Grading Struggle

• Way too many write ups are shallow, incomplete, superficial.

• Explain. Discuss. Describe. Analyze.
  – “Do a detailed analysis…”
  – “Explain the start up process, accounting for all the traffic to and from the phone.”

• What do these call for?
Can’t Be Simple Packet Listing

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>11389</td>
<td>201.013992</td>
<td>132.235.67.134</td>
<td>132.235.67.156</td>
<td>SIP Request: REGISTER sip:132.235.67.156</td>
</tr>
</tbody>
</table>

Frame 11389 (552 bytes on wire, 552 bytes captured)

Arrival Time: Oct 18, 2008 15:46:04.831859000
[Time delta from previous captured frame: 0.827048000 seconds]
[Time delta from previous displayed frame: 201.013992000 seconds]
[Time since reference or first frame: 201.013992000 seconds]
Frame Number: 11389
Frame Length: 552 bytes
Capture Length: 552 bytes
[Frame is marked: False]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]


Destination: Supermic_53:3b:33 (00:30:48:53:3b:33)
Address: Supermic_53:3b:33 (00:30:48:53:3b:33)
.... ..0. .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Source: Polycom_01:43:9b (00:04:f2:01:43:9b)
Address: Polycom_01:43:9b (00:04:f2:01:43:9b)
.... ..0. .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Type: IP (0x0800)

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0xb0 (DSCP 0x2c: Unknown DSCP; ECN: 0x00)
1011 00... = Differentiated Services Codepoint: Unknown (0x2c)
.... .0 = ECN-Capable Transport (ECT): 0
Even With “Comments”

Frame 11389 (552 bytes on wire, 552 bytes captured)
Arrival Time: Oct 18, 2008 15:46:04.831859000
[Time delta from previous captured frame: 0.827048000 seconds]
[Time delta from previous displayed frame: 201.013992000 seconds]
[Time since reference or first frame: 201.013992000 seconds]
Frame Number: 11389
Frame Length: 552 bytes  // Frame is 552 bytes long.
Capture Length: 552 bytes
Summaries Can Be Too Shallow

Q: Explain the start up process, accounting for all the traffic to and from the phone.

A: “The phone downloads a bunch of stuff from a couple of different servers.”
Q: Explain the start up process, accounting for all the traffic to and from the phone.

A: “The Ethernet checksum on this frame is e320. Appendix A shows calculation of the checksums on all of the 11797 frames in the capture.”
Seek: Balance, Context, Demonstrated Understanding

• This is a senior-level class in your major.

• Lab, in general, is designed to:
  – Complement lectures.
  – Give you insight into how things work.
  – Allow you to find exceptions and details by working to understand what you see.
Some Rules of Thumb

• Demonstrate your understanding.
  – *This frame is a REGISTER message.* Note that the From: and To: fields both say 67.156, even though the phone is 67.134. 67.134 is the Via: address, though.

• Put in terms of the lecture:
  – *This frame is an acknowledgment of the REGISTER message in the prior frame.* Neither has any authorization information, so authorization must be accomplished somewhere else or not at all. In lecture this was called a ‘simple’ registration.
More Rules of Thumb

• You can look things up elsewhere, e.g. the RFC or your 230/330 text.
  — The expire: field is 3600. According to RFC 3261, this is seconds, so it expires in an hour.
  • Take care, though. Wikipedia, although useful, is NOT authoritative. Seek confirmation elsewhere.
  — These four frames are a more-or-less standard DHCP transaction, as described in Comer. There is an extra option, though, the 66 option, “TFPT server name”.

Sunday, September 20, 2009
More Rules of Thumb

• Try to understand the big picture.
  – In packet captures of SIP calls, are all the SIP messages accounted for? How do they relate?
  – The SDP in this INVITE message from the proxy has 0.0.0.0 as the connection field. This must be an indication to stop sending audio.
Still More

• You can speculate.
  – You almost have to.
    • The contents of some packets is binary, or encrypted.
    • RFC 3261 is 269 pages long.
  – Can give supporting information.
  – This INVITE occurs in the middle of an existing call.
    Since the Call-ID: field isn’t changed, it must be some kind of change in the status of an existing call.
Still More

• You can admit ignorance.
  – You almost have to.
    • You don't get to see the internals of the telephone program code.
  – Can give supporting information.
  – I don’t know why the phone is doing DHCP again. This transaction is just like the previous one, except for the transaction id and order of the options.
Suggestion

• Who’s the audience?
  – The instructor? Yes.
  – You might be better off writing for prospective future employer.
    • What do you want them to see?
  – Or for a future you.
    • Preserve insights for future use. If you have to have debug a SIP system sometime, what do you think you’ll find useful? Suppose your lab writeup were something you could bring to the final exam…
Ultimately…

- Try to approach the captures with a sense of curiosity and desire to understand what’s going on.
- There’s no substitute for a genuine desire to learn and explore.