Q1: How many emails are there?
Answer: 1784

Q2: How many unique senders are there?
Answer: 1529

Q3: How many unique receivers are there?
Answer: 664

Q4: What is the earliest email Date (in full ISO 8601 format, translated to time zone UTC+0)?
Answer: 2002-01-01T09:35:24+00:00

Q5: What is the latest email Date (in full ISO 8601 format, translated to time zone UTC+0)?
Answer: 2025-03-10T10:03:00+00:00

Q6: What is the most popular word in plain text email bodies (content-type: text/plain)?
Answer: Your

Q7: What is the second most popular word in plain text email bodies (content-type:text/plain)?
Answer: you

Q8: How many attachments are there?
Answer: 26

Q9: How many PDF attachments are there? (based on the content-type header)
Answer: 16

Q10: How many image (JPEG or PNG) attachments are there? (based on the content type header)
Answer: 5

Q11: How many emails have been sent to CYFO INC?
Answer: 69

Q12: How many emails have been sent to each department?
Answer: rnd: 33, fin: 17, hr: 5, ops: 5, it: 4, law: 5

Q13: What servers sent the emails (i.e. the first in the received chain)?
Answer: qmail servers of unknown origin, possibly spoofed. ebox-prod-srv22.win.su.se (130.237.162.52) and IP: 130.237.200.210

Q14: What organizations own those IP-addresses? (use e.g., whois and look at DNSnames)
Answer: 130.237.200.210 = Stockholm University & 130.237.162.52 = Stockholm University

Q15: How many emails have been sent by each group?
rachel nguyen <rdelia@avaya.com>: 49 emails
bob bobness <bob.bobness@dsv.su.se>: 13 emails
sarah whitmore <sarah.whitmore.cyfoinc@gmail.com>: 7 emails

Q16: Two departments are being singled out, which ones?
Answer: R&D and Finance
Group 1 (Rachel Nguyen) - broad spam attack.
Group 2 (Bob Bobness) is only targeting R&D.
Group 3 (Sarah Whitmore) is only targeting Finance.

Q17: What country does the middle group (in terms of number of emails) most likely operate out of?
Answer: The middle group (Group 2) most likely operates out of: China (UTC+8)

Q18: What is likely the preferred username of the malware developer?
Answer: /home/kimyu

Q19: What is the IP address of the CC server?
Answer: 193.10.9.5