SharkFest '22 EUROPE AGENDA

All times are in the Western European Time Zone.
Conference days run from:
9:00 through 18:15, with evening events from 18:30-20:30

- **Pre-Conference Classes (9:00-17:00)**
- **SharkFest'22 Europe Session Agenda**
- **Session Abstracts & Instructor Bios**

SharkFest'22 EUROPE Conference Agenda

Pre-Conference Classes

Pre-Conference Class I **Learn Wireshark! Analyzer Intro, TCP Deep Dive and Intro to Threat Hunting** **INSTRUCTOR: Chris Greer** **For Class Description and Outline, please visit:** **https://sharkfesteurope.wireshark.org/register** **Atlantic Room**	**Monday, 31 October**	
	8:00-9:00	Check-in & Badge Pick up
	8:00-9:00	Breakfast
	9:00-12:00	Class in session (with morning break)
	12:00-13:00	Lunch
	13:00-17:00	Class in session (with afternoon break)
	Tuesday, 1 November	
	8:00-9:00	Breakfast
	9:00am-12:00	Class in session (with morning break)
	12:00-13:00	Lunch
	13:00-17:00	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** **Tropical Room**	**Monday, 31 October**	
	8:00-9:00	Check-in & Badge Pick up
	8:00-9:00	Breakfast
	9:00-12:00	Class in session (with morning breaks)
	12:00-13:00	Lunch
	13:00-17:00pm	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** **Tropical Room**	**Tuesday, 1 November**	
	8:00-9:00	Check-in & Badge Pick up
	8:00-9:00	Breakfast
	9:00-12:00	Class in session (with morning breaks)
	12:00-13:00	Lunch
	13:00-17:00pm	Class in session (with afternoon break)

SharkFest’22 EUROPE Conference Agenda

SharkFest Opening & Welcome Dinner

SharkFest‘22 EUROPE **Welcome Dinner & Sponsor Showcase**	**Tuesday, 1 November**	
	12:00-20:00	**SharkFest‘22 EUROPE Check-In & Badge Pick-Up**
	13:00-17:00	**Developer Den Drop-In**
	18:00-20:30	***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 *Atlantic Room*	
10:00-10:15	BREAK	
10:15-11:30	(Beginner/Intermediate) Atlantic Room	(Intermediate/Advanced) Park Suite
	01 **Network Troubleshooting from Scratch** Jasper Bongertz	**02** **Chasing packet loss of TCP based applications using Wireshark** Matthias Kaiser
11:30-11:45	BREAK	
11:45-13:00	**03** **Intro to QUIC - The TCP Killer?** Chris Greer	**04** **Wireshark and Mitre Atta&ck** Matteo Biscosi & Marco Favilli
13:00-14:00	LUNCH	
14:00-15:15	**05** **Wild PCAPs: The weird stuff is in the weeds** Chris Bidwell	**06** **Introduction to WiFi Security (session 1)** Thomas d'Otreppe
15:15-15:30	BREAK	
15:30-16:45	**07** **Wireshark at Enterprise Scale** Dr. Stephen Donnelly	**08** **Introduction to WPA Enterprise Exploitation (session 2)** Thomas d'Otreppe
16:45-17:00	BREAK	
17:00-18:15	**09** **Ask the Experts: Wireshark Q&A: New Features, Feature Requests, Bug Reports**	**10** **Decrypt Kerberos/NTLM "encrypted stub data" in Wireshark** Clément Notin
18:30-20:30	**Sponsor Technology Showcase Reception, Treasure Hunt & Dinner**	

