SMTP and ncat

https://github.com/heig-vd-dai-course

Web · PDF

L. Delafontaine and H. Louis, with the help of GitHub Copilot.

Based on the original course by O. Liechti and J. Ehrensberger.

Objectives

- Learn electronic messaging protocols:
    - SMTP
    - POP3
    - IMAP
- Focus on the SMTP protocol
- Learn how to use ncat and Java to send an email to an SMTP server

Electronic messaging protocols: SMTP, POP3 and IMAP

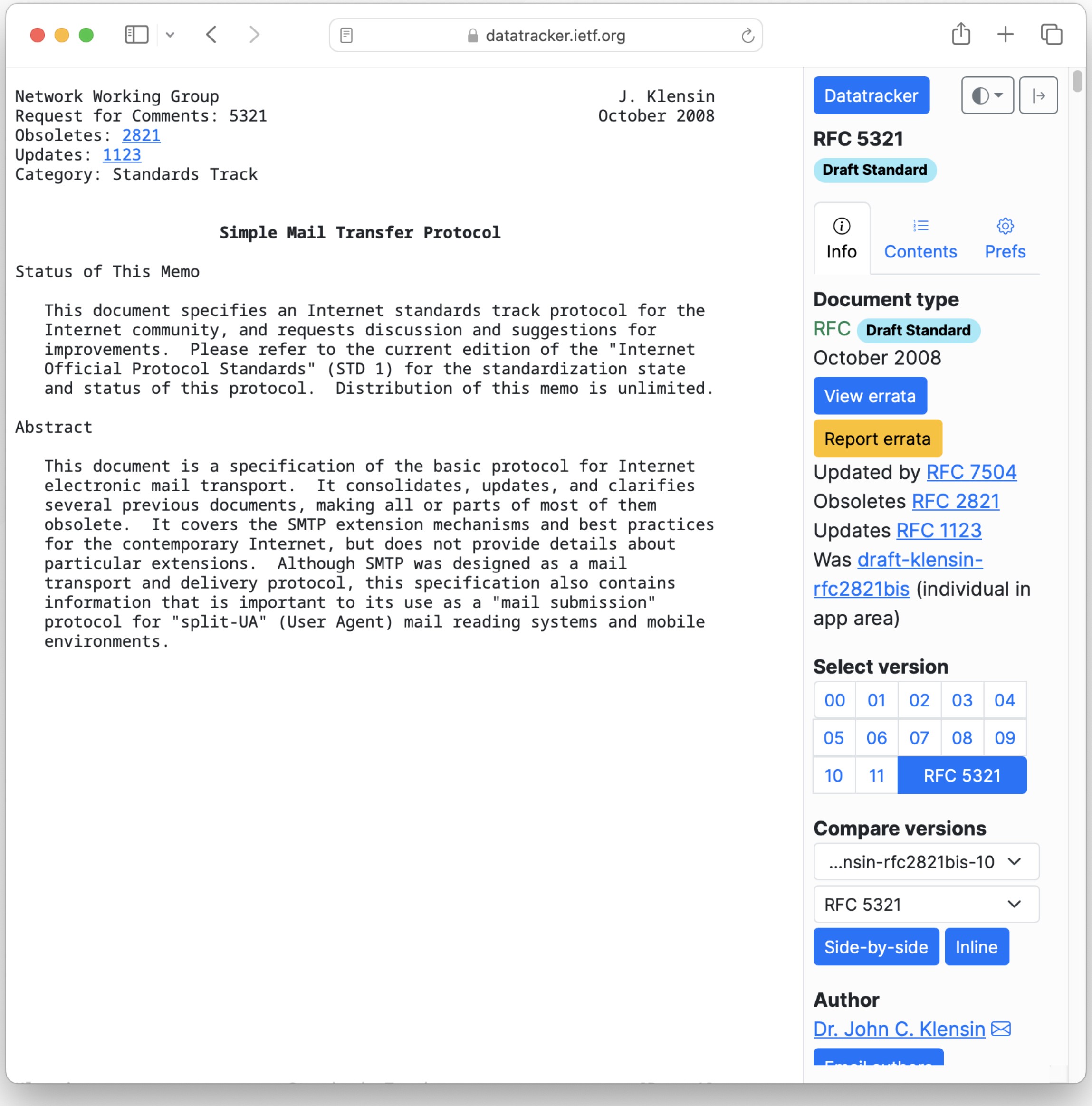
More details for this section in the course material. You can find other resources and alternatives as well.

Electronic messaging protocols: SMTP, POP3 and IMAP

- Email clients are called **Mail User Agents (MUA)**
- Email servers are called **Mail Transfer Agents (MTA)**
- They use different protocols to communicate

SMTP

- SMTP: Simple Mail Transfer Protocol
- Uses TCP port 25 (unencrypted) or 465 (encrypted)
- Used to send emails



```
Network Working Group                                         J. Klensin
Request for Comments: 5321                                  October 2008
Obsoletes: 2821
Updates: 1123
Category: Standards Track


                     Simple Mail Transfer Protocol

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.

Abstract

   This document is a specification of the basic protocol for Internet
   electronic mail transport.  It consolidates, updates, and clarifies
   several previous documents, making all or parts of most of them
   obsolete.  It covers the SMTP extension mechanisms and best practices
   for the contemporary Internet, but does not provide details about
   particular extensions.  Although SMTP was designed as a mail
   transport and delivery protocol, this specification also contains
   information that is important to its use as a "mail submission"
   protocol for "split-UA" (User Agent) mail reading systems and mobile
   environments.
```

