SharkFest '22 EUROPE AGENDA
(Draft, subject to change)

All times are in the Western European Time Zone.
Conference days run from:
9:00am through 6:15pm, with evening events from 6:30-8:30pm

- **Pre-Conference Classes (9:00am-5:00pm)**
- **SharkFest'22 Europe Session Agenda**
- **Session Abstracts & Instructor Bios**

SharkFest'22 EUROPE Conference Agenda

Pre-Conference Classes

Pre-Conference Class I

Learn Wireshark! TCP Deep Dive, Network Analysis and Threat Hunting

INSTRUCTOR: Chris Greer

For Class Description and Outline, please visit:
https://sharkfesteurope.wireshark.org/register

Monday, 31 October	
8:00-9:00am	Check-in & Badge Pick up
8:00-9:00am	Breakfast
9:00am-12:00pm	Class in session (with morning break)
12:00-1:00pm	Lunch
1:00-5:00pm	Class in session (with afternoon break)
Tuesday, 1 November	
8:00-9:00am	Breakfast
9:00am-12:00pm	Class in session (with morning break)
12:00-1:00pm	Lunch
1:00-5:00pm	Class in session (with afternoon break)

Pre-Conference Class II

Troubleshooting Voice over IP with Wireshark

INSTRUCTOR: Sake Blok

For Class Description and Outline, please visit:
https://sharkfesteurope.wireshark.org/register

Monday, 31 October	
8:00-9:00am	Check-in & Badge Pick up
8:00-9:00am	Breakfast
9:00am-12:00pm	Class in session (with morning breaks)
12:00-1:00pm	Lunch
1:00-5:00pm	Class in session (with afternoon break)

Pre-Conference Class III

Packet Capture Masterclass

INSTRUCTOR: Jasper Bongertz

For Class Description and Outline, please visit:
https://sharkfesteurope.wireshark.org/register

Tuesday, 1 November	
8:00-9:00am	Check-in & Badge Pick up
8:00-9:00am	Breakfast
9:00am-12:00pm	Class in session (with morning breaks)
12:00-1:00pm	Lunch
1:00-5:00pm	Class in session (with afternoon break)

SharkFest'22 EUROPE Conference Agenda

SharkFest Opening & Welcome Dinner

	Tuesday, 1 November	
SharkFest'22 EUROPE **Welcome Dinner & Sponsor Showcase**	12:00-8:00pm	**SharkFest'22 EUROPE Check-In & Badge Pick-Up**
	1:00-5:00pm	**Developer Den Drop-In**
	6:00-8:30pm	***SharkFest'22 EUROPE Welcome Dinner & Sponsor Showcase*** **SharkFest'22 EUROPE Attendees Only**

SharkFest'22 EUROPE Conference Agenda

Wednesday 2 November			
9:00-10:00	KEYNOTE: "*Latest Wireshark Developments & Road Map*" Gerald Combs & Friends		
10:00-10:15	BREAK		
	(Beginner/Intermediate)	(Intermediate/Advanced)	(Security and Workshops)
10:15-11:30	**01** **Automate your Analysis, tshark, the Swiss army knife** André Luyer	**02** **Chasing packet loss of TCP based applications using Wireshark** Matthias Kaiser	**03** **Wireshark and Mitre Atta&ck** Luca Deri & Marco Favilli
11:30-11:45	BREAK		
11:45-1:00	**04** **TBD**	**05** **Advanced dissector features** Roland Knall	**06** **Advanced IEC 60870-5-104 analysis with Wireshark** Martin Scheu
1:00-2:00	LUNCH		
2:00-3:15	**07** **TBD**	**08** **TBD** Peter Wu	**09** **LOG4SHELL: Getting to know your adversaries** Sake Blok
3:15-3:30	BREAK		
3:30-4:45	**10** **TBD**	**11** **TopN analysis using Wireshark** Megumi Takeshita	**12** **Introduction to WiFi Security (session 1)** Thomas d'Otreppe
4:45-5:00	BREAK		
5:00-6:15	**13** **TBD**	**14** **TBD**	**15** **Introduction to WPA Enterprise Exploitation (session 2)** Thomas d'Otreppe
6:30-8:30	**Sponsor Technology Showcase Reception, Treasure Hunt & Dinner**		

