCP and Application performance analysis. Vladimir runs personal blog and he is also a creator and administrator of the largest Russian-speaking group regarding Network Protocol Analysis.

Park Suite

32 Green Locks are not enough: Plaintext information in network protocols

Although encryption is becoming more and more common, there is still a great deal of plaintext information flowing in modern networks. Identifying, understanding and extracting such information from the packets can be extremely helpful to gain additional knowledge of who is using the network.

In this session, we will see how to extract plaintext information from certain network protocols to better identify the hosts and their distinguishing marks. We will go through protocols such as DNS, mDNS, LLMNR, SSDP and DHCP, discussing their usage and main features, and showing how their dissection can help unveiling names, available network services, operating systems, and other valuable data.

You'll leave this session with an understanding of how certain protocols disseminate plaintext information in the network, how to proficiently analyze them with Wireshark, and what you can do to prevent your hosts from telling everyone more than what is strictly necessary.

Instructor: Simone Mainardi, Senior Data Scientist, ntop

Simone Mainardi received his BSc, MSc and PhD degrees in Computer Science from the University of Pisa, Faculty of Information Engineering. He worked as a research associate both at the University of Pisa and at the Institute for Informatics and Telematics (IIT) of the Italian National Research Council (CNR). He is now with ntop as a Senior Data Scientist. He is interested in computer networking, parallel and distributed algorithms, Internet measurements and data analysis.

Tropical

33 Analysing VoIP Networks; Discover Wireshark's numerous features to troubleshoot VoIP

The analogue phone service is replaced more and more with Voice over Internet Protocol (VoIP) technology. While analogue phones are based on dedicated switched circuits, VoIP is using digitized and packetized transportation over data networks like Ethernet. But whereas voice traffic is less bandwidth demanding than most other applications, it is more time critical. Therefore, VoIP packets are marked with higher Quality of Service (QoS) priority, but networks designed only for large data volumes may not be capable of handling different QoS classes, which may result in poor voice quality. VoIP is using different protocols for call signalling (like SIP, Unify HFA, Alcatel UA etc.) and Real-Time Transport Protocol (RTP) for digitized voice.

This session will introduce you into Wireshark's VoIP features, which allows you to isolate signalling problems as well as voice streaming errors like jitter, packet loss, incorrect QoS settings etc.

Instructor: Rolf Leutert, Owner, Leutert NetServices

Leutert NetServices (LNS) is a small team of highly qualified network experts. For more than 20 years, we have offered trainings, troubleshooting, and consulting in protocol analyzing all over Europe. LNS was the first company to offer 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, incorporating real-world scenarios from our many years of troubleshooting experience. Rolf is a SNIFFER Certified Master (SCM) and Wireshark Certified Network Analyst (WCNA).

10:15–11:45 pm	
Atlantico	**34 LTE Explained…The Other Protocols** This session will walk attendees through multiple LTE, VoLTE, and 5G opt3x flows and failures to demonstrate how Wireshark can assist with protocols like S1AP, GTP, and Diameter. Also how to get through the large datasets that 5G produces in order to troubleshoot individual flow issues. **Instructor: Mark Stout, Mobile Network Technical Support Engineer, Sprint** Design, and Tech Support in Code Division Multiple Access (CDMA) and Long-Term Evolution (LTE) mobile networks, and now 5G for the last 21 years, in multiple countries. Active contributor to 3rd Generation Partnership Project (3GPP) 23, and 29 series. Currently the Lead Support Engineer for Sprint's LTE, Voice Over LTE (VoLTE), Internet of Things (IoT),and true 5G technology on the Packet Core network.
Park Suite	**35 Debugging TLS with Wireshark** Troubleshooting applications using HTTPS or TLS can be a pain since the application data is encrypted. When application logs or web developer tools fail to provide sufficient information, Wireshark is an invaluable tool to help analyze encrypted TLS communications. This session will walk you through the process of configuring applications and Wireshark to enable TLS decryption: 1. Configure applications (web browser or server) to provide session secrets. 2. Configure Wireshark to capture and decrypt TLS traffic. 3. Show how to embed secrets in a packet capture file for easier distribution. Given that keys and decrypted data can be sensitive, we will definitely cover security considerations and Wireshark features that can help here. We'll also demonstrate how Wireshark can be used to understand TLS 1.3, DNS-Queries-over-HTTPS (DoH), Encrypted Server Name Indication (ESNI), and QUIC. **Instructor: Peter Wu, Wireshark Core Developer** Peter Wu is part of the Crypto 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.
Tropical	**36 Automating cloud infrastructure for packet capture and analysis** As analysts, we are often required to analyze large captures containing GB/TB of network data. Analysis of captures this size can be time-consuming, require specialized (and expensive) hardware or require detailed processing using multiple tools before Wireshark is even opened. On-demand cloud services can assist in these circumstances by providing high-powered resources, but managing, configuring and using these services can be cumbersome. This talk will discuss processes, procedures, and tools an analyst can use to quickly and easily utilize cloud services in analysis efforts of large pcaps. We'll discuss the use of familiar analysis tools like tcpdump, tshark, and (of course) Wireshark in cloud environments and how best to leverage different cloud platforms and services to automate the use of these tools. Additionally, we will take a look at the new feature AWS recently released - VPC Traffic Mirroring - and how this tool aides us in cloud traffic analysis. **Instructor: Brad Palm & Ryan Richter, BruteForce** Brad is a seasoned problem solver and convergent thinker who enjoys the challenges of merging the physical and virtual worlds. As an analyst working in the cybersecurity and network efficiency domains, he focuses on network capture and analysis for enterprise networks, hunting those environments for malicious actors, testing emerging technologies and devices for customers, and utilizing captured traffic to influence developmental test scenarios. His professional interests include tinkering with open source virtualization/container/provisioning technologies, learning about effective communication skills to better teach security topics, and increasing the usability of secure information systems. Ryan Richter solves problems related to security, infrastructure, networking, applications, and organizations. He is an advocate of the scientific method and uses a variety of programming languages, network analysis tools, and Linux utilities in his daily work.