RFC 5321

Draft Standard

Document type

RFC Draft Standard

October 2008

Updated by RFC 7504

Obsoletes RFC 2821

Updates RFC 1123

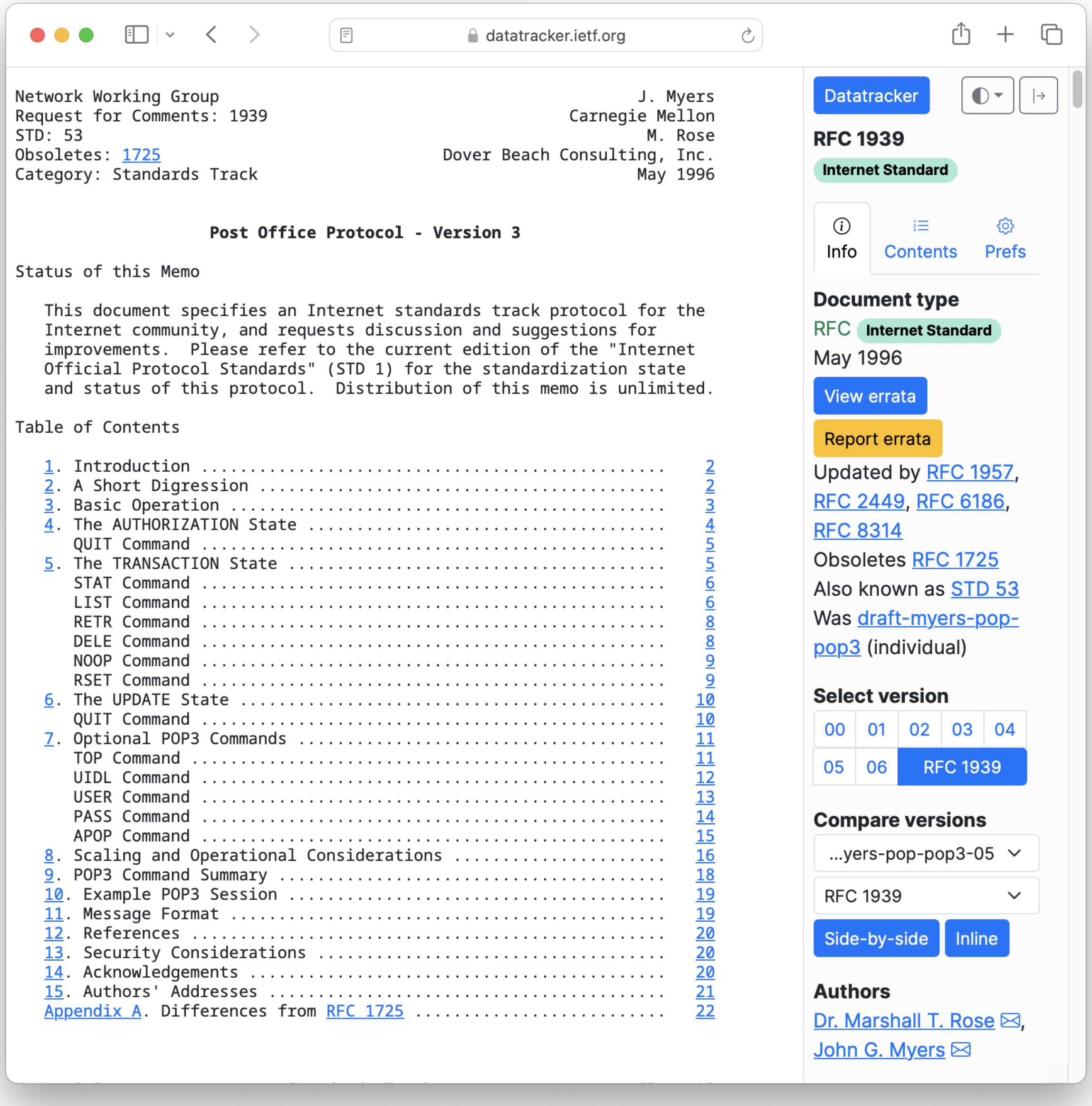
Was draft-klensin-rfc2821bis (individual in app area)

Author

Dr. John C. Klensin ✉

POP3

- POP3: Post Office Protocol
- Uses TCP port 110 (unencrypted) or 995 (encrypted)
- Used to retrieve emails from a server



```
Network Working Group                                           J. Myers
Request for Comments: 1939                               Carnegie Mellon
STD: 53                                                          M. Rose
Obsoletes: 1725                             Dover Beach Consulting, Inc.
Category: Standards Track                                       May 1996
```

Post Office Protocol - Version 3

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Table of Contents

1. Introduction 2
2. A Short Digression 2
3. Basic Operation 3
4. The AUTHORIZATION State 4
QUIT Command 5
5. The TRANSACTION State 5
STAT Command 6
LIST Command 6
RETR Command 8
DELE Command 8
NOOP Command 9
RSET Command 9
6. The UPDATE State 10
QUIT Command 10
7. Optional POP3 Commands 11
TOP Command 11
UIDL Command 12
USER Command 13
PASS Command 14
APOP Command 15
8. Scaling and Operational Considerations 16
9. POP3 Command Summary 18
10. Example POP3 Session 19
11. Message Format 19
12. References 20
13. Security Considerations 20
14. Acknowledgements 20
15. Authors' Addresses 21
Appendix A. Differences from RFC 1725 22

RFC 1939

Internet Standard

Document type

RFC Internet Standard

May 1996

Updated by RFC 1957, RFC 2449, RFC 6186, RFC 8314

Obsoletes RFC 1725

Also known as STD 53

Was draft-myers-pop-pop3 (individual)

