SharkFest'18 EUROPE
October 29th – November 2nd, 2018

THE
IMPERIAL RIDING SCHOOL
VIENNA
A RENAISSANCE HOTEL

- Pre-Conference Class Schedule
- SharkFest'18 EUROPE Session & Events Agenda
- Session Abstracts & Requirements
- Instructor Bios

SharkFest'18 EUROPE Conference Agenda

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

Pre-Conference Course and SharkFest'18 EUROPE Opening Schedule

WIRESHARK UNIVERSITY Pre-Conference Class **Troubleshooting with Wireshark** **(Rechte Pirouette)**	**Monday**	**29 October 2018**
	8:00-9:00am	Troubleshooting Class Check-in & Badge Pick up
	9:00am-12:00pm	Troubleshooting Class in session (with morning breaks)
	12:00-1:00pm	LUNCH (Class Attendees only)
	1:00-5:00pm	Troubleshooting Class in session (with afternoon breaks)
	Tuesday	**30 October 2018**
	9:00am-12:00pm	Troubleshooting Class in session (with morning breaks)
	12:00-1:00pm	LUNCH (Class Attendees only)
	1:00-5:00pm	Troubleshooting Class in session (with afternoon breaks)
		Attending SharkFest'18 Europe? See Tuesday Opening Schedule below

SharkFest'18 EUROPE Welcome Dinner (Conference Center Foyer)	**Tuesday**	**30 October 2018**
	5:00-8:30 pm	**SharkFest'18 EUROPE Check-In & Badge Pick-Up** (Registration Table, 2nd Floor Stair Foyer)
	6:00-8:30pm	***SharkFest'18 EUROPE Welcome Dinner & Sponsor Showcase*** **SharkFest'18 EUROPE Attendees Only**

Breakfast is included on Monday and Tuesday with any Imperial Riding School Hotel room reservation booked through the SharkFest'18 EUROPE Lodging site link. Those not staying at the hotel or booking rooms separately from the SharkFest room block link pay €28 for a full buffet in the Booromaeus Restaurant, should they choose to breakfast there.

SharkFest'18 EUROPE BIOS & ABSTRACTS

Wednesday	31 October 2018		
7:30-8:30am	**Breakfast – Borromaeus Restaurant***		
7:30am-12:00pm	**SharkFest Check-in & Badge Pick-up (2nd Floor Stair Foyer)**		
8:30-9:30am	***Keynote: "20 Years of Code & Community" Gerald Combs & Friends (Pirouette)***		
	Pirouette	**Grosse Reitschule**	**Kleine Reitschule**
9:30-9:45am	Break		
9:45-11:00am	01 **Back to the Basics** Hansang Bae	02 **802.11n/ac: complexity & solutions in capturing MIMO traffic** Thomas d'Otreppe	03 **Writing a Wireshark Dissector: 3 ways to eat bytes** Graham Bloice
11:00-11:15am	Break		
11:15am-12:30pm	04 **Back to the Trenches** Hansang Bae	05 **Handcrafted Packets: build network packets with Scapy** Uli Heilmeier	06 **Using More of the Features of Wireshark to Write Better Dissectors** Richard Sharpe
12:30-1:30pm	**LUNCH & LEARN (Levade, Courbette, Capriole, Croupade Rooms)**		
1:30-2:45pm	07 **TCP - Tips, Tricks, & Traces** Chris Greer	08 **Packet Analysis in the Cloud** Matthew York	09 **Crash Course: IPv6 and Network Protocols** Johannes Weber
2:45-3:00pm	Break		
3:00-4:15pm	10 **The Unusual Suspects: open source tools for enhancing big data & network forensics analysis** Jasper Bongertz	11 **IoT – Buy and Install your own Destruction! (Part 1)** Phillip Shade	12 **Slow start and TCP Reno demystified: How congestion avoidance modes can influence a session** Christian Reusch
4:15-4:30 pm	Break		
4:30-6:00pm	13 **Wireshark CLI Tools & Scripting** Sake Blok	14 **IoT – Buy and Install your own Destruction! (Part 2)** Phillip Shade	15 **TLS 1.2/1.3 and Data Loss Prevention** Ross Bagurdes
6:00-8:30pm	***Sponsor Technology Showcase Reception, Treasure Hunt & Dinner (Conference Center Foyer)***		

