COURSE ESTIMATOR/QUOTE REQUEST

CHAPPELL UNIVERSITY

Ready to train your team on Wireshark, TCP/IP analysis, troubleshooting, and network forensics? Complete Part 1 of this Cost Estimator and Quote Request Form to determine the cost of training.

Training is available in three formats:

- **Onsite**: [Onsite delivery is temporarily on-hold]
- **Online Live**: instructor-led, lab-based, connected via the Internet - customize with your own traffic files
- **On-Demand**: online recorded, available 24x7, transcripts, one-year All Access Pass subscriptions

Please contact us at info@chappellU.com if you have any questions.

Email completed forms to Pat Thibuney (pat@chappellU.com).

Part 1: Training Project Info (Required for Formal Quotes)

Use this form for group pricing for onsite, online or on-demand training.

Project Title _____

Contact Name _____

Company _____

Phone Number _____

Email Address _____

Billing Address for Quote _____

Desired Course Format
- ☐ Onsite Live
- ☐ Online Live (Virtual)
- ☐ On-Demand (All Access Pass Subscriptions)
- ☐ Other _____

Course Delivery Timeline
- ☐ Within 3 months
- ☐ 3-6 months
- ☐ 6+ months
- ☐ I have specific dates in mind (see next item)

Desired Training Dates _____

Course Location (if known) _____

COURSE ESTIMATOR/QUOTE REQUEST

Number of Students

- ☐ Up to 20 students
- ☐ 21-30 students
- ☐ 31-40 students
- ☐ 41-50 students
- ☐ Over 50 students (estimated student count: _____)

Course Length

- ☐ Less than 2 days (online training option only)
- ☐ 2 days
- ☐ 3 days
- ☐ 4 days
- ☐ 5 days
- ☐ 6 or more days (estimated course length in days: _____)

Course Objective #1 _____

Course Objective #2 _____

Course Objective #3 _____

Additional Elements to Include in Your Training Quote (optional)

- ☐ Pre- and post-course quizzes
- ☐ Discounted All Access Pass Group Subscriptions (1-year subscription)
- ☐ Wireshark Network Analysis book (1 per student)
- ☐ Wireshark 101: Essential Skills for Network Analysts book (1 per student)
- ☐ Wireshark Workbook (1 per student)
- ☐ Troubleshooting with Wireshark book (1 per student)
- ☐ WCNA - Certified Network Analyst Exam Prep Guide (1 per student)
- ☐ Follow-up Live Online Webinar
- ☐ WCNA Exam Vouchers (onsite or online proctored)
- ☐ Other: _____

Will you provide trace files for further customization of the training material?

- ☐ Yes
- ☐ No
- ☐ Unknown

Other Requests or Comments _____

_____

_____

Note: Your course can (a) focus explicitly on troubleshooting, (b) have some network forensics woven throughout, or (c) focus explicitly on network forensics. See ***Network Troubleshooting vs. Network Forensics*** on page 11.

Part 2: Design Your Course Content

Please let us know what topics you would like covered in your custom course.

Section 1	☐ **All items in this section**
Network Analysis Overview	☐ Troubleshooting Tasks for the Network Analyst
	☐ Security Tasks for the Network Analyst
	☐ Application Analysis Tasks for the Network Analyst
	☐ Security Issues Related to Network Analysis
	☐ Legal Issues Related to Listening to Network Traffic
	☐ Overcome the "Needle in a Haystack" Issue
	☐ Example of a Network Analysis Session from Symptoms to Resolution
	☐ Other: _____
Section 2	☐ **All items in this section**
Wireshark Essentials	☐ Capturing Packets on Wired or Wireless Networks
	☐ Working with Trace Files from Other Capture Devices - Wiretap Library
	☐ How Wireshark Processes Packets – Drivers, Dissectors, Filters, Plugins
	☐ Qt Interface Elements (Menus, Linked Panes, Toolbars, Areas)
	☐ Related Packets Indicator, Intelligent Scrollbar, and Status Bar
	☐ Wireshark Installation Options, Executable Files, and Configuration Files
	☐ Accessing the Wireshark Code, Updates, Q&A Site, and Bug Tracker
	☐ The First Step: Customizing Wireshark with a Profile
	☐ Efficiency: Right-Click, Click-and-Drag, and Accelerators
	☐ Building Your First Display Filter Button
	☐ Other: _____
Section 3	☐ **All items in this section**
Capture Techniques	☐ Where to Tap into the Network–Wired/WLAN, Duplex Issues, Switches
	☐ Endpoint vs. Midpoint Capture Locations
	☐ Work with Multipoint Captures
	☐ Proxy TLS Capture Options (Capture Decrypted Traffic)
	☐ Using File Sets and Optimizing for Large Capture Quantity
	☐ Unattended Capture Techniques (File Sets, Ring Buffer)
	☐ Conserve Memory with Command-line Capture (tshark, dumpcap)
	☐ Using and Adding to the Default Capture Filters (Filter by Protocol, Address, Host)
	☐ Advanced: Capture Filters (Operators and Byte Offset Filtering)

