The Making of the Wireshark Certified Analyst (WCA) Exam

Chris Greer and Ross Bagurdes

#sf25us

Let me introduce myself

- Chris Greer
- First Sharkfest 2012
- Packet Analyst, Trainer, and Content Creator
- And these are my socials:
  - YouTube, LinkedIn

Let me introduce myself

- Ross Bagurdes
- First SharkFest 2013
- More about me

- And these are my socials:
  - YouTube, LinkedIn

Goals of Certification

- Wireshark Foundation wanted a way for users to validate and demonstrate their skills
- Provide a skills pathway for network engineers
- Encourage training and development of protocol analysis skills

Yay!!

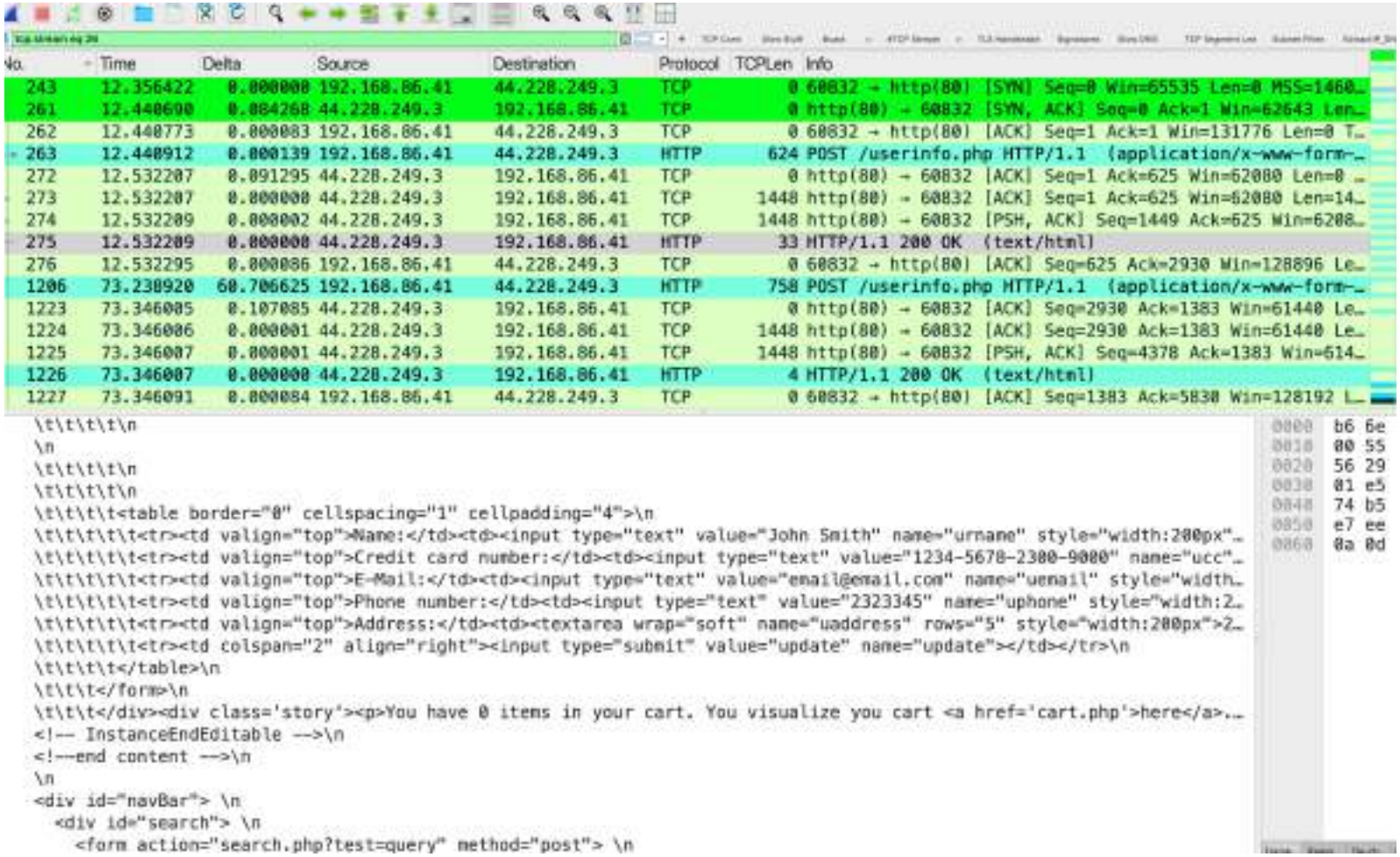
Goals for WCA

- Didn't want a cert that:
  - Boot-camp memorization
  - Wireshark Analyzer trivia
  - All little-used menu options
  - Sucked

- DID want a cert that:
  - Truly tested knowledge, not memorization
  - Accessible to entry-level
  - Represented protocol analysis skills AND analyzer knowledge
  - Belonged to the Wireshark Foundation and directly benefits them

It wasn't always easy….