MENTORING & SPONSOR VIRTUAL TECHNOLOGY LABS – PIROUETTE LOBBY

***Breakfast is included with any Imperial Riding School Hotel room reservation booked through the SharkFest'18 EUROPE Lodging site link. Those not staying at the hotel or booking rooms separately from the SharkFest room block link pay €28 for a full buffet in the Booromaeus Restaurant, should they choose to breakfast there.**

SharkFest'18 EUROPE BIOS & ABSTRACTS

Thursday	1 November 2018			
7:30-8:30am	**Breakfast – Borromaeus Restaurant***			
8:30-9:30am	***SharkBytes (Pirouette)***			
	Pirouette	**Grosse Reitschule**	**Kleine Reitschule**	
9:45-11:00am	16 **SMB in the Star Wars Universe** Eddi Blenkers	17 **To Send or Not to Send? How TCP congestion control algorithms work** Vladimir Gerasimov	18 **Generating Wireshark Dissectors: A status report** Richard Sharpe	DIVE IN WITH GERALD COMBS & WIRESHARK CORE DEVELOPERS AT THE DEVELOPER DEN!
11:00–11:15am	Break			
11:15am-12:30pm	19 **Hands-on Analysis of Multi-Point Captures** Christian Landström	20 **TCP SACK Overview and Impact on Performance** John Pittle	21 **sFlow: theory & practice of a sampling technology and its analysis with Wireshark** Simone Mainardi	
12:30–1:30pm	LUNCH			
1:30–2:45pm	22 **Writing a TCP Analysis Expert System** Jasper Bongertz	23 **BGP is not only a TCP Session: learning about the protocol that holds networks together** Werner Fischer	24 **Developer Bytes Lightning Talks** Wireshark Core Developers	
2:45–3:00pm	Break			
3:00–4:15pm	25 **Using Wireshark to Solve Real Problems for Real People: step-by-step case studies in packet analysis** Kary Rogers	26 **Troubleshooting WLANs (Part 1): Layer 1 & 2 analysis using multi-channel hardware, Wi-Spy & Other Tools** Rolf Leutert	27 **IEEE802.11ac Debugging in a Windows Environment: new ways of debugging with Wireshark in a post-AirPcap era** Megumi Takeshita	
4:15 – 4:30pm	Break			
4:30 – 6:00pm	28 **The Packet Doctors are In! Packet trace examinations with the experts** Drs. Bae, Blok, Bongertz, Landström & Rogers	29 **Troubleshooting WLANs (Part 2): Using 802.11 management & control frames** Rolf Leutert	30 **SSL/TLS decryption: uncovering secrets** Peter Wu	
6:00–8:30pm	***Group Competition Dinner & Sponsor Showcase (Conference Center Foyer)***			

***Breakfast is included with any Imperial Riding School Hotel room reservation booked through the SharkFest'18 EUROPE Lodging site link. Those not staying at the hotel or booking rooms separately from the SharkFest room block link pay €28 for a full buffet in the Booromaeus Restaurant, should they choose to breakfast there.**

SharkFest'18 EUROPE BIOS & ABSTRACTS

Friday	2 November 2018			
7:30-8:30am	Breakfast – Borromaeus Restaurant*			
	Pirouette	Grosse Reitschule	Kleine Reitschule	
8:45-10:00am	31 **Packet Monitoring in the Days of IoT and Cloud** Luca Deri	32 **Analyzing Kerberos with Wireshark** Eddi Blenkers	33 **Reliable Packet Capture** Christian Reusch	PACKET CHALLENGE SHEETS DUE BY 8 AM
10:00-10:15am	Break			
10:15-11:45am	34 **OPEN FORUM: Aha! Moments in Packet Analysis** Chris Greer	35 **TCP Split Brain: Compare/ Contrast TCP Effects on Client and Server with Wireshark** John Pittle	36 **802.11n/ac: complexity & solutions in capturing MIMO traffic** Thomas d'Otreppe	
11:45am-12:15pm	*Closing Remarks& Packet Challenge Awards (Pirouette)*			
12:15-2:00pm	*Farewell Reception & Lunch (Conference Center Foyer)*			

***Breakfast is included with any Imperial Riding School Hotel room reservation booked through the SharkFest'18 EUROPE Lodging site link. Those not staying at the hotel or booking rooms separately from the SharkFest room block link pay €28 for a full buffet in the Booromaeus Restaurant, should they choose to breakfast there.**