Select version

00 01 02 03 04 05 06 RFC 1939

Compare versions

...yers-pop-pop3-05

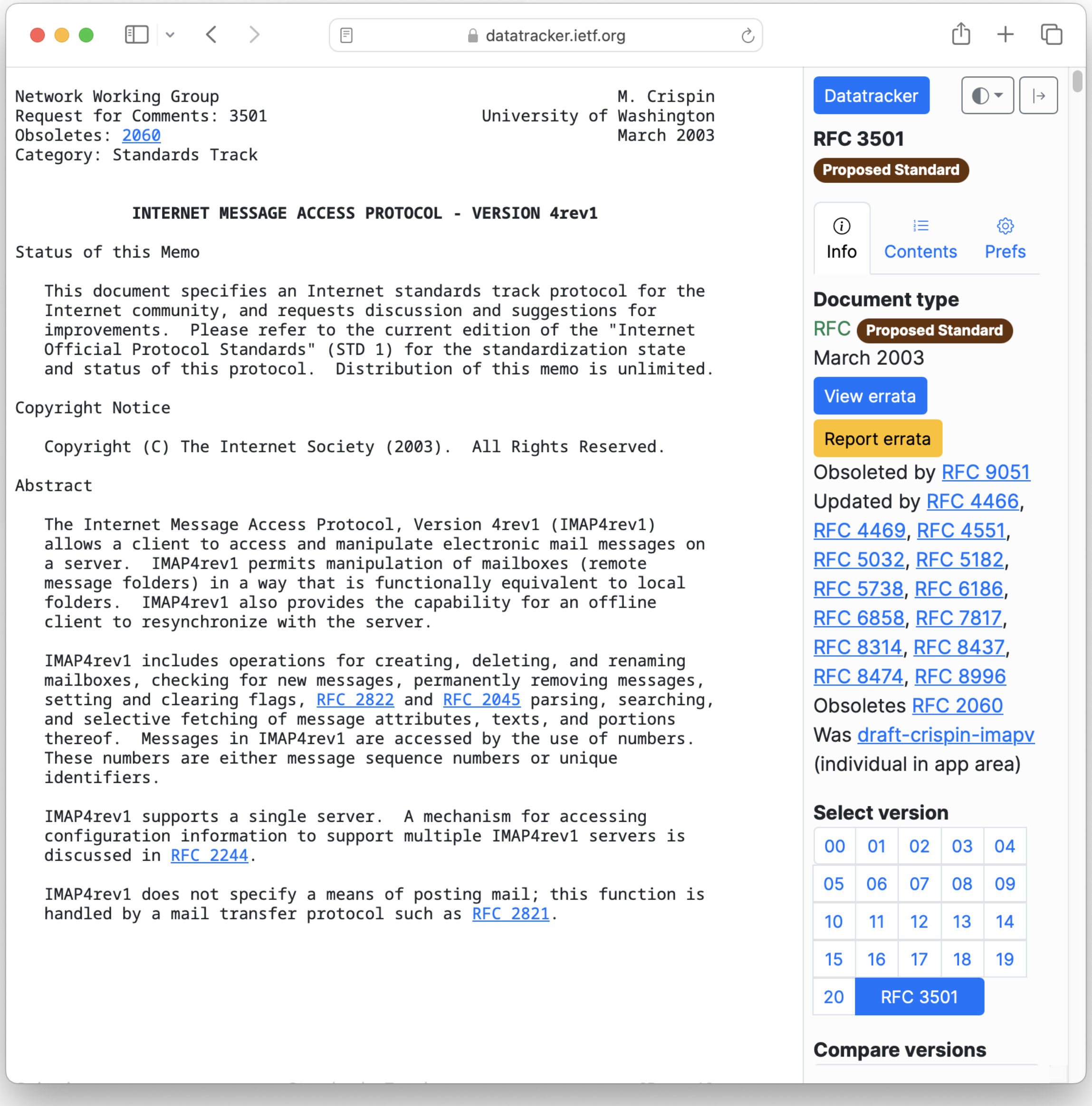
RFC 1939

Authors

Dr. Marshall T. Rose ✉, John G. Myers ✉

IMAP

- IMAP: Internet Message Access Protocol
- Uses TCP port 143 (unencrypted) or 993 (encrypted)
- Used to retrieve emails from a server
- Much more powerful than POP3 (synchronization, ...)



```
Network Working Group                                         M. Crispin
Request for Comments: 3501                      University of Washington
Obsoletes: 2060                                               March 2003
Category: Standards Track


           INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.

Copyright Notice

   Copyright (C) The Internet Society (2003).  All Rights Reserved.

Abstract

   The Internet Message Access Protocol, Version 4rev1 (IMAP4rev1)
   allows a client to access and manipulate electronic mail messages on
   a server.  IMAP4rev1 permits manipulation of mailboxes (remote
   message folders) in a way that is functionally equivalent to local
   folders.  IMAP4rev1 also provides the capability for an offline
   client to resynchronize with the server.

   IMAP4rev1 includes operations for creating, deleting, and renaming
   mailboxes, checking for new messages, permanently removing messages,
   setting and clearing flags, RFC 2822 and RFC 2045 parsing, searching,
   and selective fetching of message attributes, texts, and portions
   thereof.  Messages in IMAP4rev1 are accessed by the use of numbers.
   These numbers are either message sequence numbers or unique
   identifiers.

   IMAP4rev1 supports a single server.  A mechanism for accessing
   configuration information to support multiple IMAP4rev1 servers is
   discussed in RFC 2244.

   IMAP4rev1 does not specify a means of posting mail; this function is
   handled by a mail transfer protocol such as RFC 2821.
```

RFC 3501

Proposed Standard

Document type

RFC Proposed Standard

March 2003

Obsoleted by RFC 9051

Updated by RFC 4466, RFC 4469, RFC 4551, RFC 5032, RFC 5182, RFC 5738, RFC 6186, RFC 6858, RFC 7817, RFC 8314, RFC 8437, RFC 8474, RFC 8996

