SharkFest'22 US AGENDA

(Draft, subject to change)

SharkFest'22 US
Wireshark Developer and User Conference • Kansas City • July 9-14

All times are in the Central Standard time zone.

Conference days run from: 9:00am through 6:15pm, with evening events from 6:30-8:30pm

- Pre-Conference Classes (8:00am-5:00pm)
- SharkFest'22 US Session Agenda
- Session Abstracts & Instructor Bios

SharkFest’22 US Conference Agenda

Pre-Conference Classes

Pre-Conference Class I **Introduction to Packets – How to capture & analyze them using Wireshark** INSTRUCTOR: Betty DuBois For Class Description and Outline, please visit: https://sharkfestus.wireshark.org/register	**Saturday, July 9**	
	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)
	Sunday, July 10	
	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 **“Cybersecurity Threat Hunting – Go Deep with Wireshark”** INSTRUCTOR: Chris Greer For Class Description and Outline, please visit: https://sharkfestus.wireshark.org/register	**Monday, July 11**	
	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 Opening & Welcome Dinner

SharkFest ‘22 US **Welcome Dinner & Sponsor Showcase**	**Monday, July 11**	
	12:00-8:00pm	**SharkFest‘22 US Check-In & Badge Pick-Up**
	1:00-5:00pm	**Developer Den Drop-In**
	6:00-8:30pm	***SharkFest‘22 US Welcome Dinner & Sponsor Showcase*** SharkFest‘22 US Attendees Only

SharkFest'22 US Conference Agenda

Tuesday, July 12			
9:00-10:00	**KEYNOTE: "*Latest Wireshark Developments & Road Map*"** **Gerald Combs & Friends**		
10:00-10:15	BREAK		
10:15-11:30	**Basie AA1/BB1 (Beginner/Intermediate)**	**Andy Kirk A/B (Intermediate/Advanced)**	**Julia Lee A/B (Security and Workshops)**
	01 **Network Troubleshooting from Scratch** Jasper Bongertz	**02** **Wireshark and WiFi: Multicast Case Study** George Cragg	**03** **Dissecting WPA3** Megumi Takeshita
11:30-11:45	BREAK		
11:45-1:00	**04** **Build Your Own: Remotely accessible packet-capture drop box for troubleshooting networks with <$100** Anthony Efantis	**05** **Duct tape and baling wire: Extending Wireshark with Lua** Chuck Craft	**06** **Intrusion Analysis and Threat Hunting with Suricata** Josh Stroschein and Peter Manev
1:00-2:00	LUNCH		
2:00-3:15	**07** **Wireshark at Enterprise Scale** Dr. Stephen Donnelly	**08** **Wireshark with LTE and 5G Packet Core** Mark Stout	**09** **LOG4SHELL: Getting to know your adversaries** Sake Blok
3:15-3:30	BREAK		
3:30-4:45	**10** **Understanding TCP Throughput** Kary Rogers	**11** **Using Wireshark to learn IPv6** Jeff Carrell	**12** **Abusing the Network – An Overview of Malicious Network Activity and How to Detect It** Josh Stroschein
4:45-5:00	BREAK		
5:00-6:15	**13** **Troubleshoot like a Doctor** Josh Clark	**14** **Hands on Deep Dive** Hansang Bae	**DEVELOPER DEN DROP IN** **(In-person/Zoom/Discord)**
6:30-8:30	**Sponsor Technology Showcase Reception, Treasure Hunt & Dinner**		