SharkFest'18 EUROPE BIOS & ABSTRACTS

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

WEDNESDAY, 31 OCTOBER

8:30-9:30am	**Keynote: *"Twenty Years of Code & Community"*** **Gerald Combs & Friends**
9:45-11:00am	
Pirouette	**01 Back to the Basics** When using Wireshark for the first time, it can be an overwhelming and bewildering experience. In this session, we'll take a step back and understand TCP/IP from a troubleshooter's perspective. What does it mean to have retransmissions? Is there a problem? Is it important? What steps should I take to try and narrow down the issue: Are there any helpful guides?" So if you've ever opened up a trace file and said 'Now what the hell do I do?' then this session is for you. **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 CTO for the company. With his broad knowledge of protocol analysis in a complex enterprise infrastructure, Hansang brings a unique perspective to packet analysis.
Grosse Reitschule	**02 802.11n/ac: complexity and solutions in capturing MIMO traffic** Wireless LANs are acquiring more and more advanced features to make them a lot faster. Those features, in 802.11n and 802.11ac (and quite a few other 802.11 specs), are bringing challenges to Wi-Fi security tools and analysis techniques. 802.11n brought some complexity, but 802.11ac is bringing the big guns to the game, especially with Wave 2: up to 8 streams, multi-user MIMO, beam forming, up to 160MHz channels, channel bonding, additional frequencies, and a lot more. In this talk, we'll reminisce about the good old days when capture was simple, then detail and explain all of these fancy new features. We'll also explain the complexity of capturing MIMO and, finally, talk about hardware and software tools to capture such traffic and their respective limitations. **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. An active open source developer, Thomas contributes to other open sources projects, including WiFiBeat, and maintains (WPE) patches for hostAPd and Freeradius to test WPA Enterprise network security. Thomas also contributes to 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. Beyond his development work, Thomas has authored a pro-active wireless security course, "Offensive-Security Wireless Attacks" (aka WiFu), which has been delivered to large numbers of IT Security professionals worldwide, and is a well-known speaker at DefCon, BlackHat, DerbyCon, SharkFest, Mundo Hacker Day, BruCON and other conferences in the Americas and Europe..
Kleine Reitschule	**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.
11:15am-12:30pm	
Pirouette	**04 Back to the Trenches** In the session, Hansang provides real-world troubleshooting examples and interacts with attendees in addressing various TCP analysis scenarios. **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.

Grosse Reitschule	**05 Handcrafted Packets: build network packets with Scapy** • Want to test a Wireshark dissector you've developed but a sample capture is missing? • Want to test whether an application reacts to all defined commands? • You do a penetration test and want to see how a network device handles undefined data (e.g. with TCP MSS=0)? For all these cases, Scapy can help you build the packets you need. In this talk, I will show you how to do it. Scapy is a packet manipulation tool written in Python. It can forge or decode packets, send them on the wire, capture them, and match requests and replies. In addition to Scapy, we'll also have a brief look at other packet editing tools. **Instructor: Uli 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 favourite occupations while working as a network engineer at a German machine manufacturer.
Kleine Reitschule	**06 Using More of the Features of Wireshark to Write Better Dissectors** There are many features in Wireshark for dissector writers that many people do not seem aware of. Some are new, and some have been there for a long time. This presentation will expose people to both new and old techniques for writing better dissectors, including: * Using dissector tables * Easily adding units * Handling bit fields * Expert infos * etc It will also make reference to real dissectors to illustrate the concepts involved. **Instructor: Richard Sharpe, Principal Software Engineer, Primary Data** Richard is a long-time contributor to Wireshark who has recently started working on the 802.11 and other dissectors, including the IEEE1905 and other protocols
1:30-2:45pm	
Pirouette	**07 TCP - Tips, Tricks, & Traces** Performance problems can often be isolated using the transport layer. But how can we identify what is actually broken if we don't know how it should work in the first place? In this interactive session, we will examine: • The TCP handshake and TCP Options • TCP Windows • TCP Retransmissions • TCP Selective Acknowledgements • and more! A sample trace file will be provided so you can follow along. Additionally, a few case studies will be presented that show how aspects of TCP can be leveraged to find root cause. **Instructor: Chris Greer, Network Analyst, Packet Pioneer** Chris Greer is a Network Analyst for Packet Pioneer LLC. Chris has several years of experience in analyzing and troubleshooting networks. He regularly assists companies in tracking down the source of network and application performance problems using a variety of protocol analysis and monitoring tools including Wireshark. When he isn't hunting down problems at the packet level, he can be found teaching Wireshark classes and writing articles for technical blogs and online magazines.
Grosse Reitschule	**08 Packet Analysis in the Cloud** As more and more enterprises adopt a cloud-first strategy, how does that impact the desire and ability to analyse packets? How can we get the packets, what tools are available and should we even care? In this session, Paul will review public cloud and hybrid configurations, why we might need packets and how we get them. To illustrate, Paul will walk through a real-life case study, investigating a problem with an application hosted in Amazon Web Services (AWS). **Instructor: Matthew York, Performance & Stability Engineer Advance7** After having spent 10 years at a large enterprise software company as a software and solution architect, Matthew joined Advance7 in 2013 as a Performance & Stability Consultant. He now works with clients in multiple industries to troubleshoot intermittent application problems in distributed systems - things like slow response times, unknown errors, etc. He uses Wireshark on a daily basis to capture and analyse data and mainly works with large organisations, so tends to deal with capturing and post-processing large datasets. Matthew leads projects to build analytic tools for data captured with Wireshark, so has a really good understanding of the Pcap and PcapNg file formats. Matthew also holds Riverbed Application Performance Management and Network Performance Management certifications.

