- Pre-Conference Troubleshooting Class
- SharkFest'17 Europe Agenda
- Instructor Bios
- Session Abstracts & Requirements

SharkFest'17 Europe
November 6th - 10th, 2017

Palacio Estoril
Estoril, Portugal

SharkFest'17 US Conference Agenda

Pre-Conference Course and SharkFest'17 Opening Schedule

WIRESHARK UNIVERSITY

Pre-Conference Course

Troubleshooting with Wireshark
(Laura Chappell)

Monday	6 November, 2017	
7:30 - 9:00 am	Check-in and Badge Pick up	Imperial Room
7:30 am	Breakfast	Europa Room
9:00 am	Laptop Setup and Class begins (with morning break)	Atlantico Room
12:00 pm	Lunch Break	Europa Room
1:00 pm	Class Resumes (with afternoon break)	Atlantico Room
5:00 pm	Class day ends	Dinner–see area restaurant recommendations
Tuesday	**7 November, 2017**	
7:30 am	Breakfast	Europa Room
9:00 am	Class begins (with morning break)	Atlantico Room
12:00 pm	Lunch Break	Europa Room
1:00 pm	Class Resumes (with afternoon break)	Atlantico Room
5:00 pm	Class day ends	**Attending SharkFest'17 Europe? See Tuesday Opening Schedule below**

SharkFest'17 Europe

Opening Schedule

Tuesday	7 November, 2017	
12:00-8:30 pm	***Check-In & Badge Pick-Up for SharkFest'17 Europe***	***Imperial Room***
1:00-5:00 pm	***Developer Drop-In Workshop*** ***SharkFest'17 Europe Attendees Only***	***Tropical Room***
5:00-8:00 pm	***Welcome Dinner & Sponsor Showcase Reception*** ***SharkFest'17 Europe Attendees Only***	***Europa Room***

SharkFest'17 Europe Conference Agenda

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

Wednesday	8 November, 2017		
7:00-8:30 am	**Breakfast** (Europa Room)		
7:30am-12:00 pm	**SharkFest Check-in** (Imperial Room)		
8:30-9:30 am	***Keynote: "Wireshark: Past, Present & Future" - Gerald Combs & Friends (Atlantico Room)***		
	Atlantico Room	**Park Suite Room**	**Tropical Room**
9:30-9:45 am	Break		
9:45-11:00 am	01 **Back to the Packet Trenches (Part 1)** Hansang Bae	02 **Hands-On TCP Analysis: Packets, Sequences & Fun** Jasper Bongertz	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 **Back to the Packet Trenches (Part 2)** Hansang Bae	05 **Troubleshooting WLANs (Part 1): Layer 1 & 2 Analysis Using AirPcap, Wi-Spy & Other Tools** Rolf Leutert	06 **Generating Wireshark Dissectors from XDR Files: Why you don't want to write them by hand** Richard Sharpe
12:30-1:30 pm	LUNCH		
1:30-2:45 pm	07 **The Packet Doctors are In!** Drs. Bae, Bongertz, Landström, Blok	08 **Troubleshooting WLANs (Part 2): Layer 1 & 2 Analysis Using AirPcap, Wi-Spy & Other Tools** Rolf Leutert	09 **Developer Bytes Lightning Talks–Development Track** Wireshark Core Developers
2:45-3:00 pm	Break		
3:00-4:15 pm	10 **SMB/CIFS Analysis: Using Wireshark to Efficiently Analyze & Troubleshoot SMB/CIFS** Betty DuBois	11 **Real World Troubleshooting Tales** Graeme Bailey	12 **Developer Bytes Lightning Talks–Usage Track** Wireshark Core Developers
4:15-4:30 pm	Break		
4:30-5:45 pm	13 **SMB Handshake: The Devil Lies in the Detail** Eduard Blenkers	14 **Practical Tracewrangling: exploring trace file manipulation/extraction scenarios** Jasper Bongertz	15 **SSL/TLS Decryption: uncovering secrets** Peter Wu
6:00-8:00 pm	***Sponsor Technology Showcase Reception, Treasure Hunt & Dinner (Europa Room)***		

Pick up your Packet Challenge Sheet at the WIRESHARKUNIVERSITY table in the Europa Room