Section 4

Wireshark Customization and Navigation

- ☐ **All items in this section**
- ☐ Advanced: Custom Profile Elements, Directories, and Import/Export
- ☐ Customize Your User Interface Settings
- ☐ Working with Columns for Efficient Analysis
- ☐ Define Your Capture Preferences
- ☐ Define IP and MAC Name Resolution
- ☐ Options for Network Name Resolution
- ☐ VLAN Name Resolution Configuration
- ☐ Manual Name Resolution
- ☐ GeoIP Configuration and Use
- ☐ Define TCP, HTTP, TLS, and Other Protocol Settings
- ☐ Navigation (Find, Sort, Jump)
- ☐ Use Colors to Distinguish Traffic (Coloring Rule Naming for Filter Use)
- ☐ Mark Packets for Performance Comparison
- ☐ Temporary Coloring for Stream Separation
- ☐ Trace File/Packet Annotations and Report Generation
- ☐ Dealing with Applications Running over Non-Standard Port Numbers
- ☐ Following Streams/Reassembly Techniques
- ☐ Other: _____

Section 5

Troubleshoot with Time Values and Summary Information

- ☐ **All items in this section**
- ☐ Alter the Default Time Column (Granularity and Display)
- ☐ Measure Roundtrip Time and Path Latency (iRTT Introduction)
- ☐ Adding Key Time Columns
- ☐ Analyze Application Response Times (DNS, HTTP, SMB/SMB2, etc.)
- ☐ Acceptable vs. Unacceptable Delays
- ☐ Using Time References
- ☐ Other: _____

Section 6

Interpret Basic Trace File Statistics to Identify Trends

- ☐ **All items in this section**
- ☐ Capture File Properties (Information, Annotation, and Comparisons)
- ☐ Identify Protocols and Applications in Use
- ☐ Detect Suspicious Applications and Undissected Traffic
- ☐ Build an Essential IO Graph (aka the "Golden Graph")
- ☐ Identify the Most Active Conversations/Endpoints
- ☐ List Conversations or Endpoints for Specific Traffic Types
- ☐ List All UDP and TCP Ports Used
- ☐ Review Additional Statistics
- ☐ Other: _____

Section 7

Create and Apply Display Filters for Efficient Analysis

- ☐ **All items in this section**
- ☐ Create Display Filters Using Auto Complete
- ☐ Manage Saved Display Filters (*dfilters* file)
- ☐ Filter on Conversations, Endpoints, and Protocols
- ☐ Filter Based on Time Values
- ☐ Build Display Filters Based on Fields
- ☐ Combine Display Filters with Comparison and Logical Operators
- ☐ Contrast *any* Filters and *all* Filter Types
- ☐ Alter Display Filter Meaning with Parentheses
- ☐ Using PERL-Compatible Regular Expressions (PCRE)
- ☐ Advanced: Filter on Specific Bytes in a Packet (Byte-Offset Filtering)
- ☐ Advanced: The Slice Offset
- ☐ Advanced: Negative Slice Offset
- ☐ Advanced: Bit-Masking
- ☐ Advanced: Combine Slice Offset and Bit-Masking
- ☐ Organize Display Filter Buttons (Categories)
- ☐ Import/Export Display Filters and Display Filter Buttons
- ☐ Correct Common Display Filter Mistakes
- ☐ Other: _____