Kleine Reitschule	**09 Crash Course: IPv6 & network protocols - Understanding IPv6 & a few network protocols as seen on the wire** This presentation is split into 2 sections. Both are network protocol "crash courses" explained by a pcap walk-through. 1) IPv6: While it is quite obvious that the Internet Protocol numbers have changed, it is not that easy to understand all those new control protocols for IPv6 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 the data link layer address resolution occur? This presentation guides you through a pcap on how to interpret and filter for relevant messages. 2) Network Protocols: A switched network is a complex infrastructure with lots of protocols running between those switches and routers. This part of the presentation walks through a pcap again to explain the most common network protocols such as STP, CDP, LLDP, VTP, LACP, HSRP, as well as management protocols such as Syslog, NTP, SNMP, TFTP. **Please bring a laptop with Wireshark already installed. Sample pcap files will be distributed.** **Instructor: Johannes Weber, Network Security Consultant, webernetz** Johannes currently works as a Network Security Consultant at TÜV Rheinland i-sec GmbH. He has a Masters degree in IT-Security (Thesis: IPv6 Security) and blogs regularly at **https://blog.webernetz.net**. At customer sites, Johannes works with (next-generation) firewalls, mail and DNS appliances, and classic routers/switches.
3:00-4:15pm	
Pirouette	**10 The Unusual Suspects: open source tools for enhancing big data & network forensics analysis** There's tcpdump, there's Wireshark, and there are other tools we use to analyze packets, e.g. tshark. But there are other free tools that are worth looking at that can help in your analysis as well, especially for large numbers of packets and network forensics. This talk will look at a selection of these tools and demonstrate what they're good for. **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.
Grosse Reitschule	**11 IoT – Buy and Install your own Destruction! (Part 1)** Internet of Things (IoT) devices are ubiquitous…from lightbulbs, NEST devices to WEMO technology; they are often thought of as cool toys or simply a convenience. Unfortunately; as Mirai: an IoT DDoS Botnet showed in 2017, they're also the new frontier for exploitation. In this hands-on workshop, using open-source tools such as Wireshark, we'll examine several of the key IoT technologies including Bluetooth, WEMO, and others. Numerous hands-on exercises will be utilized for practice. **Please bring a laptop with Wireshark already installed. Sample pcap files will be distributed.** **Instructor: Phill Shade, Owner, Merlion's Keep Consulting** Phill "Sherlock" Shade is a Senior Network / Forensics Investigator and founder of Merlion's Keep Consulting, specializing in all aspects of Network and Forensics Analysis. He is an internationally recognized Network Security and Forensics expert, drawing from his over 30 years of hands-on, real world experience. A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at Cyber Warfare Forum Initiative, he is a frequent consultant for numerous international security, technology and government agencies.
Kleine Reitschule	**12 Slow Start & TCP Reno Demystified: how congestion avoidance modes are working** This presentation will demonstrate, on a real-world 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 if they can be left again. The session will explain the following mechanisms: cwnd, ssthresh, receive window, SACK and 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 sector.
4:30-5:45pm	