SharkFest'22 EUROPE Conference Agenda

Thursday 3 November			
9:00-10:00	**KEYNOTE: "Introducing Logray"** **Gerald Combs, Founder, Wireshark; Director of Open Source Projects, Sysdig and Loris Degioanni, CTO and Founder, Sysdig**		
10:00-10:15	**BREAK**		
	(Beginner/Intermediate)	**(Intermediate/Advanced)**	**(Security and Workshops)**
10:15-11:30	**16** **Contribute to Wireshark – the low hanging fruits** Uli Heilmeier	**17** **Dual Homing for redundancy and trouble** Eddie Blenkers	**18** **Visualizing and Decrypting TLS 1.3** Ross Bagurdes
11:30-11:45	**BREAK**		
11:45-1:00	**19** **The Packet Doctors are in! Packet trace examinations with the experts**		
1:00-2:00	**LUNCH**		
2:00-3:15	**20** **TCP Conversation Completeness – What it is, how to use it.** Chris Greer	**21** **TBD**	**22** **TBD**
3:15-3:30	**BREAK**		
3:30-4:45	**23** **TBD**	**24** **TBD**	**25** **TBD**
4:45-5:00	**BREAK**		
5:00-6:15	**26** **TBD**	**27** **TBD**	**28** **TBD**
6:30-8:30	**Sponsor Technology Showcase Reception, esPCAPe Group Packet Challenge & Dinner**		
	Q & A		

SharkFest'22 EUROPE Conference Agenda

Friday 4 November			
9:00-10:00	**SHARKBYTES** **SharkBytes consist of "little crunchy bits of wisdom." Like popular TED talks, SharkBytes aim to inform, inspire, surprise, and delight by delivering a speech on a personal topic in under 5 minutes.** **Information and a review of past SharkByte presentations can be found https://sharkfest.wireshark.org/sharkbytes** **Email us your SharkByte session idea: sharkfest@wireshark.org**		
10:00-10:15	**BREAK**		
	(Beginner/Intermediate)	**(Intermediate/Advanced)**	**(Security and Workshops)**
10:15-11:30	**29** **Network Troubleshooting from Scratch** Jasper Bongertz	**30** **TBD**	**31** **TBD**
11:30-11:45	**BREAK**		
11:45-1:00	**32** **Intro to QUIC - The TCP Killer?** Chris Greer	**33** **Hands on Deep Dive** Hansang Bae	**34** **DEVELOPER DEN DROP IN (In-person/Zoom/Discord)**
1:00-2:00	**A walkthrough of the SharkFest esPCAPe & CTF Challenges**		
2:00-3:00	**Closing Remarks, Challenge Awards and Farewell reception**		

SharkFest'22 EUROPE Conference Agenda

Session Abstracts & Instructor Bios

(DRAFT - UPDATED FREQUENTLY)

Wednesday 2 November

9:00-10:00

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

10:15-11:30

01 Automate your Analysis: tshark, the Swiss army knife

Many use only the graphical interface of Wireshark, but the command line tools are also very useful. And even the command line options of Wireshark itself.

This presentation shows you how to use tshark in scripts to do analysis that would be hard to do manually. By automating your analysis, you can quickly check for 'known problems' and have more time to investigate new issues. At Rabobank, we took this a step further and made it possible for novice users (DevOps team members) to upload their pcap file and get an automated report with checks and advices. At the core of this tool is tshark.

Instructor: André Luyer, Senior Performance Consultant, Rabobank
André is a senior Performance Consultant and troubleshooter at Rabobank and has been analyzing packets for over 25 years. First as a troubleshooter for network issues, both hard- and software, and later specializing in performance testing which requires a combination of in depth knowledge of networking protocols and coding skills, which is also used for testing security in the form of DDoS testing. André also is a trainer for an in-house 'Wireshark bootcamp' course.