Obsoletes RFC 2060

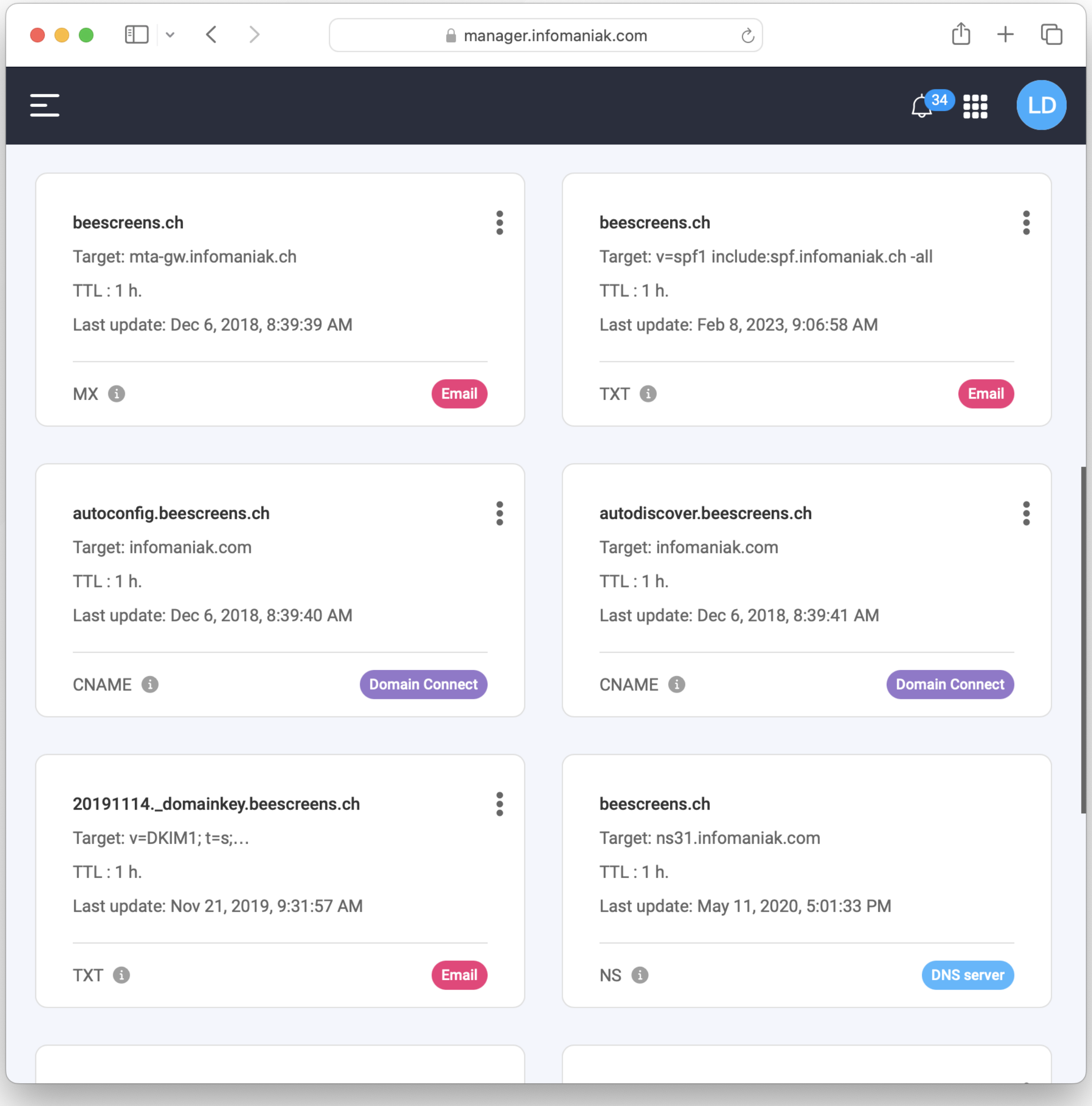
Was draft-crispin-imapv (individual in app area)

DNS records related to email

More details for this section in the course material. You can find other resources and alternatives as well.

DNS records related to email

- `MX` : Mail eXchange - Specifies the mail server responsible for a domain name
- `TXT` : Store any text-based information. Used for `SPF` records, for email authentication



beescreens.ch
Target: mta-gw.infomaniak.ch
TTL : 1 h.
Last update: Dec 6, 2018, 8:39:39 AM
MX
Email

beescreens.ch
Target: v=spf1 include:spf.infomaniak.ch -all
TTL : 1 h.
Last update: Feb 8, 2023, 9:06:58 AM
TXT
Email

autoconfig.beescreens.ch
Target: infomaniak.com
TTL : 1 h.
Last update: Dec 6, 2018, 8:39:40 AM
CNAME
Domain Connect

autodiscover.beescreens.ch
Target: infomaniak.com
TTL : 1 h.
Last update: Dec 6, 2018, 8:39:41 AM
CNAME
Domain Connect

20191114._domainkey.beescreens.ch
Target: v=DKIM1; t=s;...
TTL : 1 h.
Last update: Nov 21, 2019, 9:31:57 AM
TXT
Email

beescreens.ch
Target: ns31.infomaniak.com
TTL : 1 h.
Last update: May 11, 2020, 5:01:33 PM
NS
DNS server

Security concerns and spam

More details for this section in the course material. You can find other resources and alternatives as well.