SharkFest'22 US Conference Agenda

Wednesday, July 13			
9:00-10:00	**KEYNOTE: "Introducing Logwolf"** **Gerald Combs, Founder, Wireshark; Director of Open Source Projects, Sysdig and Loris Degioanni, CTO and Founder, Sysdig**		
10:00-10:15	BREAK		
10:15-11:30	Basie AA1/BB1 (Beginner/Intermediate)	Andy Kirk A/B (Intermediate/Advanced)	Julia Lee A/B (Security and Workshops)
	15 **Contribute to Wireshark – the low hanging fruits** Uli Heilmeier	**16** **Analyzing capture files in Python with PyShark** Dor Green	**17** **Visualizing and Decrypting TLS 1.3** Ross Bagurdes
11:30-11:45	BREAK		
11:45-1:00	**18** **The Packet Doctors are in! Packet trace examinations with the experts**		
1:00-2:00	LUNCH		
2:00-3:15	**19** **TCP Conversation Completeness – What it is, how to use it.** Chris Greer	**20** **Advanced dissector features** Roland Knall	**21** **Build Your Own Wireshark Learning Lab – 3 parts** Jeff Carrell
3:15-3:30	BREAK		
3:30-4:45	**22** **The Life of a Packet, The art of the trace file synchronization** Mike Canney	**23** **WFH Update – Analysis of VPN Network Performance** Chris Hull	**Build Your Own Wireshark Learning Lab – continued** Jeff Carrell
4:45-5:00	BREAK		
5:00-6:15	**24** **10 Tools I use that Compliment Wireshark** Anthony Efantis	**25** **TCP SACK Overview and Impact on Performance** John Pittle	**Build Your Own Wireshark Learning Lab – continued** Jeff Carrell
6:30-8:30	**Sponsor Technology Showcase Reception, esPCAPe Group Packet Challenge & Dinner**		
	Q & A		

SharkFest'22 US Conference Agenda

Thursday, July 14			
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		
10:15-11:30	Basie AA1/BB1 (Beginner/Intermediate)	Andy Kirk A/B (Intermediate/Advanced)	Julia Lee A/B (Security and Workshops)
	26 **Packet Capture 101** Jasper Bongertz	**27** **When TCP reassembly gets complicated** Tom Peterson	**28** **When a packet is not a packet** Mike Kershaw
11:30-11:45	BREAK		
11:45-1:00	**29** **Intro to QUIC - The TCP Killer?** Chris Greer	**30** **Hands on Deep Dive** Hansang Bae	**DEVELOPER DEN DROP IN** **(In-person/Zoom/Discord)**
1:00-2:00	**A walkthrough of the SharkFest esPCAPe & CTF Challenges**		
2:00-4:00	**Closing Remarks, Challenge Awards and Farewell reception**		

SharkFest'22 US Conference Agenda

Session Abstracts & Instructor Bios

(DRAFT - UPDATED FREQUENTLY)

TUESDAY, JULY 12

9:00-10:00

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

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 Wireshark and WiFi: Multicast Case Study

Multicast traffic requires special handling in the 802.11 space and Wireshark is a great tool to analyze this behavior. This is a case study in multicast gone wrong with WiFi and some of the challenges at finding a mitigation.

Instructor: George Cragg, Network Engineer, Draeger Medical Systems
George Cragg is a full time network engineer for a medical device company. Past careers include tree farmer, designing tire filling machines, and Six-Sigma Black Belt in the semiconductor industry.

03 Dissecting WPA3

Understand next wireless security standard with trace analysis using Wireshark.
We need new security standard in 6/6E generation of WiFi. WPA3 has SAE (Simultaneous Authentication of Equals) authentication handshake and PMF (Protected Management Frames) mechanism. In this session, Megumi shows you WPA3 trace analysis using Wireshark. Follow the packets and understand safe way to use wireless network.

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.

11:45-1:00

04 Build Your Own: Remotely accessible packet-capture drop-box for troubleshooting networks with <$100

I'll show you how to take less than $100 worth of network gadgets (stuff you probably already own) and build a packet capture device that can be left behind to help you catch intermittent network issues on or off the grid. When my brother in-law contacted me about a network issue he was having at his home, I finally had a legitimate reason to use all the network gadgets I've been collecting. With a Raspberry-Pi, small NVMe storage and portable network TAP I was able to leave a complete low-power setup at his house continuously capturing packets. I could remote into this device to observe live traffic or come back and retrieve the device for complete packet analysis.