02 Chasing packet loss of TCP based applications using Wireshark

Packet loss in networks can lead to serious performance degradation of your applications. But how serious is it, when packets are lost? How much can I trust the expert information messages of Wireshark? This talk will discuss typical sources for packet loss across networks and will show, how TCP based applications can be analyzed with Wireshark, when packet loss occurs. Using real-life case studies, Matthias will guide you through the process of troubleshooting packet loss by looking at packet flows, using profiles and filters, and interpreting Wireshark expert messages - in order to finally isolate the fault domain and find the root cause. Trace files are provided to follow along with the analysis.

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

03 Wireshark and Mitre Atta&ck

The Mitre ATT&CK Framework (Adversarial Tactics, Techniques, and Common Knowledge) is the most popular knowledge base containing methods and actions used by hackers to circumvent security. As Wireshark is used by many professionals for analyzing cybersecurity incidents, this talk will:
- Give an introduction to widely employed methods of Network Service Discovery as well as some techniques regarding Adversary in the Middle, Wireless Compromise and Endpoint Denial Of Service, referenced in the Mitre ATT&CK.
- present how Wireshark can be used in order to detect them.
- show some tools based on Wireshark to automate analysis of cybersecurity packet traces.

Instructor: Luca Deri, Leader, ntop Project
Luca is the leader of the ntop project (http://www.ntop.org/), which is aimed at developing an open-source monitoring platform for high-speed network traffic analysis. He shares his time between ntop and the University of Pisa, Italy, where he is a lecturer in the Computer Science department. He received his PhD in Computer Science with a thesis on Software Components from the University of Berne in 1997. He previously worked as a research scientist at the IBM Zurich Research Laboratory and as a research fellow at the University College of London. His

professional interests include network management and monitoring, software components and object-oriented technology. His home page is http://luca.ntop.org/.

Instructor: Marco Favilli

11:45-1:00

04 TBD

05 Advanced Dissector Features

This talk explains some of the more advanced programming features we can apply to dissectors and how to integrate them in your own dissectors.

The finer details of dissector work is being discussed, such as:

* Redissection
* Expert fields
* Taps

… and why you should apply them. Also some neat tricks with taps are going to be shown and we are developing a more advanced dissector live in 60 minutes from - almost - scratch.

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

06 Advanced IEC 60870-5-104 analysis with Wireshark

Recent discovery of industrial malware Industroyer2 proved that adversaries have deep industrial protocol knowledge. In order to detect such attacks, defenders need to be prepared and know their network. In this talk I will show the Industroyer2 characteristics compared to known good traffic. Further I will present a Wireshark plugin to get IEC 608-5-104 protocol insights for further use in the open source IDS ntopng.

Instructors: Martin Scheu, OT Security Engineer, SWITCH CERT
Martin is an OT Security Engineer at SWITCH CERT in Switzerland. One of his task is to support operators of critical infrastructure in doing network security monitoring of industrial networks, mainly in the energy sector. His background is all around industrial control system.

2:15-3:30

07 TBD

Instructor: TBD

08 TBD

09 LOG4SHELL: Getting to know your adversaries

What does a LOG4SHELL attack look like on the network and how to analyze the LOG4SHELL attack (including some of its deployed exploits) with Wireshark.

In December 2021, the IT world was shaken up by a CVE with score 10. A vulnerability in the widely used log4j logging library allowed an attacker to run arbitrary code on the system by making it log a specific string. As a lot of elements in the logging comes from user controlled data, the exploit was very easy use.In order to understand the attack and it's impact, I reproduced an attack in my LAB. And after that, I set up a honeypot to collect attack samples. I went one step further and set up an isolated system and deliberately infected it with some of the exploits to see what it would do.