SharkFest'17 Europe Conference Agenda

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

Thursday	9 November, 2017			
7:00-8:30 am	**Breakfast** (Europa Room)			
8:30am-9:30am	**SharkBytes*** (Atlantico Room)			
	Atlantico Room	**Park Suite Room**	**Tropical Room**	
9:30am–9:45 am	Break			
9:45am-11:00 am	16 **Using Wireshark to Solve Real Problems for Real People: Step-by-Step Case Studies in Packet Analysis** Kary Rogers	17 **Augmenting Packet Capture with Contextual Meta-Data: the What, Why & How** Dr. Stephen Donnelly	18 **extcap - Packet Capture beyond libpcap/winpcap: Bluetooth sniffing, Android dumping & other fun stuff** Roland Knall	**Visit the Vendor Showcase in the Europa Room**
11:00–11:15 am	Break			
11:15am–12:30 pm	19 **TCP Today: Packet-Level Review of Recent Improvements to Windows Operating Systems** Simon Lindermann & Christian Landström	20 **QUIC Dissection: Using Wireshark to Understand QUIC Quickly** Megumi Takeshita	21 **Introduction to ICS Protocols** Thomas Bringevald	
12:30 –1:30 pm	LUNCH			
1:30–2:45 pm	22 **Troubleshooting Layer 7 with Wireshark: because you don't know what you don't know** Betty DuBois	23 **The Network is Slow! Finding the Root Cause of Slow Application Performance** Lorna Robertshaw	24 **Designing a Requirements-based Packet Capture Strategy** John Pittle	
2:45–3:00 pm	Break			
3:00–4:15 pm	25 **Hands-On Analysis of Multi-Point Captures** Christian Landström	26 **Troubleshooting 802.11 with Monitoring Mode: Finding Patterns in your pcap** Thomas Baudelet	27 **Developer Bytes Lightning Talks–Development Track** Wireshark Core Developers	
4:15–4:30 pm	Break			
4:30–5:45 pm	28 **Transmission Control Protocol Illustrated: everything you always wanted to know about TCP* (*but were afraid to ask)** Ulrich Heilmeier	29 **Slow Start & TCP Reno Demystified: How Congestion Avoidance Modes are Working** Christian Reusch	30 **Developer Bytes Lightning Talks–Usage Track** Wireshark Core Developers	
6:00–8:00 pm	***Sponsor Showcase, Packet Palooza Dinner & Reception (Europa Room)***			

* **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'17 Europe Conference Agenda

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

Friday 10 November, 2017			
7:00-8:30 am	**Breakfast** (Europa Room)		
	Atlantico Room	**Park Suite Room**	**Tropical Room**
8:30–9:45 am	31 **New Ways to Find the Cause of Slow Response Times** Paul Offord	32 **Wireshark & Time: Accurate Handling of Time when Capturing Frames** Werner Fischer	33 **TShark Command Line using PowerShell** Graham Bloice
9:45 –10:00 am	Break		
10:00–11:15 am	34 **Turning Wireshark into a Traffic Monitoring Tool: Moving from packet details to the big picture** Luca Deri	35 **How Did They Do That? Network Forensic Case Studies** Phill Shade	36 **Using LUA to write a Simple Dissector to assist in Troubleshooting a Proprietary Protocol** Sake Blok
11:15–1:00 pm	***Wrap-up, Packet Challenge Awards & Lunch***		

SharkFest'17 Europe Bios & Abstracts

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

WEDNESDAY, 8 NOVEMBER

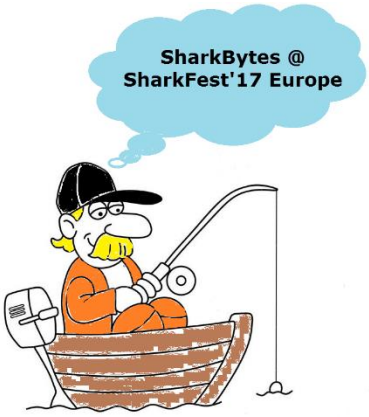
8:30–9:30 am	**Keynote: The Past, Present & Future of Wireshark** **Gerald Combs & Company**
9:45-11:00 am	
Atlantico	**01 Back to the Packet Trenches (Part 1)** In an increasingly prevalent cloud and Saas-based networking world, foundational troubleshooting practices are destined to change. In this 2-part session, Hansang will review on and off-prem cloud and SaaS troubleshooting scenarios when trying to identify root cause. He'll also discuss what it will be like as you adopt the cloud, how to capture in AWS, and how different cloud vendors may or may not have TCP/IP Offload Engines to address latency issues when uploading. He'll also show how one-sided traces to a SaaS vendor can be diagnosed. **Instructor: Hansang Bae, CTO, Riverbed Technology** 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 has since taken on the role of Chief Scientist and then CTO for the company. With his broad knowledge of protocol analysis in a complex enterprise infrastructure, Hansang brings a unique perspective to packet analysis.
Park Suite	**02 Hands-On TCP Analysis: Packets, Sequences & Fun** In this session, you'll work through a series of short but interesting sample TCP traces that will be distributed to participants prior to the beginning of the conference, giving you a chance to work and familiarize yourself with them before the group walkthrough, review and Q&A. The capture files will be made available at least 2 weeks before the conference starts at the following URL: https://blog.packet-foo.com/sharkfest-2017-hands-on-files/ **Instructor: Jasper Bongertz, Sr. Technical Consultant, Airbus DS CyberSecurity** Jasper Bongertz started working freelance in 1992 while 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 special emphasis on Wireshark and network hacking. In 2013, he joined Airbus Defence and Space CyberSecurity, concentrating on IT security, Incident Response and Network Forensics. 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.
Tropical	**03 Writing a Wireshark Dissector: 3 Ways to Eat Bytes** The presentation outlines the 3 most popular methods to write 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	
Atlantico	**04 Back to the Packet Trenches (Part 2)** In an increasingly prevalent cloud and Saas-based networking world, foundational troubleshooting practices are destined to change. In this 2-part session, Hansang will review on and off-premises cloud and SaaS troubleshooting scenarios when trying to identify root cause. He'll also discuss what it will be like as you adopt the cloud, how to capture in AWS, and how different cloud vendors may or may not have TCP/IP Offload Engines to address latency issues when uploading. He'll also show how one-sided traces to a SaaS vendor can be diagnosed. **Instructor: Hansang Bae, CTO, Riverbed Technology** 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 has since taken on the role of Chief Scientist and then CTO for the company. With his broad knowledge of protocol analysis in a complex enterprise infrastructure, Hansang brings a unique perspective to packet analysis.