SharkFest'22 EUROPE Conference Agenda

Thursday 3 November		
9:30-10:00	KEYNOTE: *"Building the Wireshark Community"* Gerald Combs *Atlantic Room*	
10:00-10:15	BREAK	
10:15-11:30	(Beginner/Intermediate) Atlantic Room	(Intermediate/Advanced) Park Suite
	11 **Contribute to Wireshark – the low hanging fruits** Uli Heilmeier	**12** **Advanced IEC 60870-5-104 analysis with Wireshark** Martin Scheu
11:30-11:45	BREAK	
11:45-13:00	**13** **The Packet Doctors are in! Packet trace examinations with the experts**	
13:00-14:00	LUNCH	
14:00-15:15	**14** **Automate your Analysis, tshark, the Swiss army knife** André Luyer	**15** **Spotting Hacking Attacks in a Trace File** Eddi Blenkers
15:15-15:30	BREAK	
15:30-16:45	**16** **IPv6 Crash Course** Johannes Weber	**17** **Security Monitoring for SMBs** Christian Landström
16:45-17:00	BREAK	
17:00-18:15	**18** **TopN analysis using Wireshark** Megumi Takeshita	**19** **LOG4SHELL: Getting to know your adversaries** Sake Blok
18:30-20:30	**Sponsor Technology Showcase Reception, esPCAPe Group Packet Challenge & Dinner**	

	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 *Atlantic Room*	
10:00-10:15	BREAK	
10:15-11:30	(Beginner/Intermediate) Atlantic Room	(Intermediate/Advanced) Park Suite
	20 **Understanding TCP Throughput** Kary Rogers	**21** **Learning Bluetooth Low Energy with Wireshark** Ville Haapakangas
11:30-11:45	BREAK	
11:45-13:00	**22** **Wireshark with LTE and 5G Packet Core** Mark Stout	**23** **Visualizing and Decrypting TLS 1.3** Ross Bagurdes
13:00-14:00	A walkthrough of the SharkFest esPCAPe & CTF Challenges	
14:00-16:00	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

BREAK (10:00 – 10:15)

10:15-11:30

01 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.

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.

BREAK (11:30 – 11:45)

11:45-13:00

03 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

04 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.

Instructors: Matteo Biscosi, Software Enginner, ntop Project and Marco Favilli
Italian born; Matteo graduated from the University of Pisa in Software Engineering. He is currently working in Ntop (networking company) as both Front-End and Back-End software engineer. He has already lectured at the Fosdem in February 2021 and SharkFest in June 2021, mainly talking about cybersecurity attacks and network traffic analysis.

Born in Pisa (Italy), Marco is a computer science student at Pisa University.

LUNCH (13:00 – 14:00)

14:00-15:15

05 Wild PCAPs: The weird stuff is in the weeds.

Taking a glance at PCAPs in detail, highlighting where some weird interesting details hide in the weeds.
e.g. What is this PCAP? where was it captured, close to what, how? What additional metadata's already there?
What are these systems likely to be? Heuristics for guessing host identities
Graph tips with the graphs I use most for bandwidth and gap analysis.

Instructor: Chris Bidwell
Chris has 15+ years working with enterprise financial networks and troubleshooting them with Wireshark. A self-described packet-head who loves to crack open Wireshark on the weekend whenever the opportunity arises, and encourages you all to try the Packet Capture Challenge!

06 Introduction to WiFi Security (part 1)

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.

BREAK (15:15 – 15:30)

15:30 - 16:45

07 Wireshark at Enterprise Scale

What motivates packet capture in Enterprise, and how applicable is Wireshark? We discuss the differences between on-demand, smart, and continuous packet capture strategies, and the practical techniques required. Performing and managing capture at large scale has its own challenges and produces prodigious amounts of data. How can we find what we are looking for in huge packet trace datasets, and can Wireshark help?

Instructor: Stephen Donnelly, CTO, Endace

Stephen has worked on packet capture and time-stamping systems for 20 years, earning his PhD for "High Precision Timing in Passive Measurements of Data Networks" from the University of Waikato, New Zealand. A founding employee of Endace, Stephen has developed FPGA-based packet capture and timing systems, clock synchronization systems, and high-performance network monitoring virtualization, and collaborated with customers in telcos, finance, test & measurement, enterprise, and government agencies to solve unique problems. Stephen is a contributor to the Wireshark, libpcap, Argus, and Suricata open-source projects.

08 Introduction to WPA Enterprise Exploitation (part 2)

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 pre-shared 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.