We would have loved a real environment… but…



No.	Time	Delta	Source	Destination	Protocol	TCPLen	Info
243	12.356422	0.000000	192.168.86.41	44.228.249.3	TCP	0	60832 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460…
261	12.440690	0.084268	44.228.249.3	192.168.86.41	TCP	0	http(80) → 60832 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len…
262	12.440773	0.000083	192.168.86.41	44.228.249.3	TCP	0	60832 → http(80) [ACK] Seq=1 Ack=1 Win=131776 Len=0 T…
263	12.440912	0.000139	192.168.86.41	44.228.249.3	HTTP	624	POST /userinfo.php HTTP/1.1 (application/x-www-form-…
272	12.532207	0.091295	44.228.249.3	192.168.86.41	TCP	0	http(80) → 60832 [ACK] Seq=1 Ack=625 Win=62080 Len=0 …
273	12.532207	0.000000	44.228.249.3	192.168.86.41	TCP	1448	http(80) → 60832 [ACK] Seq=1 Ack=625 Win=62080 Len=14…
274	12.532289	0.000082	44.228.249.3	192.168.86.41	TCP	1448	http(80) → 60832 [PSH, ACK] Seq=1449 Ack=625 Win=6208…
275	12.532289	0.000000	44.228.249.3	192.168.86.41	HTTP	33	HTTP/1.1 200 OK (text/html)
276	12.532295	0.000006	192.168.86.41	44.228.249.3	TCP	0	60832 → http(80) [ACK] Seq=625 Ack=2930 Win=128896 Le…
1206	73.230920	60.706625	192.168.86.41	44.228.249.3	HTTP	758	POST /userinfo.php HTTP/1.1 (application/x-www-form-…
1223	73.346005	0.107085	44.228.249.3	192.168.86.41	TCP	0	http(80) → 60832 [ACK] Seq=2930 Ack=1383 Win=61440 Le…
1224	73.346006	0.000001	44.228.249.3	192.168.86.41	TCP	1448	http(80) → 60832 [ACK] Seq=2930 Ack=1383 Win=61440 Le…
1225	73.346007	0.000001	44.228.249.3	192.168.86.41	TCP	1448	http(80) → 60832 [PSH, ACK] Seq=4378 Ack=1383 Win=614…
1226	73.346007	0.000000	44.228.249.3	192.168.86.41	HTTP	4	HTTP/1.1 200 OK (text/html)
1227	73.346091	0.000084	192.168.86.41	44.228.249.3	TCP	0	60832 → http(80) [ACK] Seq=1383 Ack=5830 Win=128192 L…

```
\t\t\t\t\n
\n
\t\t\t\t\n
\t\t\t\t\n
\t\t\t\t<table border="0" cellspacing="1" cellpadding="4">\n
\t\t\t\t\t<tr><td valign="top">Name:</td><td><input type="text" value="John Smith" name="urname" style="width:200px"…
\t\t\t\t\t<tr><td valign="top">Credit card number:</td><td><input type="text" value="1234-5678-2300-9000" name="ucc"…
\t\t\t\t\t<tr><td valign="top">E-Mail:</td><td><input type="text" value="email@email.com" name="uemail" style="width…
\t\t\t\t\t<tr><td valign="top">Phone number:</td><td><input type="text" value="2323345" name="uphone" style="width:2…
\t\t\t\t\t<tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" style="width:200px">2…
\t\t\t\t\t<tr><td colspan="2" align="right"><input type="submit" value="update" name="update"></td></tr>\n
\t\t\t\t</table>\n
\t\t\t</form>\n
\t\t\t</div><div class='story'><p>You have 0 items in your cart. You visualize you cart <a href='cart.php'>here</a>…
<!-- InstanceEndEditable -->\n
<!--end content -->\n
\n
<div id="navBar"> \n
  <div id="search"> \n
    <form action="search.php?test=query" method="post"> \n
```

```
0000  b6 6e
0010  80 55
0020  56 29
0030  01 e5
0040  74 b5
0050  e7 ee
0060  0a 0d
```

Focused on Objectives

- Let's check out the objectives

How to take the exam

- certifications.wireshark.org
- Hosted on Kryterion learning platform
  - On-site at Kryterion Testing Center
  - Remotely proctored
  - 50-60 questions
    - Multiple choice
    - Multiple selection
    - Weighted by question

Watch for Promos!

- Regular price is $349
- SharkFest promo - $249

How to prep

- certifications.wireshark.org
- Trusted Instructors – links to training
  - Ross, Chris, Sake, SCOS, others
  - Video course, labs
  - Book is in the works
  - Practice tests are in the works

How do I know its any good?

Feedback

Q+A

#sf25us