Park Suite	**05 Troubleshooting WLANs (Part 1): Layer 1 & 2 Analysis using AirPcap, Wi-Spy & Other Tools** 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 support staff. Various issues like physical layer interference 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 introduce you to techniques on how to approach Layer 1 and 2 WLAN problems using Wireshark, AirPcap, and Wi-Spy. All these tools will be demonstrated live and Wireshark will be customized with a specific profile to analyze different WLAN problems more efficiently. Also, the function of the important pseudo-headers "Radio Tap" and "Per Packet Information" (PPI) and the valuable information available from these fields will be explained. Trace files from real-life problem situations will be used during the session to illustrate the above topics. **Instructor: Rolf Leutert, Owner, Leutert NetServices** Rolf Leutert is a SNIFFER Certified Master (SCM) and Wireshark Certified Network Analyst (WCNA). 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 analysis 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-based, incorporating our many years of troubleshooting experience
Tropical	**06 Generating Wireshark Dissectors from XDR Files: Why you don't want to write them by hand** In any development environment where protocols are specified with a language (XDR, e.g.), having the ability to automatically generate a Wireshark dissector from your protocol specifications is an enormous benefit. Developers can immediately see whether or not their code is correct and quickly figure out where they have gone wrong. Support staff can also use the resulting dissectors as another troubleshooting aid in the field. The author developed a dissector generator for XDR-based protocols (his second, as the original SMB dissector was generated) and then rewrote the XDR dissector generator based on experience gained. This presentation will look at how to integrate a generator into the Wireshark build as well as some of the techniques used in generating such dissectors and the lessons learned from the whole exercise. It will also discuss why he rewrote the generator. **Instructor: Richard Sharpe, Principal Software Engineer, Primary Data & Wireshark Core Developer** Richard Sharpe is an open source software developer who has written a number of Wireshark dissectors. He has also contributed to the Samba project.
1:30-2:45 pm	
Atlantico	**07 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: Dr. Bae, Dr. Bongertz, Dr. Landström, Dr. Blok**
Park Suite	**08 Troubleshooting WLANs (Part 2): Layer 1 & 2 Analysis using AirPcap, Wi-Spy & Other Tools** This session is the continuation of Part 1 and will explain the function of 802.11 management & control frames (like Beacon, Probe request/response, RTS/CTS, and many more) These frames play an important role in the correct functioning of every WLAN. Profound knowledge of the different processes and using these frames to control 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-life problem situations will be used during the session to illustrate topics presented. **Instructor: Rolf Leutert, Owner, Leutert NetServices** Rolf Leutert is a SNIFFER Certified Master (SCM) and Wireshark Certified Network Analyst (WCNA). 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 analysis 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 Zurich Insurance). The trainings are very practice-based, incorporating our many years of troubleshooting experience.

