



Wireshark® Workbook 1

Practice, Challenges, and Solutions

Answer Sheets

This Answer Sheets document matches the lab list in *Wireshark Workbook 1: Practice, Challenges, and Solutions*. This document offers a more organized, efficient method for answering the lab questions rather than writing in a book or just jotting your answers on a blank sheet of paper.



Wireshark® Workbook 1

Practice, Challenges, and Solutions

Laura Chappell

Founder, Chappell University™

Creator of the WCNA Certification Program

(formerly referred to as the Wireshark Certified Network Analyst program)

Edited by James Aragon

*Always ensure you have proper authorization
before you listen to or capture network traffic.*

Protocol Analysis Institute, Inc.
59 Damonte Ranch Parkway, #B340
Reno, NV 89521 USA

Chappell University
info@chappellU.com
www.chappellU.com

Copyright Notice

Copyright 2020, Protocol Analysis Institute, Inc., dba Chappell University. All rights reserved. No part of this book, or related materials, may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording, or otherwise) without the prior written permission of the publisher.

To arrange bulk purchase discounts for sales promotions, events, training courses, or other purposes, please contact Chappell University (info@chappellU.com).

Wireshark® Workbook 1: Practice, Challenges, and Solutions ISBN10: 1-893939-63-4

Wireshark® Workbook 1: Practice, Challenges, and Solutions ISBN13: 978-1-893939-64-6

(Version 1.0a)

Distributed worldwide for Chappell University through Protocol Analysis Institute, Inc. Protocol Analysis Institute, Inc. is the educational materials distributor for Chappell University.

For general information on Chappell University or Protocol Analysis Institute, Inc., including information on corporate licenses, updates, future titles, or courses, contact the Protocol Analysis Institute, Inc., at info@chappellu.com.

For authorization to photocopy items for corporate, personal, or educational use, contact Protocol Analysis Institute, Inc., at info@chappellu.com.

Trademarks. All brand names and product names used in *Wireshark® Workbook 1: Practice, Challenges, and Solutions* and related documents are trade names, service marks, trademarks, or registered trademarks of their respective owners. Wireshark and the “fin” logo are registered trademarks of the Wireshark Foundation. At the time *Wireshark® Workbook 1: Practice, Challenges, and Solutions* book was written, the Wireshark Foundation, Inc., only had Riverbed senior management as Officers and members of the Board of Directors. I guess Wireshark is owned by Riverbed. Sigh. Shame on you, Riverbed.

Limit of Liability/Disclaimer of Warranty. The author and publisher have used their best efforts in preparing *Wireshark® Workbook 1: Practice, Challenges, and Solutions* book and the related materials. Protocol Analysis Institute, Inc., Chappell University, and the author(s) make no representations or warranties of merchantability of fitness for a particular purpose. Protocol Analysis Institute, Inc., and Chappell University assume no liability for any damages caused by following the instructions or using the techniques or tools listed in *Wireshark® Workbook 1: Practice, Challenges, and Solutions* and related materials. Protocol Analysis Institute, Inc., Chappell University, and the author(s) make no representations or warranties that extend beyond the descriptions contained in this paragraph. No warranty may be created or extended by sales representatives or written sales materials. The accuracy or completeness of the information provided herein and the opinions stated herein are not guaranteed or warranted to produce any particular result and the advice and strategies contained herein may not be suitable for every individual. Protocol Analysis Institute, Inc., Chappell University, and the author(s) shall not be liable for any loss of profit or any other damages, including without limitation, special, incidental, consequential, or other damages.

Copy Protection. In all cases, reselling or duplication of *Wireshark® Workbook 1: Practice, Challenges, and Solutions* and related materials without explicit written authorization is expressly forbidden. We will find you, ya know. So don't steal or plagiarize stuff.

