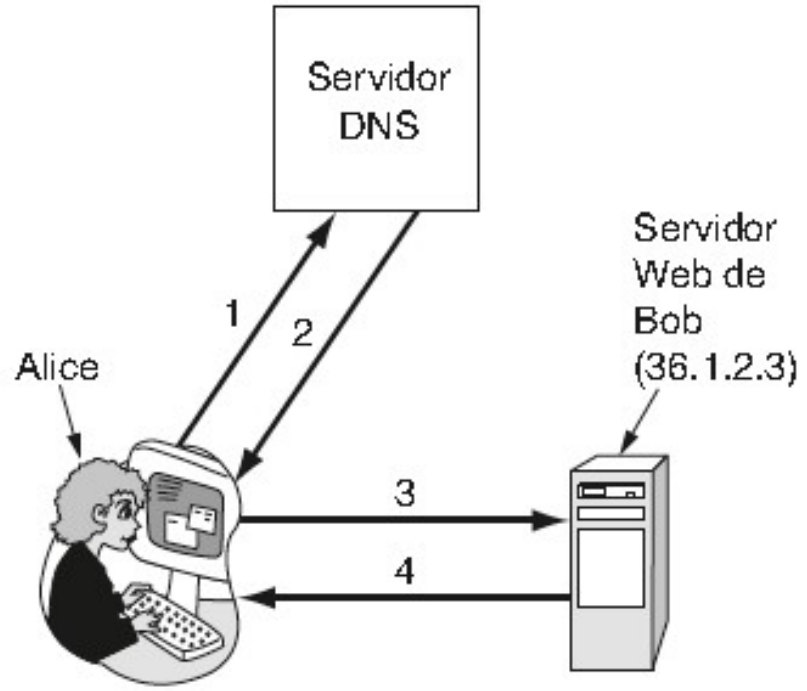
PUC Minas

Segurança na Web

- Ameaças
- Nomenclatura segura
- SSL – a camada de soquetes seguros
- Segurança em código móvel

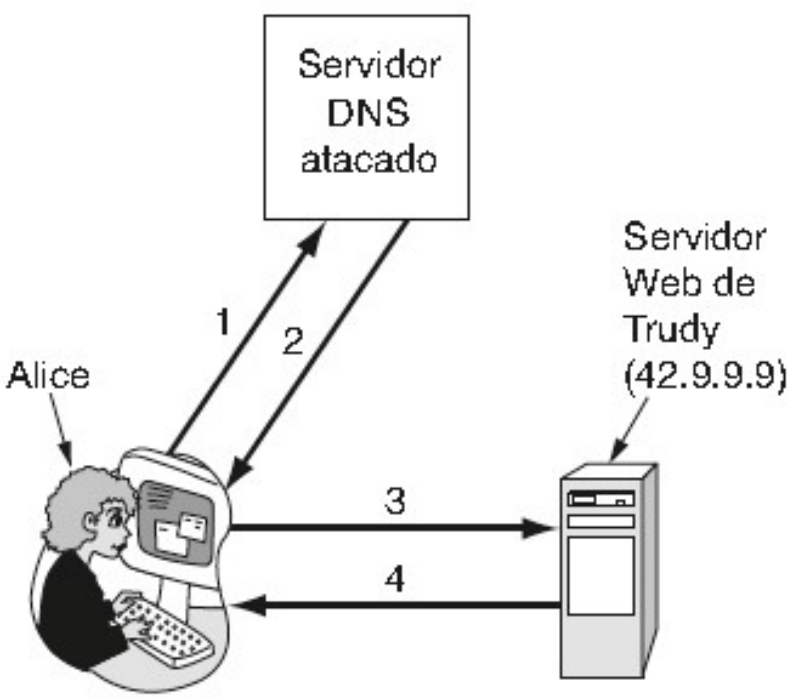
Nomenclatura segura (1)



Situação normal.