Tropical	**09 Developer Bytes Lighting Talks–Developer Track** Developer Bytes Lightning Talks focus on small, interesting topics regarding Wireshark, its development, and use cases. We will present a look behind the curtains, highlight features often overlooked, or present upcoming topics for future versions of Wireshark. This development track focuses on the following topics regarding the development of Wireshark: - Wireshark Git and CMake navigation - From protocol to dissector in 15 minutes - Make a company-internal build - Packet generation, prepare dummy data **Instructors: Wireshark Core Developers**
3:00-4:15 pm	
Atlantico	**10 SMB/CIFS Analysis: Using Wireshark to Efficiently Analyze and Troubleshoot SMB/CIFS** SMB/CIFS is a ubiquitous protocol whether we like it or not. Being able to understand the inner workings is critical to performance monitoring and troubleshooting the file transfer protocol used by Microsoft and Samba. This session will cover the SMB implementation used by Server2012/2016 and Windows 8.1/10. Trace files will be made available during the session so attendees may follow along in Wireshark. Service Response times and LOAD in I/O Graphs will be covered. **Bring your laptops!** **Instructor: Betty DuBois, Chief Detective, Network Detectives** Betty DuBois is the Chief Detective for Network Detectives. She has been analyzing networks since 1997, performing fault isolations, application profiles, and network baselines for a wide variety of clients. As an Instructor for Wireshark University, she is known for her ability to make a dry, complex subject fun and interesting by using both humor and real-world examples. Betty has presented at Sharkfest and Networld+Interop and for the Atlanta chapters of HTCIA and ISSA. Her "Network Mystery" series can be found at www.wireshark.org/docs. Betty's industry certifications include Certified Wireshark University Instructor, Wireshark Certified Network Analyst, HP ProCurve AIS, and Sniffer Certified Expert.
Park Suite	**11 Real World Troubleshooting Tales** In this session, I'll share some of the real world troubleshooting cases I've engaged in recently. These can range from small networks suffering from poorly-written applications to large global systems with thousands of servers, to virtualised environments both server and desktop, to Cloud-hosted systems like AWS, and beyond. My troubleshooting is end-to-end from the user to the storage and everything in between. I'll explain some of the methodologies I've developed and how I approach complex systems and hard-to-diagnose problems. I use Wireshark as a first line tool nearly every day and know it is the fastest way to prove root cause, not just surmise what the problem may be. There will be plenty of tips and useful insights to take away as well as sharing experiences. **Instructor: Graeme Bailey, Troubleshooter & Founder, TARCA** Graeme is a UK-based troubleshooter with nearly 40 years' experience in all aspects of system and infrastructure, having worked for Burroughs, HP, 3Com and others. He founded TARCA (Troubleshooting And Root Cause Analysis) in 2008, having identified a clear need for an independent consultancy firm with the capability to address end-to-end performance. Taking network analysis further than the network itself, TARCA encompasses applications, workstations, servers, storage, networks and connectivity to provide a unique, unbiased insight into issues. TARCA helps resolve problems for their clients more rapidly, often bringing together a wide variety of third parties and gaining agreement as to the precise cause of the issue. This maximises productivity potential for both people and equipment, often resulting in huge savings through the improvements they make together.
Tropical	**12 Developer Bytes Lighting Talks–Usage Track** Developer Bytes Lightning Talks focus on small, interesting topics regarding Wireshark, its development and use cases. We want to present a look behind the curtains and highlight some features often overlooked or present upcoming topics for future versions of Wireshark. This usage track focuses on the following topics regarding the development of Wireshark: - Get up and running with SSL dissection - Extraction of Images/Data - USB Pcap - Practical Jokes **Instructors: Wireshark Core Developers**

4:30-5:45 pm	
Atlantico	**13 SMB Handshake - The Devil Lies in the Detail: A close look at selected bits in SMB2 & SMB3 messages** Several messages have to be exchanged between client and server before a client can access a file over SMB. Only after details about the SMB dialect, the user-id, and the share have been exchanged is the file ready to use. This presentation will highlight selected details that influence the performance and available features in the ever-increasing number of SMB dialects or versions. The behavior of clients & servers running Windows is controlled through registry entries, group policy options and certain flags specified by the application programmer. Where applicable, the presentation will show the influence various configurable parameters have on performance. Expect to see the Group Policy editor side-by-side with Wireshark to translate your findings from network analysis into a configuration change and, hopefully, the correct solution. **Instructor: Eduard Blenkers, Sr. Network Consultant** Eduard "Eddi" Blenkers has analyzed countless networks and applications - often teaming up with Jasper Bongertz. Most analysis projects dumped SMB in his lap. The background in computer and network forensics often helped to link network packets to computer settings or misbehaving applications. Eddi is currently working in an incident response team chasing Windows-based malware.
Park Suite	**14 Practical Tracewrangling: Exploring Capture File Manipulation/Extraction Scenarios** Sometimes, scrolling through the packet list while filtering and inspecting the packet decodes in Wireshark isn't the right thing to do at the beginning. When the amount of packets becomes overwhelming, you need a strategy to reduce the haystack to a smaller pile you can work with without getting lost all the time. This is where Tracewrangler can help a lot, offering various extraction techniques. While Wireshark is capable of reading almost any kind of network packet or frame you throw at it, some other tools may not be that versatile. Sometimes, link layer types like Linux Cooked Capture (SLL), tunneling layers or MPLS shims make it impossible to process capture with your favorite tool because it doesn't understand those layers. Tracewrangler can help, modifying your capture files in an adaptive way without breaking layer relationships. **Instructor: Jasper Bongertz, Sr. Technical Consultant, Airbus Defence & Space CyberSecurity** Jasper Bongertz is a Senior Technical Consultant for Airbus Defence and Space CyberSecurity. He started working freelance in 1992 when he began studying computer science at the Technical University of Aachen, eventually moving to Airbus to focus on IT security, Incident Response and Network Forensics.
Tropical	**15 SSL/TLS Decryption: uncovering secrets** Troubleshooting and debugging applications or reverse engineering protocols that use SSL/TLS can be a pain since the data is encrypted. Decryption of such data is possible in Wireshark if you have access to the appropriate secrets. This session will show you how to obtain the required secret information and give a background on the relevant TLS handshake details. You will understand why possession of the server RSA key file is not always sufficient and what alternatives are available. Once decrypted data is available, you will finally be able to make use of several Wireshark and Tshark features to help you with analysis. **Instructor: Peter Wu, Wireshark Core Developer** Peter Wu is a Masters student in Information Security at the Eindhoven University of Technology, and contributor to many open source projects. His contribution to Wireshark started in 2013 with SSL decryption fixes. As Software Developer at Code Yellow, he helped in developing a VoIP product.