Lab 1: Wireshark Warm-Up

Lab 1 - Q1. _____

Lab 1 - Q2. _____

Lab 1 - Q3. _____

Lab 1 - Q4. _____

Lab 1 - Q5. _____

Lab 1 - Q6. _____

Lab 1 - Q7. _____

Lab 1 - Q8. _____

Lab 1 - Q9. _____

Lab 1 - Q10. _____

Lab 1 - Q11. _____

Lab 1 - Q12. _____

Lab 1 - Q13. _____

Lab 1 - Q14. _____

Lab 1 - Q15. _____

Lab 1 - Q16. _____

Lab 1 - Q17. _____

Lab 1 - Q18. _____

Lab 1 - Q19. _____

Lab 1 - Q20. _____

Lab 1 - Q21. _____

Lab 1 - Q22. _____

Lab 1 - Q23. _____

Lab 1 - Q24. _____

Lab 1 - Q25. _____

Lab 2: Proxy Problem

Lab 2 - Q1. _____

Lab 2 - Q2. _____

Lab 2 - Q3. _____

Lab 2 - Q4. _____

Lab 2 - Q5. _____

Lab 2 - Q6. _____

Lab 2 - Q7. _____

Lab 2 - Q8. _____

Lab 2 - Q9. _____

Lab 2 - Q10. _____

Lab 2 - Q11. _____

Lab 2 - Q12. _____

Lab 2 - Q13. _____

Lab 3: HTTP vs. HTTPS

Lab 3 - Q1. _____

Lab 3 - Q2. _____

Lab 3 - Q3. _____

Lab 3 - Q4. _____

Lab 3 - Q5. _____

Lab 3 - Q6. _____

Lab 3 - Q7. _____

Lab 3 - Q8. _____

Lab 3 - Q9. _____

Lab 3 - Q10. _____

Lab 4: TCP SYN Analysis

Lab 4 - Q1. _____

Lab 4 - Q2. _____

Lab 4 - Q3. _____

Lab 4 - Q4. _____

Lab 4 - Q5. _____

Lab 4 - Q6. _____

Lab 4 - Q7. _____

Lab 4 - Q8. _____

Lab 4 - Q9. _____

Lab 4 - Q10. _____

Lab 4 - Q11. _____

Lab 4 - Q12. _____

Lab 4 - Q13. _____

Lab 4 - Q14. _____

Lab 4 - Q15. _____

Lab 4 - Q16. _____

Lab 5: TCP SEQ/ACK Analysis

Lab 5 - Q1. _____

Lab 5 - Q2. _____

Lab 5 - Q3. _____

Lab 5 - Q4. _____

Lab 5 - Q5. _____

Lab 5 - Q6. _____

Lab 5 - Q7. _____

Lab 5 - Q8. _____

Lab 5 - Q9. _____

Lab 5 - Q10. _____

Lab 5 - Q11. _____

Lab 5 - Q12. _____

Lab 5 - Q13. _____

Lab 5 - Q14. _____

Lab 5 - Q15. _____

Lab 5 - Q16. _____

Lab 5 - Q17. _____

Lab 5 - Q18. _____

Lab 5 - Q19. _____

Lab 6: You're Out of Order!

Lab 6 - Q1. _____

Lab 6 - Q2. _____

Lab 6 - Q3. _____

Lab 6 - Q4. _____

Lab 6 - Q5. _____

Lab 6 - Q6. _____

Lab 6 - Q7. _____

Lab 6 - Q8. _____

Lab 6 - Q9. _____

Lab 6 - Q10. _____

Lab 6 - Q11. _____

Lab 6 - Q12. _____

Lab 6 - Q13. _____

Lab 6 - Q14. _____

Lab 6 - Q15. _____

Lab 6 - Q16. _____

Lab 6 - Q17. _____

Lab 6 - Q18. _____

Lab 6 - Q19. _____

Lab 6 - Q20. _____

Lab 6 - Q21. _____

Lab 6 - Q22. _____

Lab 6 - Q23. _____

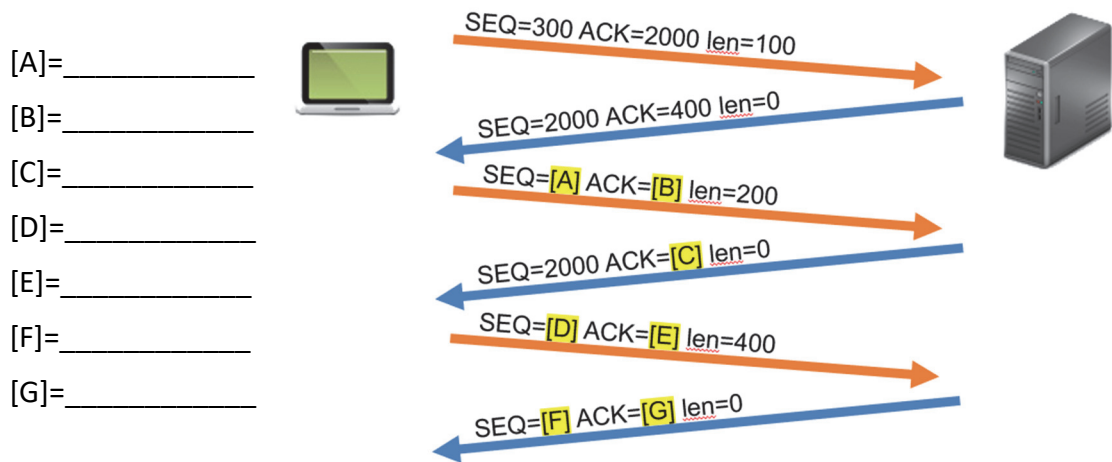
Quick Test 1

Let's see where you are on the filters at this point. Write in the display filter for each of the desired traffic.