Security concerns and spam

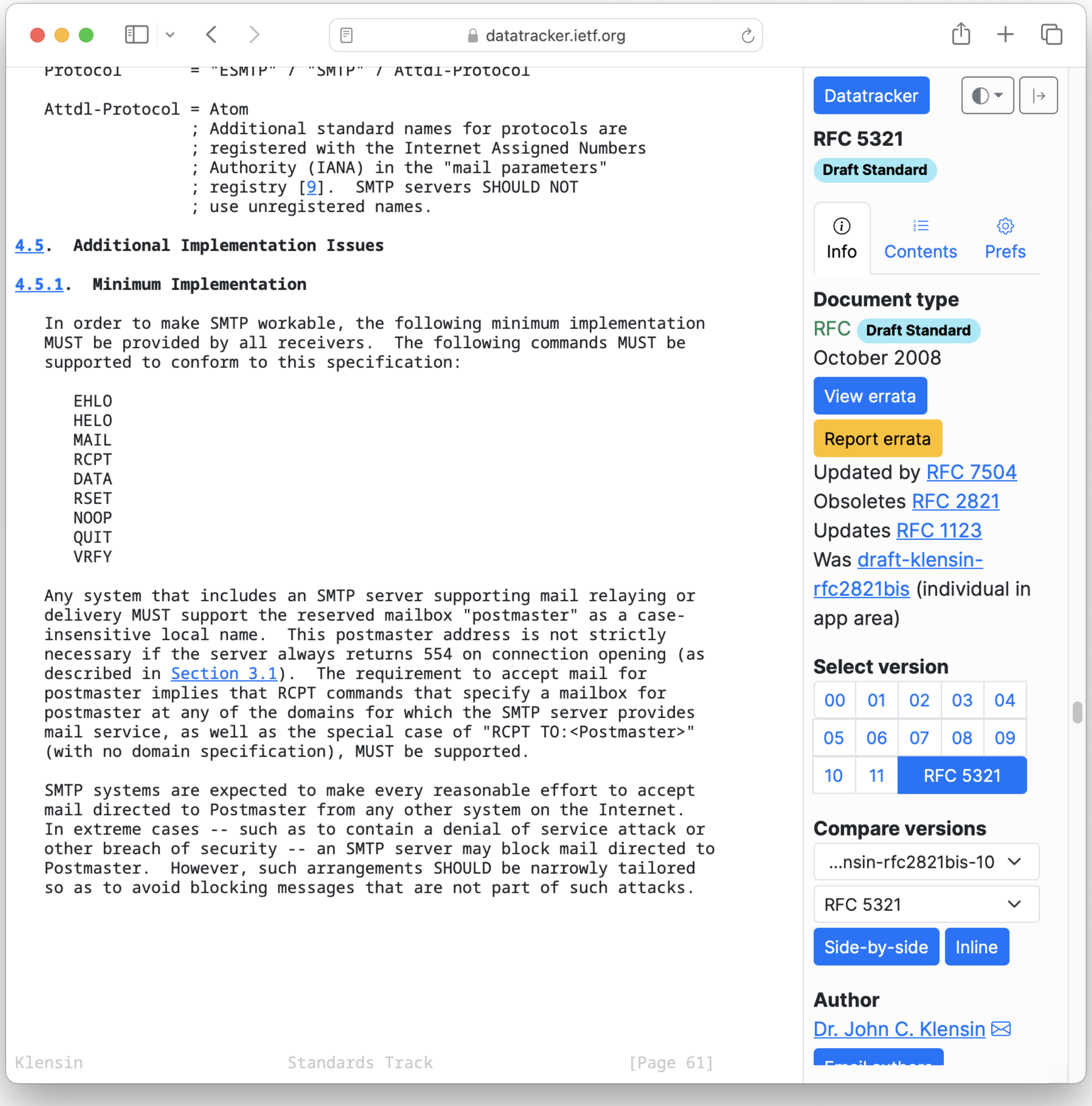
- SMTP is old and insecure
- Easy to spoof and forge emails
- Hard to maintain
- ➡️ Your email server can be used for spam and can be blocked
- ➡️ We will use a mock server to simulate an email server

A focus on the SMTP protocol

More details for this section in the course material. You can find other resources and alternatives as well.