Pirouette	**13 Wireshark CLI Tools and Scripting** While working in a GUI environment is great, there are advantages to working in a Command Line Interface (CLI). In this session, you'll get become familiar with some of the Wireshark CLI tools (tshark, editcap, mergecap and capinfos). The basic usage of the tools will be discussed first before diving into more advanced usage when integrating with other commands to create new ways of processing pcap(ng) files. **Sake Blok, Relational Therapist for Computer Systems, SYN-bit.nl** Sake has been analyzing packets since the end of the last century. In the course of his work, he discovered many bugs in devices and presented his findings to the vendors to fix the issues. He also discovered configuration issues that led to functional problems or performance issues in applications running over the network. These issues were resolved based on reports Sake presented to his customers. In 2009, Sake started the company SYN-bit to provide network analysis services to enterprises across Europe. As part of his work to service his customers, 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.
Grosse Reitschule	**14 IoT – Buy and Install your own Destruction! (Part 2)** Internet of Things (IoT) devices are ubiquitous…from lightbulbs, NEST devices to WEMO technology; they are often thought of as cool toys or simply a convenience. Unfortunately; as Mirai: an IoT DDoS Botnet showed in 2017, they're also the new frontier for exploitation. In this hands-on workshop, using open-source tools such as Wireshark, we'll examine several of the key IoT technologies including Bluetooth, WEMO, and others. Numerous hands-on exercises will be utilized for practice. **Please bring a laptop with Wireshark already installed. Sample pcap files will be distributed.** **Instructor: Phill Shade, Owner, Merlion's Keep Consulting** Phill "Sherlock" Shade is a Senior Network / Forensics Investigator and founder of Merlion's Keep Consulting, specializing in all aspects of Network and Forensics Analysis. He is an internationally recognized Network Security and Forensics expert, drawing from his over 30 years of hands-on, real world experience. A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at Cyber Warfare Forum Initiative, he is a frequent consultant for numerous international security, technology and government agencies.
Kleine Reitschule	**15 TLS 1.2/1.3 and Data Loss Prevention** HTTPs encryption using TLS is becoming more and more prolific industry wide. Using encryption prevents unknowing parties from snooping on your private information. However, if you own sensitive information as part of a corporation with many employees, encryption also makes it difficult for corporate authorities to determine if corporate information is leaking via encrypted channels over the public network. This presentation will examine the differences between TLS 1.2 and the new TLS 1.3 and then use Wireshark to find evidence of Data Loss Prevention or Man in the Middle decryption technology. **Instructor: Ross Bagurdes, Network Engineer/Educator, Bagurdes Technology** Ross has had a diverse career in engineering, beginning as a structural engineer, then project engineer for a gas utility, Ross was always quickly assigned the de-facto network administrator, typically after no one else was brave enough to break, and later fix, the network. Ross eventually ended up working as a network engineer designing and implementing enterprise networks for University of Wisconsin Hospital and Clinics. Here he worked with Extreme Networks, HP, Cisco, Tipping Point, among other network technology, as well as honed his Wireshark and protocol analysis skills. Until changing paths very recently, Ross spent 7 years teaching data networking at Madison College, and is currently authoring and producing IT training videos in Wireshark/Protocol Analysis, Cisco, and general networking topics for www.Pluralsight.com. In his free time, you'll find Ross and his dog, traveling, hiking, backpacking, or snowboarding somewhere in the western US