In this talk I'll present the problem set, the environment, and hardware I use and the tools I used, as well as the network issue I was tracking down and ultimately what the solution was.

Instructor: Anthony Efantis, Principal Network Engineer at Sealing Teach

Tony E. is a Principal Network Security Engineer working for a govt contractor servicing the DoD. He has built many global network security architectures and responsible for all layers of the OSI model. Tony holds many industry certifications including: CCIE# 64908, GNFA, PCNSA & SEC+. He maintains a blog @ https://showipintbri.github.io and is the co-host on the Network Collective podcast and live stream: https://networkcollective.com . He enjoys participating in packet hacking challenges and CTF's at security conferences.

05 Duct tape and baling wire: Extending Wireshark with Lua

"There has to be a way to do this" can be quite a time sink in Wireshark. Eventually you may find a solution but often it would be quicker to throw together a small Lua script and get on with solving the original problem.The workshop will go through examples from the Wireshark Ask Q&A site where a piece was missing from Wireshark and a Lua script helped in the solution. The resulting Lua scripts were then added to the Wireshark Wiki Lua Contrib section.

NOTE: The information in SharkFest'15, session 11 (https://sharkfestus.wireshark.org/sf15) is a pre-requisite to this workshop.

Instructor: Chuck Craft

Chuck is a volunteer and contributor on the Wireshark project. His career spans from real-time 68000 Pascal/Assembler programming for Railroad MoW to sales engineer for Fintech, telco and xLA network/security monitoring.

06 Intrusion Analysis and Threat Hunting with Suricata

In today's threat landscape, sophisticated adversaries have routinely demonstrated the ability to compromise enterprise networks and remain hidden for extended periods of time. In Intrusion Analysis and Threat Hunting with Suricata, you will learn how to dig deep into network traffic to identify key evidence that a compromise has occurred, learn how to deal with new forms of attack, and develop the skills necessary to proactively search for evidence of new breaches. We will explore all phases of adversary tactics and techniques - from delivery mechanisms to post-infection traffic and data exfiltration to get hands-on analysis experience. Open-source tools such as Suricata, Moloch and Kibana will be utilized to generate data, perform exhaustive traffic analysis, and develop comprehensive threat hunting strategies. By the end of this course, you will have the knowledge and skills necessary to discover new threats in your network and build an effective threat hunting program.

Instructors: Josh Stroschein, Director of Training and Peter Manev, QA/Trainer, Open Information Security Foundation

Josh is an experienced malware analyst and reverse engineer who has a passion for sharing his knowledge with others. He is the Director of Training for OISF, where he leads all training activity for the foundation and is also responsible for academic outreach and developing research initiatives. Josh is an accomplished trainer, providing training in the aforementioned subject areas at BlackHat, DerbyCon, Toorcon, Hack-In-The-Box, Suricon and other public and private venues. Josh is an Assistant Professor of Cyber Security at Dakota State University where he teaches malware analysis and reverse engineering, an author on Pluralsight, and a threat researcher for HP Wolf Security.

Peter has been involved with Suricata IDS/IPS/NSM from its very early days in 2009 as QA lead, currently a Suricata executive council member. Peter has 15 years' experience in the IT industry, including enterprise and government level IT security practice. As an adamant admirer and explorer of innovative open source security software he is also one of the creators of SELKS - an open source threat detection security distro. He is also one of the founders of Stamus Networks, a company providing security solutions based on Suricata.

2:15-3:30

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 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

Mark is Principle Engineer for T-Mobile, focused on 4G, and 5G EPC nodes. He served as one of the first members to launch Sprints LTE service in 2009, and support 5G standalone today. Authored 3GPP contributions for the 23, and 29 series.

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 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.