Section 8	☐ **All items in this section**
Follow Streams and Reassemble Data	☐ Follow and Reassemble UDP Conversations
	☐ Follow and Reassemble TCP Conversations
	☐ Follow and Reassemble HTTP Conversations
	☐ Use Reassembly to Identify the Purpose of Undissected Traffic
	☐ Use Reassembly to Extract Files Transferred Across a Network (“Carving”)
	☐ Identify Common File Types Based on File Identifiers
	☐ Follow and Reassemble TLS Conversations
	☐ Other: _____
Section 9	☐ **All items in this section**
TCP/IP Traffic Analysis Overview - Resolutions	☐ Define Basic TCP/IP Functionality
	☐ Define the Multistep Resolution Process
	☐ Define Port Number Resolution
	☐ Define Network Name Resolution
	☐ Define Location Resolution and CIDR Usage
	☐ Define Local MAC Address Resolution for a Target (IPv4 vs. IPv6)
	☐ Define Local MAC Address Resolution for a Gateway (IPv4 vs. IPv6)
	☐ Advanced: Mask Too Short Issue/Traffic Patterns (ARP)
	☐ Advanced: Mask Too Long Issue/Traffic Patterns (ICMP)
	☐ Other: _____
Section 10	☐ **All items in this section**
Analyze Domain Name System (DNS) Traffic	☐ Analyze Normal DNS Queries/Responses (Record Types/Reply Codes)
	☐ Analyze Unusual DNS Queries/Responses
	☐ Field-by-Field: Dissect the DNS Packet Structure
	☐ Common DNS Filter Mistakes
	☐ Identify DNS Faults with Display Filter Buttons
	☐ Measure DNS Response Times
	☐ Overview of DNS-over-HTTP (DoH) Functionality/Security
	☐ Overview of DNS-over-TLS (DoT) Functionality/Security
	☐ Other: _____

Section 11	☐ **All items in this section**
Analyze Address Resolution Protocol (ARP) Traffic	☐ Analyze Normal ARP Requests/Responses
	☐ Analyze Unusual ARP Requests/Responses
	☐ Field-by-Field: Dissect the ARP Packet Structure
	☐ Analyze ARP Probes, ARP Announcements, and Gratuitous ARP
	☐ Security: Non-Zero ARP Padding Issue
	☐ Other: _____
Section 12	☐ **All items in this section**
Analyze Internet Protocol (IPv4) Traffic	☐ Analyze Normal IPv4 Traffic
	☐ Analyze Unusual IPv4 Traffic
	☐ Field-by-Field: Dissect the IPv4 Header Structure
	☐ Set Your IP Protocol Preferences
	☐ Identify Issues Related to Fragmentation and Reassembly
	☐ Identify Black Hole Detection Blocking Issues
	☐ Analyze the Use of Differentiated Services Code Point (DSCP)
	☐ Examine Explicit Congestion Notification Bits
	☐ Identify Multicast, Broadcast, and Loopback Addresses
	☐ Other: _____
Section 13	☐ **All items in this section**
Analyze Internet Control Messaging Protocol (ICMP) Traffic	☐ Analyze Normal ICMP Traffic
	☐ Analyze Unusual ICMP Traffic
	☐ Field-by-Field: Dissect the ICMP Packet Structure
	☐ Service Refusal Detection – Destination Unreachable
	☐ ICMP Black Hole Detection Trace File Analysis
	☐ Interpretation of Registered ICMP Types and Codes
	☐ Analyze an ICMP-based Traceroute Process
	☐ Analyze Suspicious ICMP Traffic (Indications of Scanning)
	☐ Other: _____

Section 14

Analyze User Datagram Protocol (UDP) Traffic

- ☐ **All items in this section**
- ☐ Analyze Normal UDP Traffic
- ☐ Analyze Unusual UDP Traffic
- ☐ Field-by-Field: Dissect the UDP Header Structure
- ☐ Work with UDP Stream Index Values
- ☐ Analyze UDP Delta Timestamps
- ☐ Analyze UDP-based Multicast Video Streams
- ☐ Use UDP to Differentiate Queuing Along a Path from Packet Loss
- ☐ Other: _____