SharkFest'18 EUROPE BIOS & ABSTRACTS

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

THURSDAY, 1 NOVEMBER

8:30-9:30am	
9:45-11:00am	
Pirouette	**16 SMB in the Star Wars Universe** SMB is found in virtually every office network and even in many home networks. Despite it's ubiquity, the protocol offers challenges to network and system administrators alike. This presentation will introduce you to SMB network analysis using examples taken right from the Star Wars Universe. Using Wireshark, we answer all the burning questions left unanswered by the movies. The topics in detail: • Performance: Identify bottlenecks in server, client or the network • Security: Locate questionable default security in a trace file • DFS: Why does the client often ask for "DFS referrals"? • Filters and Wireshark settings that help you locate problems quickly • By the end of the presentation, you'll know if the Millenium Falcon can outrun a Star Destroyer and why Luke Skywalker could make it to Endor using an old code. Jedi and non-Jedi are welcome. No blasters, please! **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.
Grosse Reitschule	**17 To Send or Not to Send? how TCP congestion control algorithms work** This session is fully dedicated to the topic of TCP congestion control and will explain: - Why TCP congestion control is necessary - The history of its development - What the fixed terms: "cliff", "congestion collapse", "global synchronization".mean - Why this problem is so difficult to solve even now - Current approaches to handle TCP congestion We will compare different TCP congestion control algorithms (using sample trace files and Wireshark) with an emphasis on the most recent ones (CUBIC, CDG, BBR) and learn what main ideas are implemented in different kinds of TCP congestion control. We'll also take a look at some tricks like "Hybrid slow start" as a part of CUBIC algorithm, and several ways to trick the sender's behavior" **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 has 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.
Kleine Reitschule	**18 Generating Wireshark Dissectors: a status report** I presented a session at SharkFest'17 EUROPE on generating Wireshark Dissectors from XDR and suggested that I was working on generating them from a simple protocol description using the ANTLR4 tool. I have developed code that can now generate a dissector using a simple description of a protocol and this presentation is a progress report on my efforts and shows how to generate complex dissectors from a protocol description. **Instructor: Richard Sharpe, Principal Software Engineer, Primary Data** Richard is a long-time contributor to Wireshark who has recently started working on the 802.11 and other dissectors, including the IEEE1905 and other protocols.

11:15am – 12:30pm	
Pirouette	**19 Hands-on Analysis of Multi-Point Captures** This session will take you on the challenging journey of analyzing performance issues throughout a whole network path. Loadbalancers, firewalls, proxy servers might be involved, and finding the right spot to analyze the problem is not always an easy task. This talk focuses on multipoint capture file analysis and packet matching from different capture points. **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 been working in IT since 2004, focusing strongly 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 Fast Lane GmbH in 2009 as Senior Consultant for network analysis and security. Since 2013, he has been working as a Senior Consultants for Airbus Defence and Space CyberSecurity focusing on IT security, Incident Response and Network Forensics.
Grosse Reitschule	**20 TCP SACK Overview and Impact on Performance** TCP SACK is an important performance enhancement to TCP. Learn the details of how to interpret the SACK field and relate to performance of the application. **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 his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, Transaction Analyzer, IT Guru, Sniffer, HP Network Advisor, and the list goes on. Sr. Performance Consultant with OPNET Technologies since 2005, then came to Riverbed with the OPNET acquisition in 2012. Working as the America's Distinguished Performance Consultant since 2015 reflecting expertise in the entire portfolio of Riverbed visibility and performance analysis products, as well as technical leadership within the consulting practice for complex performance related customer engagements.
Kleine Reitschule	**21 sFlow: theory and practice of a sampling technology and its analysis with Wireshark** sFlow is sampling technology for monitoring traffic in high-speed networks. sFlow agents, embedded in switches and routers, periodically sample and export raw packets as well as network interface statistics to an sFlow collector. Sampling makes sFlow suitable to provide network-wide visibility, by enabling the continuous monitoring of tens, or even hundreds, of multi-Gigabit switches and routers. Sampling processes, although unable to offer 100% exact results, are able to provide results with a statistically-quantifiable accuracy. This session provides a detailed overview of sFlow, and demonstrates the suitability of Wireshark as an sFlow collector. When operating in this (unconventional) mode, Wireshark is not only able to analyze sampled packets at scale, but also to display new indicators such as switching and routing information as well as links status, load and congestion. **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.
1:30 – 2:45pm	
Pirouette	**22 Writing a TCP Analysis Expert System** TCP is a protocol that may seem simple, but can be quite complex to analyze. Most network analyzers have an expert system to help detecting common problems, but I wanted to write my own, just for the fun of it (that, and because it's useful). This talk will show what I have done so far, what the pitfalls are, and what the next steps could be. **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.
Grosse Reitschule	**23 BGP is not only a TCP Session: learning about the protocol that holds networks together** Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet - this is what Wikipedia tells us. But BGP is more right now - not only focused on internet but also on local network and data centers. In this sessions, we will investigate sample trace files and thoroughly review the dissector of BGP together. Please bring your own Wireshark and a powerful text editor to follow the session. The presenter will share his experience and the secrets he is using to learn and extend his protocol knowledge over the years with Wireshark and you. **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, Werner worked as a Network Project Engineer for Siemens AG.
Kleine Reitschule	**24 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 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**
3:00 – 4:15pm	
Pirouette	**25 Using Wireshark to Solve Real Problems for Real People: real-world packet analysis case studies** 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.
Grosse Reitschule	**26 Troubleshooting WLANs (Part 1): Layer 1 & 2 analysis using multi-channel hardware, 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 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 introduce you to the technique of approaching WLAN problems on Layer 1 and 2 using Wireshark, multi-channel hardware, and Wi-Spy. All of 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 problem situations will be used during the session to illustrate above topics. **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 been offering trainings, troubleshooting services, and protocol analysis consulting throughout Europe. LNS was the first company offering Network General's Sniffer trainings and, in 2006, the first to offer Wireshark trainings in Europe. LNS has trained thousands of students all over Europe in renowned companies from A(TT) to Z(urich Insurance). The trainings are very practice-oriented and based on our many years of troubleshooting experience. Rolf Leutert is a SNIFFER-Certified Master (SCM) and Wireshark Certified Network Analyst (WCNA).
Kleine Reitschule	**27 802.11ac Debugging in Windows: new ways of debugging with Wireshark in a post-AirPcap era** We've been in a wireless troubleshooting deadlock in Windows environments since the demise of AirPcap. Eye P.A. from Metageek, supporting IEEE802.11n and 802.11ac capture in Windows is now available, however, and lets you export filtered WLAN data directly to Wireshark! This session will show you the latest and best way to capture 802.11ac traffic in a Windows environment, using Eye P.A., AirPcap, AcrylicWiFi and will also show Linux and macOS methods. Adding to this, Megumi will walk you through a wireless troubleshooting case study using Wireshark with trace files. Utilizing the power of new Wireshark wireless features, debugging and troubleshooting can catch up with the new spec of Wi-Fi speed. **Instructor: Megumi Takeshita, Packet Otaku and Founder, Ikeriri Network Service, Tokyo** Megumi Takeshita, Packet Otaku (Twitter:@ikeriri), runs a packet analysis company, Ikeriri Network Service, in Japan. Ikeriri provides packet analysis services for troubleshooting, debugging, and network security inspections, and is also a reseller of wired/wireless capture and analysis devices and software for Riverbed, MetaGeek, Profitap, Dualcomm, and other related technology vendors. Megumi has authored more than 10 books on Wireshark and packet analysis in Japanese and is an avid contributor to the Wireshark project as well.