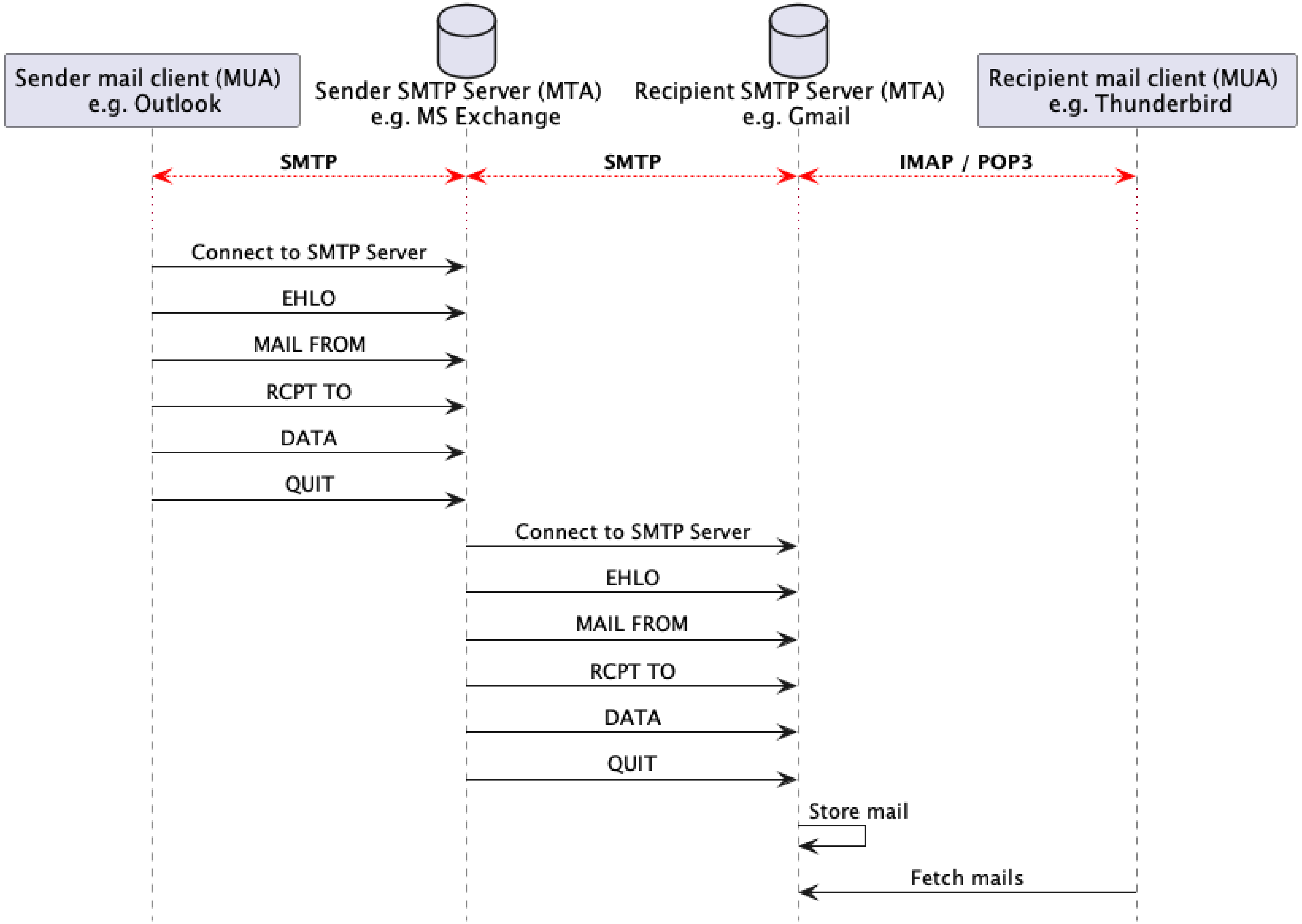
A focus on the SMTP protocol

- SMTP is a text-based protocol
- Commands are sent by the client to the server
- The server responds with a status code
- The client can send the next command



```
   Protocol        = "ESMTP" / "SMTP" / Attdl-Protocol

   Attdl-Protocol = Atom
                  ; Additional standard names for protocols are
                  ; registered with the Internet Assigned Numbers
                  ; Authority (IANA) in the "mail parameters"
                  ; registry [9].  SMTP servers SHOULD NOT
                  ; use unregistered names.

4.5.  Additional Implementation Issues

4.5.1.  Minimum Implementation

   In order to make SMTP workable, the following minimum implementation
   MUST be provided by all receivers.  The following commands MUST be
   supported to conform to this specification:

      EHLO
      HELO
      MAIL
      RCPT
      DATA
      RSET
      NOOP
      QUIT
      VRFY

   Any system that includes an SMTP server supporting mail relaying or
   delivery MUST support the reserved mailbox "postmaster" as a case-
   insensitive local name.  This postmaster address is not strictly
   necessary if the server always returns 554 on connection opening (as
   described in Section 3.1).  The requirement to accept mail for
   postmaster implies that RCPT commands that specify a mailbox for
   postmaster at any of the domains for which the SMTP server provides
   mail service, as well as the special case of "RCPT TO:<Postmaster>"
   (with no domain specification), MUST be supported.

   SMTP systems are expected to make every reasonable effort to accept
   mail directed to Postmaster from any other system on the Internet.
   In extreme cases -- such as to contain a denial of service attack or
   other breach of security -- an SMTP server may block mail directed to
   Postmaster.  However, such arrangements SHOULD be narrowly tailored
   so as to avoid blocking messages that are not part of such attacks.

Klensin                     Standards Track                   [Page 61]
```

- `HELO` / `EHLO`
- `MAIL FROM`
- `RCPT TO`
- `DATA`
  - `Subject:`
  - `From:`
  - `To:`
  - End by `.`
- `QUIT`