11 Using Wireshark to learn IPv6

IPv6 is new or not as well known to many in IT. Many technologists use Wireshark to validate network operations and troubleshoot network issues. This hands-on session will cover IPv6 basics and then dive into configuring Wireshark to assist in viewing IPv6 more effectively. Wireshark configuration profiles, display filters, and color rules will be discussed and demonstrated to aid the understanding of what you will be seeing.

Everyone is encouraged to bring their own laptop with Wireshark loaded as this will also be a hands-on/follow Jeff session where attendees will be able to load trace files in order to fully experience the conveyed topics.

Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enterprise

Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.

12 Abusing the Network – An Overview of Malicious Network Activity and How to Detect It

Nearly every cyber-attack is facilitated by the network, from initial delivery to lateral movement, command and control and data exfiltration. In this talk, we'll look at how malware authors use and abuse the network to achieve their malicious activity. We'll take a deep dive into the network traffic to get a better understanding of how this activity can be detected and understood. We'll use industry standard network monitoring and inspection tools such as Wireshark, Suricata and Arkime to aide us along our journey. We will also spend time exploring how the network traffic is connected to the host-based components, such as executables and scripts, helping to build a more complete picture of the acitivity. By the end of this talk, you'll have explored malicious traffic from a variety of sources and have new insights into how to detect it.

Instructors: Josh Stroschein, Director of Training, Open Information Security Foundation

Josh is an experienced malware analyst and reverse engineer who has a passion for sharing his knowledge with others. He is the Director of Training for OISF, where he leads all training activity for the foundation and is also responsible for academic outreach and developing research initiatives. Josh is an accomplished trainer, providing training in the aforementioned subject areas at BlackHat, DerbyCon, Toorcon, Hack-In-The-Box, Suricon and other public and private venues. Josh is an Assistant Professor of Cyber Security at Dakota State University where he teaches malware analysis and reverse engineering, an author on Pluralsight, and a threat researcher for HP Wolf Security.

5:15-6:30

13 Troubleshoot Like a Doctor

The medical field has been diagnosing people for thousands of years, and it has developed a detailed framework to understand and teach diagnosis. This talk shows how medical diagnostics works and teaches you to apply it to your troubleshooting. If you are already a skilled problem solver, then learn how to better teach others! If some problems feel overwhelming, then learn a proven method to systematically attack the problem!

Instructor: Josh Clark, Distributed Performance Engineer, Huntington National Bank

Josh is a Distributed Performance Engineer at Huntington National Bank, which means he gets to have fun with all the weirdest problems in the most complex systems the bank implements. Wireshark is his tool of choice to figure things out.

14 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.

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.

6:30-8:30

Sponsor Technology Showcase Reception, Treasure Hunt & Dinner

WEDNESDAY, JULY 13

9:00-1:00

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

Keynote: Introducing Logwolf

10:15-11:30

15 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.

16 Analyzing capture files in Python with PyShark

PyShark is a Python library which wraps Wireshark in order to allow handling captures and packets in Python.In this workshop we will learn how to use PyShark to capture packets, to analyze them and access their fields in various ways and other advanced PyShark features. We will build simple utilities which can automate work over packet captures as well as build tools that can be integrated into existing code.

Instructor: Dor Green
Dor Green is the writer and maintainer of PyShark, a popular packet analysis Python package which utilizes Wireshark. He has been working in the cybersecurity field for over a decade, specializing in packet analysis. Currently he is a Technical Lead at Armis Security, which leverages packet analysis (among other things) to provide IoT security to enterprise companies as well as companies in the OT and health fields.

17 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

18 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

19 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

20 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.

21 Build Your Own Wireshark Learning Lab

This 3-part session is about building a no-cost * virtual lab environment specifically targeted to gain experience on using Wireshark to decode many different network protocols, however the lab system can easily be configured/expanded for many different types of uses.