4:30 – 6:00pm	
Pirouette	**28 The Packet Doctors Are In! Packet trace examinations with the experts** The experts on this panel have been asked to look at a trace file and help find a reason for certain behaviors by attendees at many SharkFests. Based on this, they've decided to create a public forum for examining individual trace files with a broader audience for a collective learning experience. Trace files will be gathered from attendees 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 ANALYSIS BY THE PANEL!** Packet Doctors: Dr. Bae, Dr. Bongertz, Dr. Landström, Dr. Blok, Dr. Rogers
Grosse Reitschule	**29 Troubleshooting WLANs (Part 2): Using 802.11 management & control frames** 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 understanding of the different processes, using these frames for controlling the 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 above topics. 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 been offering trainings, troubleshooting services, and protocol analysis consulting throughout Europe. LNS was the first company offering Network General's Sniffer trainings and, in 2006, the first to offer Wireshark trainings in Europe. LNS has trained thousands of students all over Europe in renowned companies from A(TT) to Z(urich Insurance). The trainings are very practice-oriented and based on our many years of troubleshooting experience. Rolf Leutert is a SNIFFER-Certified Master (SCM) and Wireshark Certified Network Analyst (WCNA).
Kleine Reitschule	**30 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 improvements in order to assist in analyzing encrypted application traffic. Peter added TLS 1.3 decryption support to Wireshark and has worked on an actual TLS 1.3 implementation at Cloudflare.

SharkFest'18 EUROPE BIOS & ABSTRACTS

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

FRIDAY, 2 NOVEMBER

8:45 – 10:00am

Pirouette

31 Packet monitoring in the Days of IoT and Cloud

The advent of cloud services and IoT devices has changed traffic patterns. Listening to music or dimming the light can be done using your voice or a mobile application that performs this action by talking to a cloud service. This trend has changed traffic patterns observed in networks, forced us to rethink edge network security, and made service discovery a key technology as users demand zero-configuration networks. This talk covers in detail how network devices advertise themselves in networks, how you can use Wireshark to analyze this network traffic, and the privacy issues involved when using modern technologies in everyday life.