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



Submit a SharkByte!

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.php.

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

THURSDAY, 9 NOVEMBER

8:30–9:30 am	SharkBytes (Atlantico)
9:45-11:00 am	
Atlantico	**16 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	**17 Augmenting Packet Capture with Contextual Meta-Data: the what, why & how** Full packet capture and archiving are increasingly important, providing 'ground truth' evidence for investigating security incidents and performance issues. But captured packets by themselves lack context–such as where they were captured and the environment at the time of capture. Augmenting packet data with meta-data can provide useful context about when, where, and how packets were captured and the environment at the time of capture. This presentation will discuss what types of meta-data can be useful, what they can be useful for, and how meta-data can be encoded into packet capture data to ensure permanent context to packets captured. **Instructor: Dr. Stephen Donnelly, CTO, Endace** Stephen has worked on packet capture and timestamping systems for 20 years, receiving his PhD on "High Precision Timing in Passive Measurements of Data Networks" from the University of Waikato, New Zealand. A founding employee at 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 to solve unique problems. Stephen is a contributor to the Wireshark, libpcap, Argus and Suricata open source projects.
Tropical	**18 extcap-Packet Capture beyond libpcap/winpcap: Bluetooth sniffing, Android dumping & other fun stuff** The presentation focuses on extcap - the external capture interface for Wireshark, and its application in modern-day scenarios. It will demonstrate the capabilities of extcap and how to write its own utility with Python and C-code. Furthermore we are going to demonstrate Bluetooth sniffing capabilities as well as dumping of log files from an Android phone and some new debugging techniques for dissector development. **Instructor: Roland Knall, Wireshark Core Developer** Roland is a Software System Architect for machine safety protocols at B&R Industrial Automation, a division of ABB. He started developing software some 20 years ago and has seen nearly all parts of software development, but focusing the last 10 years on industrial machine applications and mainly on systems in the area of industrial ethernet. He has been a Core Developer of Wireshark since 2016 and focuses mainly on the integration of external capture devices as well as UI improvements.
11:15 am–12:30 pm	
Atlantico	**19 TCP Today: Packet-Level Review of Recent Improvements to Windows Operating Systems** Windows 10 and Windows Server 2016 users can expect performance improvements in TCP-based communications used to connect IoT devices to cloud-backend services and data. In conjunction with the Windows 10 development roadmap, new TCP features will or have been rolled out, including: 1. TCP Fast Open (TFO) for zero RTT TCP connection setup. IETF RFC 7413 2. Initial Congestion Window 10 (ICW10) by default for faster TCP slow start 3. TCP Recent ACKnowledgment (RACK) for better loss recovery (experimental IETF draft) 4. Tail Loss Probe (TLP) for better Retransmit TimeOut response (experimental IETF draft) 5. TCP LEDBAT for background connections IETF RFC 6817. This session will provide an overview of these TCP improvements by looking into them at the packet level. **Instructors: Simon Lindermann, Network Engineer, Miele & Cie. KG & Christian Landström, Sr. Consultant, Airbus DS CyberSecurity**