BREAK (16:45 – 17:00)

17:00-18:15

09 Ask the Experts: Wireshark Q&A: New Features, Feature Requests, Bug Reports

10 Decrypt Kerberos/NTLM "encrypted stub data" in Wireshark

We often use Wireshark to analyze Windows and Active Directory network protocols, especially those juicy RPC! But we are often interrupted in our enthusiasm by the payload dissected as "encrypted stub data". Until we discover that Wireshark has a helpful feature to decrypt this traffic, which is protected by secrets derived from the prior Kerberos or NTLM authentication. We will briefly describe the theory and show in practice how to configure Wireshark, and fill the required keytab file, so this "encrypted stub data" gets decrypted. This feature will offer you more visibility into those protocols in your future network analysis sessions.

Instructor: Clément Notin, Staff Reseach Engineer, Tenable

Clément Notin has been a cybersecurity engineer for around ten years. He started to learn about programming and network, when Wireshark was still called Ethereal!
He started as a pentester and auditor, first in a consulting company, then, for a global French industrial group.
He is now a researcher in Active Directory security for Tenable in order to contribute to the Tenable.ad product that allows to identify in real time the weaknesses of such environments and detect the attacks underway.

18:30-20:30

Sponsor Technology Showcase Reception, Treasure Hunt & Dinner

SharkFest'22 EUROPE Conference Agenda

THURSDAY 3 NOVEMBER

9:00-10:00

KEYNOTE: Building the Wireshark Community

BREAK (10:00 – 10.15)

10:15-11:30

11 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.

12 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.

BREAK (11:30 – 11:45)

11:45-13:00

13 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!**

LUNCH (13:00 – 14:00)

14:00-15:15

14 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.

15 Spotting Hacking Attacks in a Trace File

Barely a week passes, without reports of a successful hacking attack showing in the mainstream media.Practically all hacking attacks have one thing in common: The attackers snug in through the network. In this presentation we go through a number of trace files, that document hacking activities from reconnaissance to a complete system take over.
Trace files included. For a best experience, bring your own computer.

Instructor: Eddi 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.

BREAK (15:15 – 15:30)

15:30-16:45

16 IPv6 Crash Course

While it is quite obvious that the IP addresses have changed, it is not that easy to understand all those new control protocols such as ICMPv6 with its Router Advertisements, Neighbor Solicitations, and so on. How does a router propagate itself? How does a new IPv6 client get an IPv6 address? How does he know about the DNS server? How does the data link layer address resolution (ARP in v4) occur? How does a residential Internet connection get its IPv6 prefix via DHCPv6? What about routing protocols such as OSPF and BGP? --> We've got you covered.

This presentation guides you through pcaps and how to interpret and filter for relevant IPv6 messages with Wireshark.

Instructor: Johannes Weber

Johannes works as a senior security engineer at LBBW Asset Management, financial services. He has a master's degree in IT-Security (thesis: IPv6 Security) and blogs regularly at https://weberblog.net, covering IPv6, VPNs, DNSSEC, NTP, Wireshark, and other topics. Johannes works with next-generation firewalls, mail- and DNS-appliances, as well as classical routers/switches.

17 Security Monitoring for SMBs

Security Monitoring is a must have nowadays. Still small - and mid-sized companies suffer from talent shortage and expensive security components when it comes to proper detection and response mechanisms. This Talk will provide an innovative hybrid approach to provide maximum detection and response capabilities for companies and organizations who cannot afford bleeding edge solutions like SIEM, SOC etc.
Cyber attacks are an everyday threat - the damage and follow-up costs from successful attacks are enormous. Investing in dedicated personnel who have both the time to analyze log data and the skills for targeted attack detection is usually not affordable for small and medium-sized businesses.
Through our years of experience in fighting cybercrime, we have been able to design a innovative, hybrid approach to security monitoring that combines and efficiently implements the most effective measures from SOC-as-a-service, Managed SIEM and other managed security offerings. Your protection needs can thus be met at a high level and at the same time in a cost-efficient manner.