We will cover one specific process of building a lab system based on a virtual machine platform on a Windows 11 host. You may have a Windows 7,8,10 or Linux or Mac based system to use and that is OK, as the main applications are also available for these OSs.

Prior to start of the workshop, you will need to download the main applications and additional files. A list will be made available.

* assumes you have a computer with at least a dual-core processor, 8G RAM, 250G storage, less than 8yrs old (depends on CPU), and it must support VT-x or AMD-V (nested virtualization). More CPU/memory capability available will provide for a better experience.

Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enterprise

Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.

3:30-4:45

22 The Life of a Packet, The art of the trace file synchronization

During this intermediate Wireshark talk, you will learn how to perform a Router, Firewall and Proxy Server impact analysis using Wireshark.

We will walk through how and where you'll need to capture the packets, and how to use Wireshark to analyze individual trace files, and then we'll show you how to synchronize those trace files to present a full path impact analysis.

Multiple use case scenarios will be analyzed:

First, a simple client to cloud-based server scenario (google),

Next, a complex web-based meeting scenario (MS Teams)

Rounding it out, a synchronization of pcaps in a multi-proxy server environment with an in-house developed mission critical application (Dev/Ops example).Come learn how to calculate the impact (on the speed of the packet) of individual network devices as a packet traverses the network.

Instructor: Mike Canney

Over the past 30 years Mike has helped 100's of companies identify and resolve their application and network performance issues. Mike has also developed coursework and taught engineers around the world how to identify, remediate, and prevent network and application issues by analyzing traffic flows at the packet level.

Mike has also invented and patented technologies in the field of measuring latency and congestion as it relates to accurately measuring end user experience.

23 WFH Update - Analysis of VPN Network Performance

Measuring network performance for VPN-connected user is a challenge, and this discussion covers some fo the approaches used to manage performance at a large corporation that went 100% virtual in the third week of March, 2020. Real time monitoring was key, but other techniques including packet analysis, and synthetic testing allowed us to triage and troubleshoot issues. And the problems went beyond just the ISP connectivity and VPN capacity, extending to the security stack and cloud service providers.

In this talk, Chris will go through a variety of strategies to monitor in real time, benchmark and test performance and troubleshoot with a variety of data sources. Packets captured in the datacenter can be a start, but how do you measure packet loss with UDP-based VPNs with DTLS? Can you see those packets outside the VPN tunnel in the datacenter? Or how can you capture the right packets with Wireshark or other agents on the client workstations?

Instructor: Chris Hull, Network Engineer, Capital One

Chris is a network engineer and packet analysis expert, currently working network operations at Capital One. Chris has previously worked at OPNET/Riverbed, first as a developer, and later in professional services. In OPNET, he developed and lead the STAR24 service, where we provided a quick response, guaranteed, application and network performance troubleshooting service. This experience has carried through to Capital One, where he provides network incident top-level escalation analyses and network architecture support. Recent efforts include replacement of network visibility solutions, supporting our now-completed zero datacenter migration and COVID/WFH engineering.

Build Your Own Wireshark Learning Lab – continued

This 3-part session is about building a no-cost * virtual lab environment specifically targeted to gain experience on using Wireshark to decode many different network protocols, however the lab system can easily be configured/expanded for many different types of uses.

We will cover one specific process of building a lab system based on a virtual machine platform on a Windows 11 host. You may have a Windows 7,8,10 or Linux or Mac based system to use and that is OK, as the main applications are also available for these OSs.

Prior to start of the workshop, you will need to download the main applications and additional files. A list will be made available.

* assumes you have a computer with at least a dual-core processor, 8G RAM, 250G storage, less than 8yrs old (depends on CPU), and it must support VT-x or AMD-V (nested virtualization). More CPU/memory capability available will provide for a better experience.

Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enterprise

Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.