Park Suite	**20 QUIC Dissection: Using Wireshark to Understand QUIC Quickly** QUIC (Quick UDP Internet Connection) is an essential protocol in today's internet. You've already used QUIC if you've googled something, and Wireshark has recently added a new QUIC dissector. In this presentation, Megumi explains the details of QUIC, and shows you how to understand the protocol and mechanisms involved. Using sample trace files,Megumi will show how to inspect and visualize QUIC traffic and explain the advantage of QUIC in comparison with other protocols too. **Instructor: Megumi Takeshita, Packet Otaku and Owner, Ikeriri Network Service** Megumi Takeshita, or Packet Otaku (Twitter: @ikeriri) runs a packet analysis company, Ikeriri Network Service, after having worked at BayNetworks and Nortel Networks in Japan. Ikeriri concerns packet analysis for troubleshooting, debugging and security inspection. Ikeriri is also a reseller of many wired/wireless capture and analysis devices and software for Riverbed, Metageek, Profitap, Dualcomm etc. Megumi has authored 10+ books about Wireshark and packet analysis in Japanese and she is one of contributors to the Wireshark project too.
Tropical	**21 Introduction to ICS Protocols** With the internet of things, industrial control systems become more and more connected (similar to normal IT systems 40 years ago). Much like them, ICS protocols experience problems regarding authentication and encryption. This session will be an introduction to those protocols and their issues. Along with a general overview of ICS protocols, a few specific ones will be picked out to show the variety of simple to redesigned and improved protocols. **Instructor: Thomas Bringewald, IT Engineer & Lars Siefert, IT/CyberSecurtiy, Airbus Group** While completing his Bachelors' degree in Computer Science Thomas Bringewald found a connection with IT security, which led to a Masters' degree in network and information security. While working as a security engineer, he designed and implemented security concepts for endpoint and network perimeter security. His area of focus was ICS networks, requiring him to take the special requirements of ICS and SCADA into account.
1:30–2:45 pm	
Atlantico	**22 Troubleshooting Layer 7 with Wireshark: because you don't know what you don't know** If the world were perfect, we would have the time to analyze each different application used in our environment. However in the real world, we are firefighters. This session is designed to equip you with the tools necessary to contain the fire when it starts. We will use Wireshark to isolate common problems in all applications; slow response, no response, and error response. You will walk away with the knowledge necessary to get the following applications under control; HTTP/s, DNS, SMB2/3, LDAP, Citrix, Oracle, MS SQL, and Diameter. Analysis of critical fields of each protocol will help you avoid getting burned. **Please bring your laptop, this will be a Hands-On session.** **Instructor: Betty DuBois, Chief Detective, Network Detectives** Betty DuBois is the Chief Detective for Network Detectives. She has been analyzing networks since 1997, performing fault isolations, application profiles, and network baselines for a wide variety of clients. As an Instructor for Wireshark University, she is known for her ability to make a dry, complex subject fun and interesting by using both humor and real-world examples. Betty has presented at Sharkfest and Networld+Interop and for the Atlanta chapters of HTCIA and ISSA. Her "Network Mystery" series can be found at www.wireshark.org/docs. Betty's industry certifications include Certified Wireshark University Instructor, Wireshark Certified Network Analyst, HP ProCurve AIS, and Sniffer Certified Expert.
Park Suite	**23 The Network is Slow! Finding the Root Cause of Slow Application Performance** Packet analysis is often used to figure out why users are experiencing poor performance with an application. The root cause may be a network problem, but often the problem is instead a slow server, a timeout, or inefficient application behavior. It can be very challenging to search through large packet traces to figure out where the delays are happening and why. This session first covers how to use Wireshark to quickly look for some common "smoking guns" that often cause poor performance. It then discusses how to determine the causes of delay for any TCP traffic, as well as for some common application protocols, including HTTP. Lastly, it covers some ways to use Wireshark and other tools to share your findings in a way that is helpful to colleagues who aren't as familiar with packets and network protocols - and prove that your findings are correct. **Instructor: Lorna Robertshaw** Lorna Robertshaw spent the last 16 years working for OPNET and Riverbed as a sales engineer and subject matter expert on performance management solutions. She has always enjoyed the challenge of using packet traces to troubleshoot application and network performance problems and solve mysteries for her customers. Lorna is now taking on these same challenges as an independent contractor, using her extensive experience with Wireshark, along with Riverbed's Packet Analyzer and Transaction Analyzer, to provide packet analysis and other performance management services. Lorna earned a BSc in Computer Science at the University of Virginia. She also enjoys rock climbing, video games, and hiking.

