Ethereal Strengths (30 Respondees)	Percentage of Responses
Full view of all packet parameters	27%
Capture and display filters	27%
Dissect and analyze protocols	27%
Ability to sort list elements	7%
Summary by packet type/packet headers	7%
Network stream reconstruction	7%
Ability to use coloring rules to highlight packets	7%
Ability to view packets in hexadecimal	3%
Detail oriented search for something specific	3%
Various modes of capture (live and to disk)	3%
Interface	3%
Statistical analysis of data (RTT times)	3%
Ability to filter network streams	3%
Ability to alert on known signatures	3%
Great for beginners	3%
Great deep packet analysis down to the bit	3%
Human readable packet contents / ASCII view	3%
Great for performing spot analysis	3%
Troubleshooting misconfigured networks	3%
Open source	3%
Filtering	3%
Flexibility	3%
Ethereal Weaknesses (27 Respondees)	Percentage of Responses
Overwhelming detail / too much for human to process	22%
Impossible to properly visualize a large dataset without getting lost and confused	11%
GUI too cumbersome	11%
Complex filter syntax	7%
Interface does not scale well	7%
Loss of context / big picture is hard to see	7%
Time consuming	7%
Small/limited data views	7%
Difficult to find patterns and trends	7%
Too much information for a list representation	7%
Not good for constant analysis over a long period of time	4%
SSL makes much of the payload uninformative	4%
Not good at network flow analysis	4%
Inability to disregard non-relevant packets	4%
Lack of time based histograms of number of hosts	4%
S/N ratio is low in a busy network	4%
Snort Strengths (18 Respondees)	Percentage of Responses
Robust and configurable filtering	39%
High quality signature database	28%
Helps to focus human resources	11%
Flexibility	11%
Ability to access details of packets/alerts	11%
Open source	11%
Useful as a packet capture program with signature matching capability	6%
Quick and dirty intrusion detection	6%
Trend analysis	6%
De-facto standard	6%
Automated analysis of data over a long period of time	6%
Flow based approach	6%
Cost	6%
Snort Weaknesses (17 Respondees)	Percentage of Responses
Too many false positives	41%
Reliance on known signatures	41%
Time and difficulty in selecting right set of signatures for a given network.	18%
Front end GUIs are poor	12%
Tedious analysis	6%
Dependency on well written rules	6%
Steep learning curve	6%
Snort management	6%
Tuning rules too tightly will cause false negatives	6%
Lack of good intrusion detection rules	6%
Backend database slows down with several million entries (MySQL)	6%
Lack of visual (e.g. non-text) output	6%

Table 2: Summary of Ethereal and Snort Strengths and Weaknesses