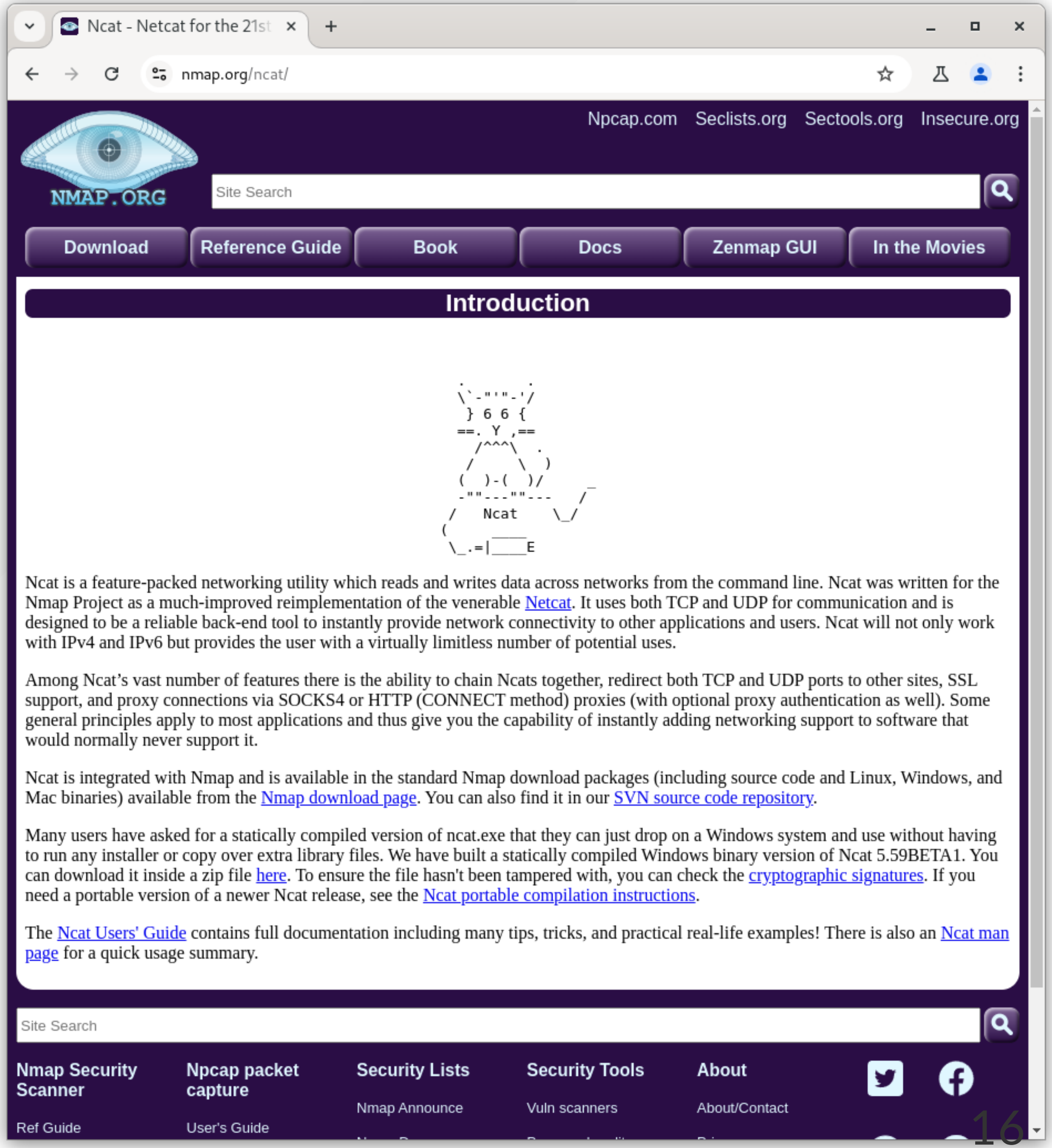


ncat

More details for this section in the course material. You can find other resources and alternatives as well.

ncat

- ncat is network utility for reading from and writing to network connections
- It is used to connect to a remote server (SMTP, HTTP, ...)
- We will use it to interact with a SMTP server



Introduction

```
 .                .
 \`-"'"-'/
  } 6 6 {
 ==. Y ,==
   /^^^\  .
  /     \  )
 (  )-(  )/     _
 -""---""---   /
/   Ncat    \_/
(     ____
 \_.=|____E
```

Ncat is a feature-packed networking utility which reads and writes data across networks from the command line. Ncat was written for the Nmap Project as a much-improved reimplementation of the venerable Netcat. It uses both TCP and UDP for communication and is designed to be a reliable back-end tool to instantly provide network connectivity to other applications and users. Ncat will not only work with IPv4 and IPv6 but provides the user with a virtually limitless number of potential uses.

Among Ncat's vast number of features there is the ability to chain Ncats together, redirect both TCP and UDP ports to other sites, SSL support, and proxy connections via SOCKS4 or HTTP (CONNECT method) proxies (with optional proxy authentication as well). Some general principles apply to most applications and thus give you the capability of instantly adding networking support to software that would normally never support it.

Ncat is integrated with Nmap and is available in the standard Nmap download packages (including source code and Linux, Windows, and Mac binaries) available from the Nmap download page. You can also find it in our SVN source code repository.

Many users have asked for a statically compiled version of ncat.exe that they can just drop on a Windows system and use without having to run any installer or copy over extra library files. We have built a statically compiled Windows binary version of Ncat 5.59BETA1. You can download it inside a zip file here. To ensure the file hasn't been tampered with, you can check the cryptographic signatures. If you need a portable version of a newer Ncat release, see the Ncat portable compilation instructions.

The Ncat Users' Guide contains full documentation including many tips, tricks, and practical real-life examples! There is also an Ncat man page for a quick usage summary.