Tropical	**24 Designing a Requirements-based Packet Capture Strategy…and how it fits into an overall performance visibility strategy** Learn how to create a requirements-based packet capture strategy for your organization. Understand how packets are a cornerstone to your performance management capabilities and how to create a roadmap that you can use to communicate priorities and performance management capabilities that bring value to the business. **Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.** Actively focused on Performance Engineering for networks, systems, and applications since the early 90s, performance troubleshooting is my passion and joy. I've used NG Sniffer, HP Network Advisor, Ethereal, Wireshark, NetShark, AppResponse, Packet Analyzer, Transaction Analyzer, IT Guru, and the list goes on... Sr. Performance Consultant with OPNET Technologies since 2005, then came to Riverbed with the OPNET acquisition in 2012. Promoted to Distinguished Performance Consultant in 2015 reflecting expertise in the entire portfolio of Riverbed visibility and analysis products, as well as technical leadership within the consulting practice for complex customer engagements.
3:00–4:15 pm	
Atlantico	**25 Hands-On Analysis of Multi-Point Captures** This talk focuses on multipoint capture file analysis and packet matching from different capture points to take you on the challenging journey of analyzing performance issues throughout a whole network path. Load balancers, firewalls, proxy servers might be involved, and finding the right spot to analyze the problem is not always an easy task. **This will be an interactive session with live analysis, so bring your Wireshark and join the fun!** **Instructor: Christian Landström, Senior Consultant, Airbus DS CyberSecurity** Christian Landström has worked in IT since 2004, with a strong focus on network communications and IT security. After graduating in computer science in 2008, Christian joined Synerity Systems and then moved with the whole Synerity team to work for Fast Lane GmbH in 2009 as a Senior Consultant for network analysis and security. Since 2013, Christian has worked as a Senior Consultant for Airbus Defence and Space CyberSecurity focusing on IT security, Incident Response and Network Forensics.
Park Suite	**26 Troubleshooting 802.11 with Monitoring Mode: Finding Patterns in your pcap** This talk will present the basics of 802.11 protocol and the challenges of Wi-Fi packet captures compared to Ethernet. We'll answer many questions you'll face when analyzing a Wi-Fi network, such as: What are the different capture method options? Why are packets missing in my traces? How can I capture 802.11n/802.11ac? And more. We'll then present a methodology and practical examples to answer the ultimate question: Why is my Wi-Fi slow? **Instructor: Thomas Baudelet, Network & Security Analyst, iwaxx Sarl** After graduating as an engineer in 2003, Thomas worked for 3 years for Alcatel-Lucent as an integrator of GPRS services for national telecom operators in countries such as Russia, Nigeria, Egypt, United Arab Emirates, Thailand, Yemen, Togo, & Sri Lanka. In 2006, he joined the Geneva University Hospitals network team and worked on network and security technologies, including firewalls, VPNs, routing, administration of a public class B network, wireless, PKI, load balancers, and VoIP. He also set up the actual WLAN architecture: 1,800 Access Points with PKI authentication. In 2010, he created his own company, iwaxx Sarl, and since then has been offering his services in troubleshooting, network analysis, integration and training to private banks, public organizations, and international organizations. Thomas is the creator and main developer of Debookee, an OS X network analyzer that uses Wireshark at its core level for Ethernet and Wi-Fi monitoring captures.
Tropical	**27 Developer Bytes Lighting Talks–Development Track** Developer Bytes Lightning Talks focus on small, interesting topics regarding Wireshark, its development, and use cases. We will present a look behind the curtains, highlight features often overlooked, or present upcoming topics for future versions of Wireshark. This development track focuses on the following topics regarding the development of Wireshark: - Wireshark Git and CMake navigation - From protocol to dissector in 15 minutes - Make a company-internal build - Packet generation, prepare dummy data **Instructors: Wireshark Core Developers**

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

4:30–5:45 pm	
Atlantico	**28 Transmission Control Protocol Illustrated: everything you wanted to know about TCP* (*but were afraid to ask)** In this hands-on lab, you'll have a look at some nice captures to discover all the common features of TCP. We'll see how sequence numbers are handled, the difference between Fast Retransmit and Retransmit, how latency and windows size affects the maximum throughput, and so on. This knowledge may help with application and performance troubleshooting. **To take part in this lab you should be full of curiosity and have a current Wireshark installation with you.** **Instructor: Ulrich Heilmeier, Network Architect, Krones AG** Uli Heilmeier has been a network protocol enthusiast for years. He believes in RFCs and sharing knowledge. Hunting packets is one of his favorite occupations while working as a network engineer at a German machine manufacturer.
Park Suite	**29 Slow Start & TCP Reno Demystified: How Congestion Avoidance Modes are Working** This presentation will demonstrate, on a real-world case basis, how congestion avoidance algorithms and slow start work, and how they influence the performance of a session in a significant way. It will also explain how TCP Reno works, what triggers entry in these congestion avoidance modes and the following mechanisms: cwnd, ssthresh, receive window, SACK, Duplicate ACK. Tool demonstrations will include Wireshark. **Instructor: Christian Reusch, Network Engineer 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 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.
Tropical	**30 Developer Bytes Lighting Talks–Usage Track** Developer Bytes Lightning Talks focus on small, interesting topics regarding Wireshark, it's development and use cases. We want to present a look behind the curtains and highligh some features often overlooked or present upcoming topics for future versions of Wireshark. This usage track focuses on the following topics regarding the development of Wireshark: - Get up and running with SSL dissection - Extraction of Images/Data - USB Pcap - Practical Jokes **Instructors: Wireshark Core Developers**

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

FRIDAY, 10 November

10:00–11:15 am

Atlantico

31 New Ways to Find the Cause of Slow Response Times

Higher speeds, greater data volumes, increased system complexity and the widespread use of encryption are making it increasingly difficult to find the cause of intermittent response time problems. In this presentation we look at how new Wireshark features can help, and how we can upcycle other trace and log data to gain complete visibility.