Section 15

Analyze Transmission Control Protocol (TCP) Traffic

- ☐ **All items in this section**
- ☐ Analyze Normal TCP Communications
- ☐ Analyze Unusual TCP Communications (Packet Loss, Congestion, etc.)
- ☐ Field-by-Field: Dissect the TCP Header Structure
- ☐ Learn How TCP Segmentation Offload Can Affect Your Analysis
- ☐ Work with TCP Stream Index Values
- ☐ Analyze Various TCP Connections (3-Way Handshakes) and TCP Options
- ☐ Define How TCP-Based Services are Refused
- ☐ Service Refusals Identification: Endpoints vs. Midpoints
- ☐ TCP Timestamp Analysis
- ☐ TCP Initial Round Trip Time (and Retransmission Timeout/Out-of-Order Issues)
- ☐ TCP Sequential Byte Tracking (Sequence, Acknowledgment Numbers)
- ☐ Examine Explicit Congestion Notification Bits in the TCP Header
- ☐ Packet Loss Detection and Recovery (RTO vs. Fast Retransmission)
- ☐ Retransmissions vs. Fast Retransmissions vs. Spurious Retransmissions
- ☐ Dealing with Out-of-Order Indications (False Positives vs. Accurate Detections)
- ☐ TCP Selective ACK (SACK) Analysis
- ☐ Define TCP Flow Control (Receiver Congestion, Congestion Window, Sliding Window)
- ☐ TCP Window Scaling Analysis and Issues
- ☐ Set TCP Protocol Preferences (Reassembly)
- ☐ Graph TCP Streams (tcptrace Time-Sequence, RTT, Throughput, Window Scaling)
- ☐ IO Graph using Y-Axis Operators and Y-Field Values (MIN, AVG, MAX, SUM, etc.)
- ☐ Multipoint Capture and Detection of Infrastructure Device Problems
- ☐ Other: _____

Section 16

Use Wireshark's Expert System to Identify Anomalies

- ☐ **All items in this section**
- ☐ Malformed Frames
- ☐ DNS Retransmissions
- ☐ ARP Duplicate Address Detection
- ☐ Reserved Fields with Non-Zero Values
- ☐ Filter on TCP Expert Information Elements
    - ☐ Expert Info: tcp_analysis_retransmission
    - ☐ Expert Info: tcp_analysis_fast_retransmission
    - ☐ Expert Info: tcp_analysis_spurious_retransmission
    - ☐ Expert Info: tcp_analysis_out_of_order
    - ☐ Expert Info: tcp_analysis_reused_ports
    - ☐ Expert Info: tcp_analysis_lost_segment
    - ☐ Expert Info: tcp_analysis_ack_lost_segment
    - ☐ Expert Info: tcp_analysis_window_update
    - ☐ Expert Info: tcp_analysis_window_full
    - ☐ Expert Info: tcp_analysis_keep_alive
    - ☐ Expert Info: tcp_analysis_keep_alive_ack
    - ☐ Expert Info: tcp_analysis_duplicate_ack
    - ☐ Expert Info: tcp_analysis_zero_window
    - ☐ Expert Info: tcp_analysis_zero_window_probe
    - ☐ Expert Info: tcp_analysis_zero_window_probe_ack
- ☐ Interpret Developer Comments in the Wireshark Code
- ☐ Other: _____

Section 17

Analyze Dynamic Host Configuration Protocol (DHCP) Traffic

- ☐ **All items in this section**
- ☐ Analyze Normal DHCP Traffic (Inside/Outside Lease Times)
- ☐ Analyze Unusual DHCP Traffic
- ☐ Field-by-Field: Dissect the DHCP Packet Structure
- ☐ Lease Time (LT), Renew Time (T1), and Rebind Time (T2)
- ☐ Analyze Relay Agent Use
- ☐ Other: _____