Instructor: Christian Landström, Head of Managed Security Services, G DATA Advanced Analytics

Christian Landström works as Head of Managed Security Services at G DATA Advanced Analytics. Working in IT from 2004, with a strong focus on network communications and IT security, he graduated in computer science in 2008 and joined Synerity Systems and afterwards moved with the whole Synerity team to work for Fast Lane GmbH. There Christian created and delivered various Network Analysis Trainings and worked as Senior Consultant for network analysis and IT security. In 2013 he started working for Airbus Defence and Space CyberSecurity, where he stayed until 2019 as Incident Response and security audit expert. He shares his passion about network analysis together with Jasper and Eddi from the original Synerity Team on the Sharkfest conferences and on blog.packet-foo.com.

BREAK (16:45 – 17:00)

17:00-18:15

18 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.

19 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.

18:30-20:30

Sponsor Technology Showcase, esPCAPe Group Packet Challenge, Reception & Dinner

FRIDAY 4 NOVEMBER

9:00-10:00

SharkBytes

BREAK (10:00 – 10:15)

10:15-11:30

20 Understanding TCP Throughput

A Walk-Through of the Factors that can limit TCP Throughput Performance. If you've ever been asked why a user's download is slow and didn't know where to start, this session is for you. We'll go over the common issues that affect TCP throughput performance with pcap examples.

Instructor: Kary Rogers, Senior Director of Services Excellence, ZScaler
Kary has spent many years solving difficult system, network, and application problems by looking at the packets. Even though he's been in management for a while, he still occasionally finds himself chasing the high of unraveling a packet mystery. He has a YouTube channel called PacketBomb where he posts Wireshark videos or has a live stream with your favorite packeteers.

21 Learning Bluetooth Low Energy with Wireshark

Bluetooth Low Energy (BLE) is a common method for IoT device connections. In this workshop we will get to know BLE communication and different messages by capturing and analyzing BLE data. After we understand the basics of BLE communication we'll try to use that information to "exploit" a unprotected IoT device.
This interactive workshop includes an introduction presentation, demonstrations and analysis of pcap files. The pcap files corresponding to the captures generated during demos will be distributed to participants for analysis. Wireshark is used to capture and analyze BLE communication along with some other tools like BLE dongle, Ubertooth and Gatttool (with Kali Linux). Some tips and tricks for creating your own basic BLE test environment will be given.
Preliminary plan:
Part 1:
- What is Bluetooth Low Energy (very shortly)
- Demo: Capturing BLE communication from test environment
- Analyzing BLE communication data

Part 2:
- Demo: Capturing BLE communication of a real IoT device
- Analyzing captured data and [demo] using it to "exploit" IoT device

The real IoT device will be a BLE bulb, lock or something like that which communicates with a mobile phone.

Instructor: Ville Haapakangas, Senior Lecturer, Tampere University of Applied Sciences
Teacher of computer networks, network security and cybersecurity, user of Wireshark since Ethereal, always enthusiastic about learning new things by analyzing packets.

BREAK (11:30 – 11:45)

11:45-13:00

22 Wireshark with LTE, and 5G Packet Core

Review example captures for end to end flow of data in, and between LTE, and 5G nodes. This includes how to setup Wireshark to display tunneling information while packets are inside the 3gpp networks. Also will give example LUA dissector to show NAT64 dissection. Will include some IOT examples.

Instructors: Mark Stout, Principle Enginner, T-Mobile
Design, and Tech Support for Long-Term Evolution (LTE) mobile networks, and 5G for the last 21 years, in multiple countries. Active contributor to 3rd Generation Partnership Project (3GPP) 23, and 29 series. Currently the Principle Support Engineer for T-Mobile's LTE, Voice Over LTE (VoLTE), Internet of Things (IoT),and true 5G technology on the Packet Core network.

23 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.

13:00-14:00

A walkthrough of the SharkFest CTF & Group Packet Competitions

14:00-16:00

Closing Remarks & Packet Challenge Awards
Farewell Reception