Instructor: Luca Deri, Founder & Leader, ntop Project, CS Lecturer, University of Pisa

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

Grosse Reitschule

32 Analyzing Kerberos with Wireshark

The Kerberos protocol plays an integral part in modern office networks. As Kerberos is used for authentication and authorization, any failure will likely result in a call to the Help Desk.

This presentation will introduce you to the concept of Kerberos as a security mechanism and the protocol itself. You will learn to use Wireshark to locate misconfigurations, system problems and user errors. Troubleshooting is just a matter of understanding the somewhat special Kerberos terminology.

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.

Kleine Reitschule

33 Reliable Packet Capture

This session will explain what you should consider when seeking reliable data capture on Ethernet networks, and will cover:

- How ethernet network traffic can be captured
- Capture setup hints
- What is needed for precise file captures
- Parameters to consider for reliable captures
- Best practice capture strategies
- Pros and cons for capturing from various capture points (localhost/virtual machine/network)
- Pitfalls that can be happen during capturing

The session will also show some demo traces of common capture errors.

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 sector.

10:15 – 11:30am

Pirouette

34 OPEN FORUM: Aha! Moments in Packet Analysis

SharkFest has proven to be a ripe environment for exchanging tribal knowledge about those moments when a Wireshark discovery was made that seemed a breakthrough in an individual's use of the tool or step-up in their packet analysis skill set.

This forum, moderated by Chris Greer, opens the floor to attendees to learn from one another by revealing their Wireshark Aha! moments. Have you created a personal Wireshark configuration that makes a particular diagnostic exercise a breeze? Stumbled onto a feature in Wireshark that blew you away? **Bring your trace files to share your discoveries with the crowd and enlighten fellow attendees!**

	Instructor: Chris Greer, Network Analyst, Packet Pioneer Chris Greer is a Network Analyst for Packet Pioneer LLC. Chris has several years of experience in analyzing and troubleshooting networks. He regularly assists companies in tracking down the source of network and application performance problems using a variety of protocol analysis and monitoring tools including Wireshark. When he isn't hunting down problems at the packet level, he can be found teaching Wireshark classes and writing articles for technical blogs and online magazines.
Grosse Reitschule	**35 TCP Split Brain: Compare/Contrast TCP Effects on Client and Server with Wireshark** 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.** Actively focused on Performance Engineering 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, Transaction Analyzer, IT Guru, Sniffer, HP Network Advisor, and the list goes on. Sr. Performance Consultant with OPNET Technologies since 2005, then came to Riverbed with the OPNET acquisition in 2012. Working as the America's Distinguished Performance Consultant since 2015 reflecting expertise in the entire portfolio of Riverbed visibility and performance analysis products, as well as technical leadership within the consulting practice for complex performance related customer engagements.
Kleine Reitschule	**36 802.11n/ac: complexity and solutions in capturing MIMO traffic** Wireless LANs are acquiring more and more advanced features to make them a lot faster. Those features, in 802.11n and 802.11ac (and quite a few other 802.11 specs), are bringing challenges to Wi-Fi security tools and analysis techniques. 802.11n brought some complexity, but 802.11ac is bringing the big guns to the game, especially with Wave 2: up to 8 streams, multi-user MIMO, beam forming, up to 160MHz channels, channel bonding, additional frequencies, and a lot more. In this talk, we'll reminisce about the good old days when capture was simple, then detail and explain all of these fancy new features. We'll also explain the complexity of capturing MIMO and, finally, talk about hardware and software tools to capture such traffic and their respective limitations. **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. An active open source developer, Thomas contributes to other open sources projects, including WiFiBeat, and maintains (WPE) patches for hostAPd and Freeradius to test WPA Enterprise network security. Thomas also contributes to 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. Beyond his development work, Thomas has authored a pro-active wireless security course, "Offensive-Security Wireless Attacks" (aka WiFu), which has been delivered to large numbers of IT Security professionals worldwide, and is a well-known speaker at DefCon, BlackHat, DerbyCon, SharkFest, Mundo Hacker Day, BruCON and other conferences in the Americas and Europe.