Traffic to View	Display Filter
SYN packets only	
SYN/ACK packets only	
SYN or SYN/ACK packets	
DNS responses	
TCP Resets	
SACK option in the TCP handshake packets	
DNS queries over IPv6	

Quick Test 2

Let's see how you are doing with the TCP Sequence/Acknowledgment numbering process. Enter the missing number for the image below. Check your answers against the answers on page **Error! Bookmark not defined.**



Lab 7: Sky High

Lab 7 - Q1. _____

Lab 7 - Q2. _____

Lab 7 - Q3. _____

Lab 7 - Q4. _____

Lab 7 - Q5. _____

Lab 7 - Q6. _____

Lab 7 - Q7. _____

Lab 7 - Q8. _____

Lab 7 - Q9. _____

Lab 7 - Q10. _____

Lab 7 - Q11. _____

Lab 7 - Q12. _____

Lab 7 - Q13. _____

Lab 7 - Q14. _____

Lab 7 - Q15. _____

Lab 7 - Q16. _____

Lab 7 - Q17. _____

Lab 7 - Q18. _____

Lab 8: DNS Warm-Up

Lab 8 - Q1. _____

Lab 8 - Q2. _____

Lab 8 - Q3. _____

Lab 8 - Q4. _____

Lab 8 - Q5. _____

Lab 8 - Q6. _____

Lab 8 - Q7. _____

Lab 8 - Q8. _____

Lab 8 - Q9. _____

Lab 8 - Q10. _____

Lab 8 - Q11. _____

Lab 9: Hacker Watch

Lab 9 - Q1. _____

Lab 9 - Q2. _____

Lab 9 - Q3. _____

Lab 9 - Q4. _____

Lab 9 - Q5. _____

Lab 9 - Q6. _____

Lab 9 - Q7. _____

Lab 9 - Q8. _____

Lab 9 - Q9. _____

Lab 9 - Q10.

Lab 10: Timing is Everything

Lab 10 - Q1. _____

Lab 10 - Q2. _____

Lab 10 - Q3. _____

Lab 10 - Q4. _____

Lab 10 - Q5. _____

Lab 10 - Q6. _____

Lab 10 - Q7. _____

Lab 10 - Q8. _____

Lab 10 - Q9. _____

Lab 10 - Q10. _____

Lab 10 - Q11. _____

Lab 10 - Q12. _____

Lab 10 - Q13.

Lab 11: The News

Lab 11 - Q1. _____

Lab 11 - Q2. _____

Lab 11 - Q3. _____

Lab 11 - Q4. _____

Lab 11 - Q5. _____

Lab 11 - Q6. _____

Lab 11 - Q7. _____

Lab 11 - Q8. _____

Lab 11 - Q9. _____

Lab 11 - Q10. _____

Lab 11 - Q11. _____

Lab 11 - Q12. _____

Lab 12: Selective ACKs

Lab 12 - Q1. _____

Lab 12 - Q2. _____

Lab 12 - Q3. _____

Lab 12 - Q4. _____

Lab 12 - Q5. _____

Lab 12 - Q6. _____

Lab 12 - Q7. _____

Lab 12 - Q8. _____

Lab 12 - Q9. _____

Lab 12 - Q10. _____

Lab 12 - Q11. _____

Lab 12 - Q12. _____

Lab 12 - Q13. _____

Lab 12 - Q14. _____

Lab 12 - Q15. _____

Lab 12 - Q16. _____

Lab 12 - Q17. _____

Lab 12 - Q18. _____

Lab 12 - Q19. _____

Lab 12 - Q20. _____

Lab 12 - Q21. _____

Lab 13: Just DNS

Lab 13 - Q1. _____

Lab 13 - Q2. _____

Lab 13 - Q3. _____

Lab 13 - Q4. _____

Lab 13 - Q5. _____

Lab 13 - Q6. _____

Lab 13 - Q7. _____

Lab 13 - Q8. _____

Lab 13 - Q9. _____

Lab 13 - Q10. _____

Lab 13 - Q11. _____

Lab 13 - Q12. _____

Lab 13 - Q13. _____

Lab 13 - Q14. _____

Lab 13 - Q15. _____

Lab 13 - Q16. _____

Lab 13 - Q17. _____

Lab 14: Movie Time

Lab 14 - Q1. _____

Lab 14 - Q2. _____

Lab 14 - Q3. _____

Lab 14 - Q4. _____

Lab 14 - Q5. _____

Lab 14 - Q6. _____

Lab 14 - Q7. _____

Lab 14 - Q8. _____

Lab 14 - Q9. _____

Lab 14 - Q10. _____

Lab 14 - Q11. _____

Lab 15: Crafty

Lab 15 - Q1. _____

Lab 15 - Q2. _____

Lab 15 - Q3. _____

Lab 15 - Q4. _____

Lab 15 - Q5. _____

Lab 15 - Q6. _____

Lab 15 - Q7. _____

Lab 15 - Q8. _____

Lab 15 - Q9. _____

Lab 15 - Q10. _____

Lab 16: Pattern Recognition

Lab 16 - Q1. _____

Lab 16 - Q2. _____

Lab 16 - Q3. _____

Lab 16 - Q4. _____

Lab 16 - Q5. _____

Lab 16 - Q6. _____