Instructor: Paul Offord, CTO, TribeLab

Paul is the founder of TribeLab, a division of the IT troubleshooting company, Advance7. Through its community website, tools and publications, TribeLab helps support engineers use advanced diagnostic techniques to solve IT problems.

Park Suite

32 Wireshark and Time: Accurate Handling of Timing when Capturing Frames

Sometimes an analysis task requires accurate handling of timing in capturing frames. Also, NTP and IEEE 1588 PTPv2 (Precision Time Protocol) are the most widely used time protocols for network synchronization. These standard protocols are used for time synchronization networking systems with accuracies ranging from micro to milliseconds, depending on different network environments. In this presentation, we will dig into problems rooted in time symptoms. Wireshark configuration profiles, display filters, and color rules can provide specific focus when you troubleshoot time issues.

Instructor: Werner Fischer, Principal Networking Consultant, avodaq AG

Werner Fischer is 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.

Tropical

33 TShark Command Line using PowerShell

Topics to be covered include:

- PowerShell, an introduction
- Using Tshark with PowerShell
- Converting *nix commands
- Advanced PowerShell functionality

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.

11:15–1:00 pm

Atlantico

34 Turning Wireshark into a Traffic Monitoring Tool: Moving from packet details to the big picture

Wireshark is a packet sniffer and analyser designed to dissect packets and provide packet-level statistics. As it provides many low-level counters and metrics, it's a great solution for problems that have been already partially identified and need to be solved at packet level. Unfortunately it is not always possible to see problems without being able to analyse traffic from a more abstracted layer - in particular in high-speed networks and large enterprises. Typical questions include "what DNS is used by local hosts?", "is anybody using Tor" and thus potentially hiding sensitive information? This talk covers in detail some open-source scripts and libraries that the author has integrated in Wireshark in order to extend it and make it suitable for traffic monitoring. This for providing users more information about the network traffic they are analysing, thus easing the iterative process of drill down to packet level where Wireshark is the ultimate tool to use.

Instructor: Luca Deri, Founder & Leader, ntop Project

Luca Deri is the leader of the ntop project (www.ntop.org), aimed at developing an open-source monitoring platform for high-speed traffic analysis. He worked for University College of London and IBM Research prior to receiving his PhD at the University of Berne with a thesis on software components for traffic monitoring applications. Well known in the open-source and Linux community, he currently shares his time between the ntop project and the University of Pisa where he has been appointed as lecturer for the CS department.

Park Suite	**35 How Did They Do That? Network Forensic Case Studies** The ringing of the phone heralds the news that every Network Security Professional dreads; "I think the network was hacked". Suddenly you are faced with answering questions you hoped never to encounter: 1. Who was the intruder? 2. How did the intruder penetrate your security precautions? 3. What damage has been done - Did the intruder leave anything such as a new user account, a Trojan horse or perhaps some new type of Worm or Bot software behind? 4. Did you capture sufficient data to analyze and reproduce the attack and verify the fix will work? This session will demonstrate how to use Wireshark to find answers and prepare you for the eventuality of being hacked. **Instructor: Phill Shade, Owner, Merlion's Keep Consulting** Bio - 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.
Tropical	**36 Using LUA to write a Simple Dissector to assist in Troubleshooting a Proprietary Protocol** In this session, Sake will demonstrate how to write a dissector to help troubleshooting proprietary protocols using real-life examples. Come to this session to learn more about LUA development in a real-world setting. **Instructor: Sake Blok, Packet Analyst, SYN-bit** Sake has been analyzing packets since the end of the last century. Over the years, he's uncovered device bugs from multiple vendors and presented his findings to the vendors to fix issues. He's also discovered many misconfiguration on customer networks that have led to functional or performance problems with applications running over the network and provided resolutions through reports presented to his customers. In 2009, Sake started the company SYN-bit to provide Network Analysis services to enterprises across Europe. In the course of his work, Sake started developing extra functionality for Wireshark that he missed in his day-to-day job. He also enhanced multiple protocol dissectors to suit his analysis needs. In 2007 he was asked by Gerald to join the Wireshark Core Development team