Section 18

Analyze Common Hypertext Transfer Protocol (HTTP/HTTPS) Traffic

- ☐ **All items in this section**
- ☐ Analyze Normal HTTP Communications
- ☐ Analyze Unusual HTTP Communications
- ☐ Field-by-Field: Dissect the HTTP Header Structure
- ☐ Filter on HTTP and HTTPS Traffic
- ☐ Export and Display HTTP Objects (Reassembly)
- ☐ Graph HTTP Traffic Flows
- ☐ HTTP Response Time Measurement
- ☐ HTTP Statistics
- ☐ HTTP/2 Overview
- ☐ HTTP/2 Dissection and Separation of Streams
- ☐ HTTP/2 Error Responses
- ☐ Other: _____

Section 19

Analyze Transport Layer Security (TLS)

- ☐ **All items in this section**
- ☐ Analyze the TLS Handshake Process (TLS Version Comparison)
- ☐ Key TLS Filters
- ☐ Essential TLS Fields
- ☐ Using the TLS ALPN Field(s)
- ☐ Decrypt HTTPS Traffic Using an RSA Key
- ☐ Decrypt HTTPS Traffic Using a Session Key
- ☐ Embedding/Discarding/Extracting the Session Keys
- ☐ Analyzing TLS Connection Issues
- ☐ Other: _____

Section 20

Analyze File Transfer Protocol (FTP) Traffic

- ☐ **All items in this section**
- ☐ Analyze Normal FTP Communications
- ☐ Analyze Unusual FTP Communications
- ☐ Detect FTP Error Responses
- ☐ Analyze FTP Active Mode Communications
- ☐ Analyze FTP Passive Mode Communications
- ☐ Reassemble FTP Data Transfers
- ☐ Colorize FTP Commands
- ☐ Other: _____

Section 21 **Voice over IP (VoIP) Analysis Fundamentals**	☐ **All items in this section** ☐ Define VoIP Traffic Flows ☐ Analyze SIP Call Setup Traffic ☐ Examine RTP Call Traffic ☐ Detect if DSCP is Affecting Directional Traffic Flows ☐ Analyze VoIP Problems and Error Response Codes ☐ Playback Unencrypted VoIP Calls ☐ Simulate Jitter Buffer Issues ☐ Other: _____
Section 22 **Use Command-Line Tools**	☐ **All items in this section** ☐ Use Wireshark.exe (Command-Line Launch) ☐ Capture Traffic with Tshark ☐ Capture Traffic with Dumpcap ☐ List Trace File Details with Capinfos ☐ Edit Trace Files with Editcap ☐ Merge Trace Files with Mergecap ☐ Other: _____
Network Troubleshooting vs. Network Forensics	Your course can focus on troubleshooting only, some network forensics, or primarily network forensics. If your focus is network forensics, the topics listed in Sections 23-27 will be woven through the appropriate protocol deep dive sections.
Section 23 **Network Forensics Fundamentals**	☐ **All items in this section** ☐ Methodology and Wireshark Use ☐ The “Good Traffic” Rule ☐ Anomaly and Signature Locations ☐ Capture Location and Methods ☐ Methods for Avoiding Capture Detection ☐ Essential Capture Filters ☐ Offset and String-Matching Capture Filters ☐ Building a Network Forensics Profile ☐ Detect Active Applications and Hosts ☐ Right-Click Features Used for Network Forensics ☐ Using the Expert to Detect Anomalies ☐ Exporting Traffic Subsets from Large Trace Files

☐ Using GeoIP Mapping
☐ Data Carving and Object Reassembly
☐ Annotating for a Network Forensics Report
☐ Display Filter Essentials for Network Forensics
☐ Applying Conversation Filters
☐ Building and Applying Compound Filters
☐ Keyword Filtering
☐ Advanced: PERL-Compatible Regular Expression (Regex) Filters for Network Forensics
☐ Turn Network Forensic Filters into Buttons
☐ Colorize Unusual Traffic Patterns
☐ Check out Complementary Forensic Tools
☐ Other: _____