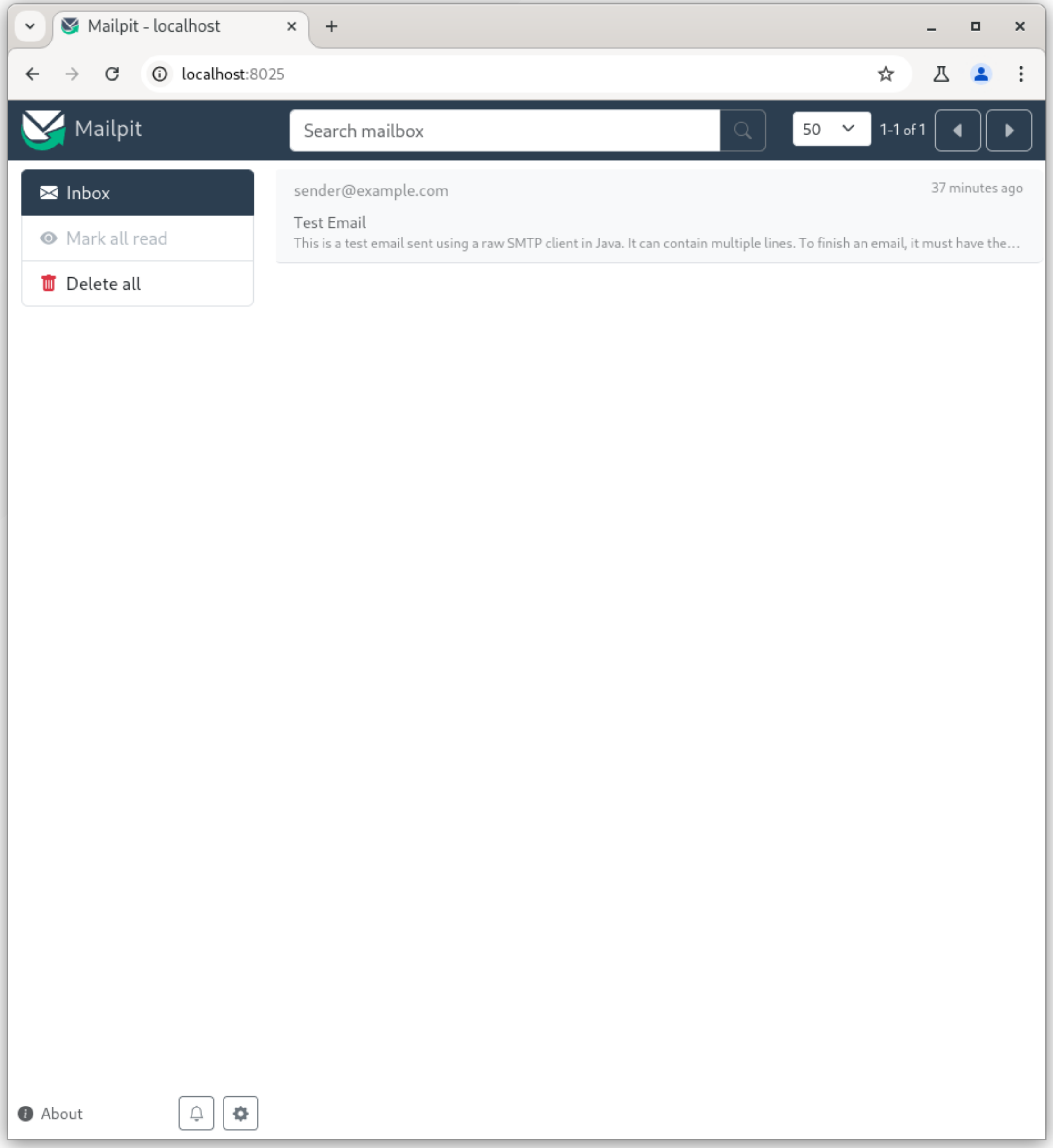
Questions

Do you have any questions?

Practical content

What will you do?

- Install and configure ncat
- Start a SMTP server with Docker Compose
- Send an email with ncat to the SMTP server
- Send an email with Java to the SMTP server



sender@example.com

37 minutes ago

Test Email

This is a test email sent using a raw SMTP client in Java. It can contain multiple lines. To finish an email, it must have the…

Find the practical content

You can find the practical content for this chapter on GitHub.

Finished? Was it easy? Was it hard?

Can you let us know what was easy and what was difficult for you during this chapter?

This will help us to improve the course and adapt the content to your needs. If we notice some difficulties, we will come back to you to help you.

➡️ GitHub Discussions

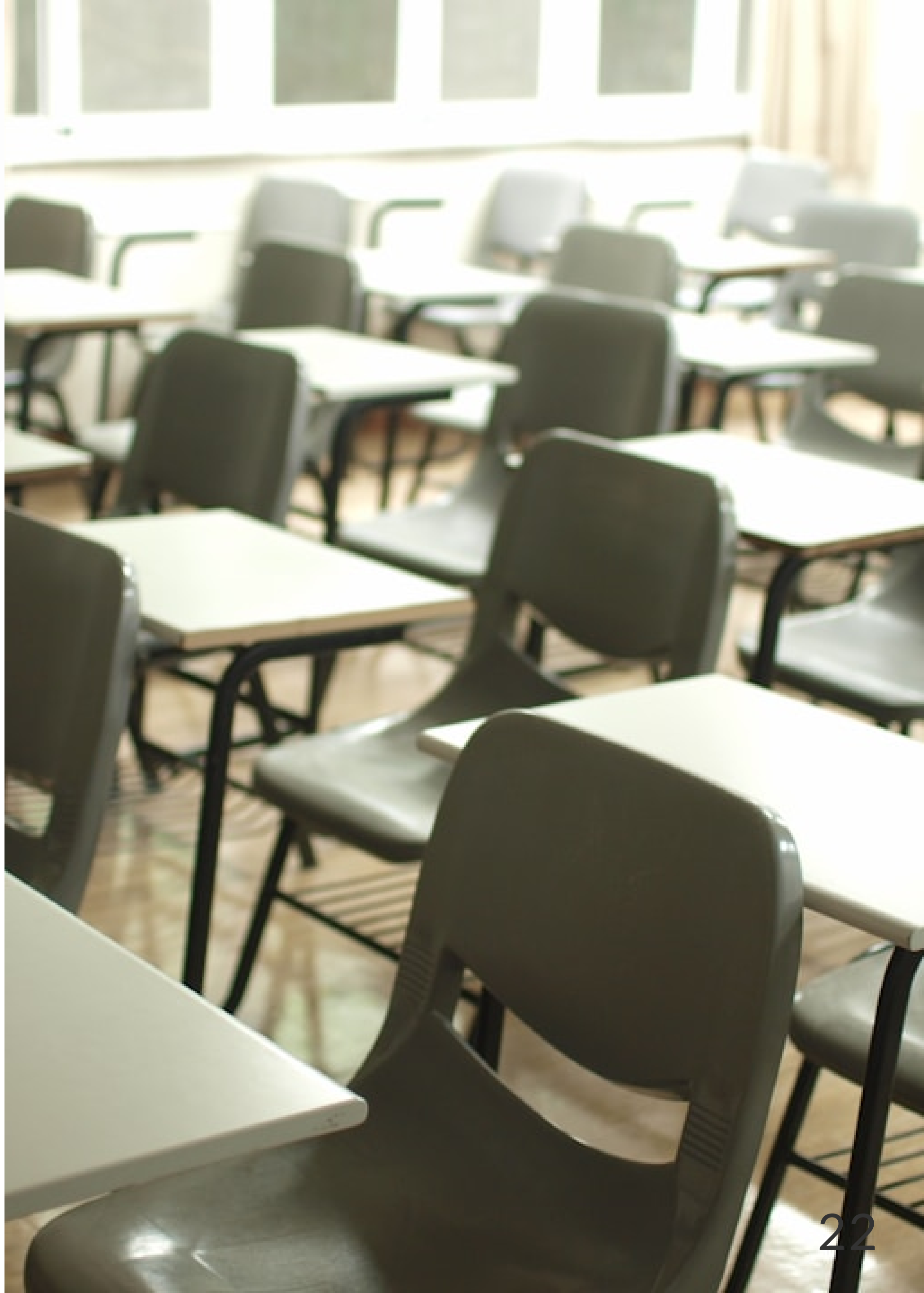
You can use reactions to express your opinion on a comment!

What will you do next?

We are arriving at the end of the second part of the course.

An evaluation will be done to check your understanding of all the content seen in this second part.

More details will be given in the next chapter.



Sources

- Main illustration by Joanna Kosinska on Unsplash
- Illustration by Aline de Nadai on Unsplash
- Illustration by Nik on Unsplash
- Illustration by MChe Lee on Unsplash