In this talk I will walk through the process of (safely) setting up the LAB systems, the honeypot and the infected victim. The captured traffic will be analyzed with Wireshark and some hints and tips on how to use Wireshark in a security context will be given.

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

3:45 -5:00

10 TBD

11 TopN analysis using Wireshark

Useful TopN analysis method using Wireshark, finding problem from bunch of traces.

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

12 Introduction to WiFi Security
This workshop is split in two sessions, each with hands-on exercise. While they are independent sessions, this first one will teach the basics, which are important to understand things in the second part, Introduction to WPA Enterprise exploitation.

We will learn the basics of Wi-Fi where we will briefly go over the standards and amendments, network structure, and encryption. Afterward, we will be using Linux to determine the capabilities of our Wi-Fi hardware to ensure our hardware is adequate, and do a packet capture using airodump-ng and Wireshark.

Instructor: Thomas d'Otreppe
Thomas d'Otreppe is a wireless security researcher and author of Aircrack-ng, the most popular open source suite of tools for WiFi network security assessments. He is an active open source developer and contributor. He also created OpenWIPS-ng and WiFiBeat, maintains patches for hostAPd and Freeradius to test WPA Enterprise networks security.

Thomas contributed to the WiFi stack and toolset in Backtrack Linux, which has now become Kali Linux, the de facto choice Linux distribution for penetration testing and vulnerability assessment. He is also the author of a pro-active wireless security course, Offensive-Security Wireless Attacks (aka WiFu, or PEN-210) which has been delivered to large numbers of IT Security professionals worldwide. Thomas speaks and teaches in the Americas and Europe. He is a well-known speaker at DefCon, BlackHat, DerbyCon, SharkFest, Mundo Hacker Day, BruCON and other conferences.

SharkFest'22 EUROPE Conference Agenda

5:15-6:30

13 TBD

14 TBD

15 Introduction to WPA Enterprise Exploitation

This workshop is split in two sessions, each with hands-on exercise. While they are independent sessions, the first one, Introduction to Wi-Fi Security, taught the basics, which are important to understand things in this part.

We will learn how WPA (either WPA1, WPA2, or WPA3) Enterprise differs from preshared keys (PSK) used in home networks. WPA Enterprise uses EAP which allows a number of different authentication protocols, and we will review a detailed exchange with PEAP/EAP-MSCHAPv2, a commonly chosen one, to better understand how the key exchange works. This is followed by the exploitation of such a set-up.

Instructor: Thomas d'Otreppe

Thomas d'Otreppe is a wireless security researcher and author of Aircrack-ng, the most popular open source suite of tools for WiFi network security assessments. He is an active open source developer and contributor. He also created OpenWIPS-ng and WiFiBeat, maintains patches for hostAPd and Freeradius to test WPA Enterprise networks security.

Thomas contributed to the WiFi stack and toolset in Backtrack Linux, which has now become Kali Linux, the de facto choice Linux distribution for penetration testing and vulnerability assessment. He is also the author of a pro-active wireless security course, Offensive-Security Wireless Attacks (aka WiFu, or PEN-210) which has been delivered to large numbers of IT Security professionals worldwide. Thomas speaks and teaches in the Americas and Europe. He is a well-known speaker at DefCon, BlackHat, DerbyCon, SharkFest, Mundo Hacker Day, BruCON and other conferences.

6:30-8:30

Sponsor Technology Showcase Reception, Treasure Hunt & Dinner

SharkFest'22 EUROPE Conference Agenda

THURSDAY 3 NOVEMBER

9:00-10:00

KEYNOTE: "Introducing Logray"
Loris Degioanni, CTO & Founder, Sysdig and
Gerald Combs, Director of Open Source Projects, Sysdig

Keynote: Introducing Logray

10:15-11:30

16 Contribute to Wireshark – the low hanging fruits

You use the great and free software Wireshark and want to give something back. But you are not a programmer and don't know how: Relax. In this session we will take a walk through all the different ways to contribute to the community without writing a line of code.

