

Guidelines for ITL Lab Reports

Why Guidelines?

In short, ease of grading. This reduces errors on the part of the graders, and reduces turn-around time for the assignments. Most of all, it reduces irritation on the part of the graders. This is good for your grade! This is good for your grade! An improperly formatted lab report will have points deducted!

Mantra for Lab Reports – The easier you make it to grade the higher your grade is likely to be. Corollary - Presentation (how it looks on paper) counts!

How do I Write Pretty Reports?

There are plenty of labs open on campus that may be used to write a lab report. Microsoft Word or LATEX are perfectly capable of producing a document that follows these specifications.

Explain, Discuss, Compare – Questions that ask for this type of information want you to write an answer in **YOUR own words**. It is not sufficient to look it up on the internet and paste (and site) your answer.

Sniffer output – It's your responsibility to learn out to get the correct output from the packet sniffer program. In Wireshark printing to a file is a great option as you can then cut and paste into your report. Reformatting of the data by shrinking the font of packet data will help it to fit better into your report.

No Cover Sheets – The reports will be large enough as it is and therefore require no coversheet. However, each page should have the page number out of the total (i.e. 3 of 12), your name (Bill Smith) and the date (1/2/2007). This way if a page is found the grader will know what to do with it. Do not add extra pages or attach the lab report print out.

Example page footer:

Bob Jones 1/3/2004 pg. 2 of 15

Brevity - When writing lab reports, the more concise your answer is the more likely you are to get full credit. Do not make your answer so short that it does not answer the question, but a brief paragraph answering each question is all that is necessary (or a table, if that is appropriate). Partial answers will gain partial credit.

Organization - Each question should be answered, in-order, in your lab report; the question's number should be clearly listed in a heading of some sort for each answer. A numbered list is wonderful. Keep all relevant data with the answer. Making the grader work to figure out your answer or try to find all of your relevant data will lower your grade. Most reports should not require an appendix of additional data. If you put data in your report it should be part of an answer to a question (otherwise its just extra paper).

Font Styles - For each answer, your synthesized work should be in a separate font from packet dump data (packet dump data will be in a fixed-width, typewriter-style font as in this guide). Numerical answers to questions (for questions which have an obvious numerical answer) should be in a bold font. Make your answers **stand out**. Otherwise the grader may assume that you simply did not understand what the answer was.

Supporting Data - In many questions, it may be in your best interest to provide supporting data to your answer. This may follow your first paragraph in your answer, if little supporting data is needed. Packet dumps must be filtered before being attached to lab handouts. Do not hand in a packet dump with 2,000 packets if only 10 are required to support your argument. Filtering can either be done by hand during the lab write-up, or during the collection of data. Data that actually answers the question should be **bolded** in your packet dumps. This will make your answers stand out. Otherwise the grader may assume that you simply did not understand what the answer was.

Staples - Staples must be used in all lab reports. As a general rule, if your lab report is too thick to be stapled it should be thinned down! The sheer number of lab handouts prevents paperclips from being a reasonable tool.

Hints for Data Collection

Data collection and organization is crucial to these labs; there will be a lot of data available, and knowing how to extract the useful data is part of what we're trying to teach. The first problem many students have is getting their raw data out of the lab. The two easiest ways to get data out of the lab are to use scp/sftp to copy the data to another machine or to use a USB jump drive. Email clients will also be available, if you would like to email a copy of the lab data to yourself and your partner, but the previous two methods are faster and easier to verify quickly (as Oak can take quite some time to deliver emails during the day).

Remember, your data will be **erased** after the lab section is over. The lab machines are reset for the next lab, thus erasing any data you would have saved. Make sure that you have all of your raw data collected before you leave!

How much Packet data?

What kind of output should you put in your report depends on what the question is asking for. The best rule to follow is the smallest amount of data that answers the question. Using the packet collection tools several levels of output are possible. In some cases the only data needed will be summary data (shown below).

This is the summary data for one packet.

No.	Time	Source	Destination	Protocol	Info
153	2.631836	00:07:e9:5e:8a:a6	ff:ff:ff:ff:ff:ff	ARP	Who has 132.235.58.46? Tell 132.235.58.79

At other times you may need to show more information about a packet(s). There are many sections to a packet. Do not assume that all need to be shown as this will take up many pages in your report to show only a small amount of data. Below is an example of more information that can be shown.

No.	Time	Source	Destination	Protocol	Info
153	2.631836	00:07:e9:5e:8a:a6	ff:ff:ff:ff:ff:ff	ARP	Who has 132.235.58.46? Tell 132.235.58.79

```
Frame 153 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:07:e9:5e:8a:a6 (00:07:e9:5e:8a:a6), Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: 00:07:e9:5e:8a:a6 (00:07:e9:5e:8a:a6)
  Sender IP address: 132.235.58.79 (132.235.58.79)
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 132.235.58.46 (132.235.58.46)
```

In this example the packet has three sections (Frame, Ethernet II and Address Resolution Protocol) but only one section has been expanded. Not all sections need be expanded to answer the question and therefore were not expanded.

How do I look at my raw data later?

The other common problem in labs with data collection is what to do with packet dump files. If both you and your lab partner have access to WireShark (aka Ethereal) or tcpdump outside of the lab, saving all of your packet dumps as binary data and then processing them while writing the lab is your best choice. This allows you to filter packets during the write-up, which reduces the amount of cut-and-paste work you will have to do with text output. If you cannot use binary dump files, try to filter the text output from Wire Shark and tcpdump before leaving the lab.

To generate a binary file with `tcpdump`, use `tcpdump -w FILENAME` to write to the file `FILENAME`, and `tcpdump -r FILENAME` will re-read file `FILENAME` and process it like incoming data.

To generate text output from Wire Shark, use File|Export, and select File.

At any time, filter strings can be used in both Wire Shark and `tcpdump` to limit the amount of data collected (be careful when filtering while collecting data. Filtering after collection is far safer, as you do not lose data; it is merely suppressed for viewing).

If you have any questions about data collection or filtering, ask your lab attendant for more information.