5:00-6:15

24 10 Tools I use that Compliment Wireshark

Wireshark is excellent for examining the bits or bytes of packet flows and breaking down protocols but sometimes it isn't the right tool for the job. I'll share my top 10 "go-to's" for when I pivot to Wireshark or pivot away from Wireshark. In this talk I'll go over my top 10 tools I use alongside Wireshark to augment my packet or session analysis. I'll be demonstrating each tool with 1 use case and showcase the unique capabilities of the tools and the why and when I use them.

Instructor: Anthony Efantis, Principal Network Engineer at Sealing Teach

Tony E. is a Principal Network Security Engineer working for a govt contractor servicing the DoD. He has built many global network security architectures and responsible for all layers of the OSI model. Tony holds many industry certifications including: CCIE# 64908, GNFA, PCNSA & SEC+. He maintains a blog @ https://showipintbri.github.io and is the co-host on the Network Collective podcast and live stream: https://networkcollective.com . He enjoys participating in packet hacking challenges and CTF's at security conferences.

25 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 it to performance of the application, using a very interesting case study from an actual customer. TCP SACK is an important performance enhancement to TCP.

Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.

As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.

Build Your Own Wireshark Learning Lab – continued

This 3-part session is about building a no-cost * virtual lab environment specifically targeted to gain experience on using Wireshark to decode many different network protocols, however the lab system can easily be configured/expanded for many different types of uses.

We will cover one specific process of building a lab system based on a virtual machine platform on a Windows 11 host. You may have a Windows 7,8,10 or Linux or Mac based system to use and that is OK, as the main applications are also available for these OSs.

Prior to start of the workshop, you will need to download the main applications and additional files. A list will be made available.

* assumes you have a computer with at least a dual-core processor, 8G RAM, 250G storage, less than 8yrs old (depends on CPU), and it must support VT-x or AMD-V (nested virtualization). More CPU/memory capability available will provide for a better experience.

Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enterprise

Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.

6:30-8:30

Sponsor Technology Showcase Reception, Group Packet Competition & Dinner

THURSDAY, JULY 14

9:00-10:00

SharkBytes

10:15-11:30

26 Packet Capture 101

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.

27 When TCP reassembly gets complicated

Armed with a pcap file, we can examine and analyze the packets that were sent and how they were responded to on the network. We rely on our tools to show us how a TCP stream was reassembled or to give us a list of HTTP websites accessed in a pcap file. But what happens when TCP segments overlap or when new options like TCP Fast Open are used? Does every device and tool reassemble TCP exactly the same in all cases? Are the latest TCP options supported by all of the tools we use? Could this be used to disguise malicious behavior? In this session, we'll look at how TCP packets are processed by operating systems, including Linux and Windows. When these don't match, we'll look at the packets themselves and go over ways to test how the packets are really being processed. If you know how TCP reassembly works when packets are received simply out of order you might be surprised to see what happens when we look at packet scenarios during this session!

Instructor: Tom Peterson, QA Cafe

Tom works at QA Cafe on CloudShark helping bring pcap analysis to the web. Getting started with networking in 2005 performing testing at the InterOperability Lab at UNH, he began by learning IPv6 and moved from there testing IPsec, firewalls, and other network security devices. Testing a variety of protocols and devices has led to a passion of looking for strange behavior in a pcap file and getting to the bottom of it.

28 When a packet is not a packet

From wireless thermometers, weather stations, and tire pressure monitors to airplane collision avoidance, there are thousands of devices which communicate wirelessly but have no network cards and don't use traditional packets. We can still find these devices and capture data using software defined radio, sometimes for as little as $25USD in hardware. An introductory look into existing tools to capture non-traditional wireless data, and even how to start writing your own capture tools.

Instructor: Mike Kershaw, Wi-Fi Hacker. Kismet Wireless

Mike Kershaw is the author of several open source tools, including Kismet, a Wi-Fi and general wireless capture tool and IDS, as well as other open source hardware and software projects, typically related to wireless technologies.

11:45-1:00

29 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

30 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.

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