Section 24

Detect Scanning and Discovery Processes

☐ **All items in this section**
☐ Detect ARP Scans (aka ARP Sweeps)
☐ Detect ICMP Ping Sweeps
☐ Detect Various Types of TCP Port Scans
☐ Detect UDP Port Scans
☐ Detect IP Protocol Scans
☐ Define Idle Scans
☐ Know Your ICMP Types and Codes
☐ Analyze Traceroute Path Discovery
☐ Detect Dynamic Router Discovery
☐ Define Application Mapping Processes
☐ Use Wireshark for Passive OS Fingerprinting
☐ Detect Active OS Fingerprinting
☐ Identify Spoofed Addresses and Scans
☐ Other: _____

Section 25

Analyze Suspect Traffic

☐ **All items in this section**
☐ Define Suspicious Traffic Types
☐ Identify Vulnerabilities in the TCP/IP Resolution Processes
☐ Identify Unacceptable Traffic
☐ Locate .exe, .zip, .jar Files in Trace Files Using Regular Expressions
☐ Find Maliciously Malformed Packets
☐ Identify Invalid or Dark Destination Addresses

☐ Differentiate between Flooding or Standard Denial of Service Traffic
☐ Find Clear Text Passwords and Data
☐ Identify Phone-Home Behavior
☐ Catch Unusual Protocols and Applications
☐ Detect and Analyze Applications that Use Non-Standard Port Numbers
☐ Locate Route Redirection that Uses ICMP
☐ Catch ARP Poisoning
☐ Catch IP Fragmentation and Overwriting
☐ Spot TCP Splicing
☐ Watch Other Unusual TCP Traffic
☐ Identify Password Cracking Attempts
☐ Other: _____

LABS

Troubleshooting and Network Forensics in Action (Sample Lab List)

Courses include related hands-on labs – you can request specific labs, if desired.

☐ Create Your Troubleshooting/Network Forensics Profile
☐ Use GeoIP Mapping to Find an Issue
☐ Build a Coloring Rule to Differentiate DNS Traffic
☐ Detect and Differentiate Delays
☐ Find the Top Talkers and Protocols/Applications on a Network
☐ Create and Use an I/O Graph to Spot Performance Issues
☐ Practice Display Filtering
☐ Catch DNS Errors and Slow DNS Responses
☐ Find the Fault – Network Disconnects
☐ Filter on Problem Addresses
☐ Analyze and Color ICMP Traffic
☐ Analyze UDP-based Multicast Streams and Queuing Delays
☐ Use an IO Graph to Locate TCP Performance Issues
☐ Determine the Cause of Slow Page Loading
☐ Create a Button to Detect HTTP Error Responses
☐ Export an HTTP Object (Carving)
☐ Decrypt HTTPS Communications
☐ Evaluate, Extract, and Capture with CLI Tools
☐ Identify Site Dependencies
☐ Detect Suspicious Endpoint Locations with GeoIP Mapping
☐ Apply Names to Suspect Hosts

☐ Build a Coloring Rule to Differentiate DNS Traffic
☐ Detect and Identify Malicious Downloads
☐ Locate a Compromised Host with Emerging Threats Signature
☐ Interpret a Russian Connection
☐ Detect a Bot-Infected Host and C2 Traffic
☐ Identify Exfiltration and Poisoning
☐ Identify Blacklisted IP Addresses
☐ Detect and Annotate Suspicious ICMP Traffic
☐ Locate UDP-Based Scans
☐ Detect Suspicious TCP Traffic
☐ Apply, Inject, and Export TLS Secrets
☐ Identify Interesting and Suspicious TCP and HTTP Traffic
☐ Merge, Split, and Extract Suspect Traffic

New Additions

☐ QUIC analysis
☐ Bundle v7 Analysis (Interplanetary Internet)
☐ Licklider Transport Protocol (LTP) Analysis (Interplanetary Internet)
☐ Overview of Interplanetary Internet Communications using Bundle v7

Extra Hands-On Lab Exercises

By default, your custom course will include hands-on labs. If you would like to add more labs, the length of the course will be affected. We will estimate the course length based on the sections/topics selected on this document. If you have a set maximum number of course days, we will inform you if your lab count causes the course to extend past the desired course length.

Number of labs desired: _____

Focus of Extra Labs: _____

Additional Course Requests

_____
_____
_____
_____
_____
_____

SAVE THIS FORM after filling it out. Email your completed form to Pat Thibuney (pat@chappellU.com) to receive a formal quote after we review your request.