Instructors: Uli Heilmeier, DevSecOps Engineer

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

17 Dual Homing for redundancy and trouble

This talk covers configuration issues that might occur, when end systems are using two or more network interface cards. Problems usually occur on layers 2 or 3. Of course, we will use trace files to diagnose the issues.

Critical systems are usually equipped with two or more network cards. This might be for redundancy, security or enhanced performance.

Some configurations require that network engineers and system engineers work together to achieve the desired results. This talk covers configurations, where this cooperation could be, ahem, improved.

Instructor: Eddie Blenkers, Security Analyst
Eduard "Eddi" Blenkers has analyzed countless networks and applications - often teaming up with Jasper Bongertz. The majority of analysis projects dumped SMB on his lap. The background in computer and network forensics often helped to link network packets to computer settings or misbehaving applications.

In his current occupation as Security Analyst he frequently uses Wireshark to analyze malware behavior or identify compromised systems.

18 Visualizing and Decrypting TLS 1.3

In this beginner level talk, you will learn the essentials of TLS encryption. We will start with a brief history of TLS which will both introduce the main concepts as well as provide the necessary vocabulary to understand the protocol. Then we will offer a visualization of TLS encryption to understand the encryption process, which will be valuable when we examine a Wireshark Capture of TLS encrypted packets. Then we will walk through how to capture session keys, decrypt traffic, and analyze the protocols being carried with TLS. You will leave this talk with a great visual to imagine TLS encryption, as well as everything you need to decrypt and examine TLS encryption in an HTTPs session.

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

11:45-1:00

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

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

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

2:00-3:15

20 TCP Conversation Completeness – What it is, how to use it.

Let's take a closer look at how this Wireshark value is calculated, what it means, and what practical ways it can be used for troubleshooting.

The TCP Conversation Completeness field sorta snuck up on us. It appeared in Wireshark version 3.6 as a new Wireshark field in the TCP header. It's a cool little feature! Prior to this, it was difficult to determine how far a TCP conversation had progressed in a pcap. But, what is that little number next to the field? How is it derived? And most importantly, how can we practically use this new feature?

Let's dig!

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

21 TBD

22 TBD

3:30-4:45

23 TBD

24 TBD

25 TBD

5:00-6:15

26 TBD

SharkFest'22 EUROPE Conference Agenda

27 TBD
28 TBD
6:30-8:30
Sponsor Technology Showcase Reception, Group Packet Competition & Dinner

SharkFest'22 EUROPE Conference Agenda

FRIDAY 4 NOVEMBER

9:00-10:00

SharkBytes

10:15-11:30

29 Network Troubleshooting from Scratch

A client application doesn't work because something fails. Of course it's the network. Is it really? While it's not impossible it could also be a number of other things. This talk is going to look at various scenarios, troubleshooting the problem step by step with whatever tools are available (Wireshark included, of course), and show how to get to the root of the problem. If you're a beginner in troubleshooting network issues this talk is going to get you up to speed.

Instructor: Jasper Bongertz, Network Security Expert, G DATA Advanced Analytics

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

30 TBD

31 TBD

11:45-1:00

32 Intro to QUIC - The TCP Killer?

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

Instructor: Chris Greer, Network Analyst, Packet Pioneer

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

33 Hands on Deep Dive

Not every packet analysis troubleshooting leads to the smoking gun. Sometimes, you have to tease out the most likely culprit. And to do that requires DETAILED TCP/IP knowledge. In this session, we'll see how packet analysis can be used to "solve" complex issues.

Instructor: Hansang Bae, Field CTO, Netspoke

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

SharkFest'22 EUROPE Conference Agenda

34 DEVELOPER DEN DROP-IN - In-Person/Zoom/Discord

This dedicated session is the perfect time to pop-in, meet the Wireshark core developers and ask them all your Wireshark questions.

1:00-2:00

A walkthrough of the SharkFest CTF & Group Packet Competitions

2:00-4:00

Closing Remarks & Packet Challenge Awards
Farewell Reception