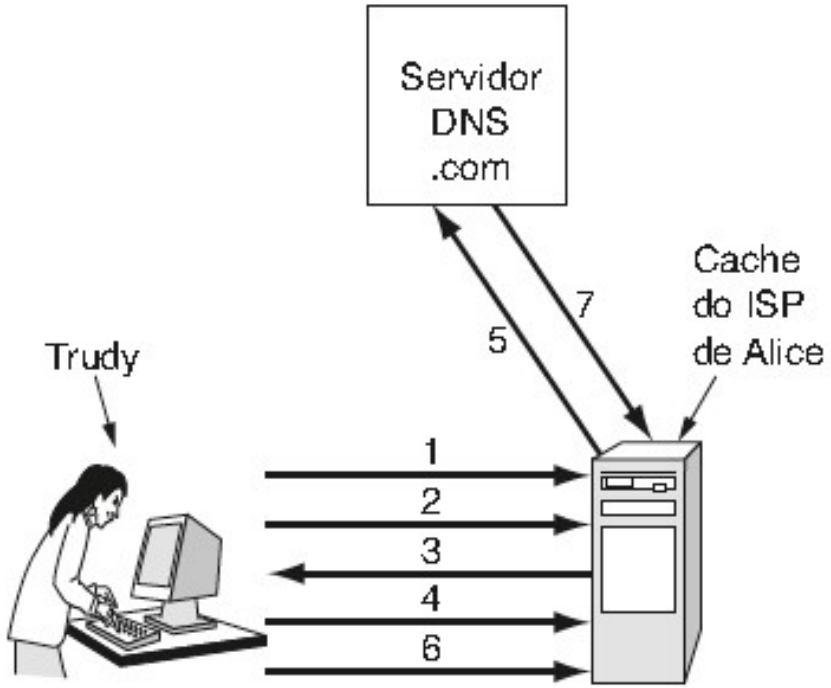
Nomenclatura segura (2)

PUC Minas



Ataque baseado na invasão do DNS e modificação do registro de Bob.

Nomenclatura segura (3)



1. Procura foobar.trudy-the-intruder.com
   (para forçá-lo para o cache do ISP)
2. Procura www.trudy-the-intruder.com
   (para obter o próximo número de sequência do ISP)
3. Pedido para www.trudy-the-intruder.com
   (para forçar o ISP a consultar o servidor .com na etapa 5)
4. Rapidamente, procura bob.com
   (para forçar o ISP a consultar o servidos no passo 5)
5. Consulta legítima para bob.com com seq = n+1
6. Resposta forjada de Trudy: Bob é 42.9.9.9, seq = n+1
7. Resposta real (rejeitada; tarde demais)

Como Trudy engana o ISP de Alice.

Nomenclatura segura (4)

PUC Minas

Serviços fundamentais do DNSsec:

- Prova de onde os dados são originados
- Distribuição de chave pública
- Autenticação de transação e solicitação

Nomenclatura segura (5)

PUC Minas

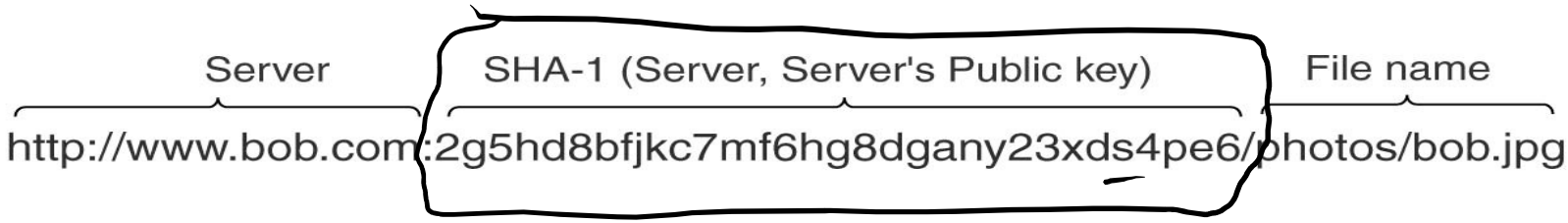
Responsável .com

Nome de domínio	Tempo de vida	Classe	Tipo	Valor
bob.com.	86400	IN	A	36.1.2.3
bob.com.	86400	IN	KEY	3682793A7B73F731029CE2737D...
bob.com.	86400	IN	SIG	86947503A8B848F5272E53930C...

Exemplo de RRSet para *bob.com*. O registro *KEY* é a chave pública de Bob. O registro *SIG* é o hash assinado do servidor .com de alto nível dos registros *A* e *KEY*, a fim de verificar a autenticidade.

Nomenclatura segura (6)

SHA-1 (DADOS DO SITE)
SM

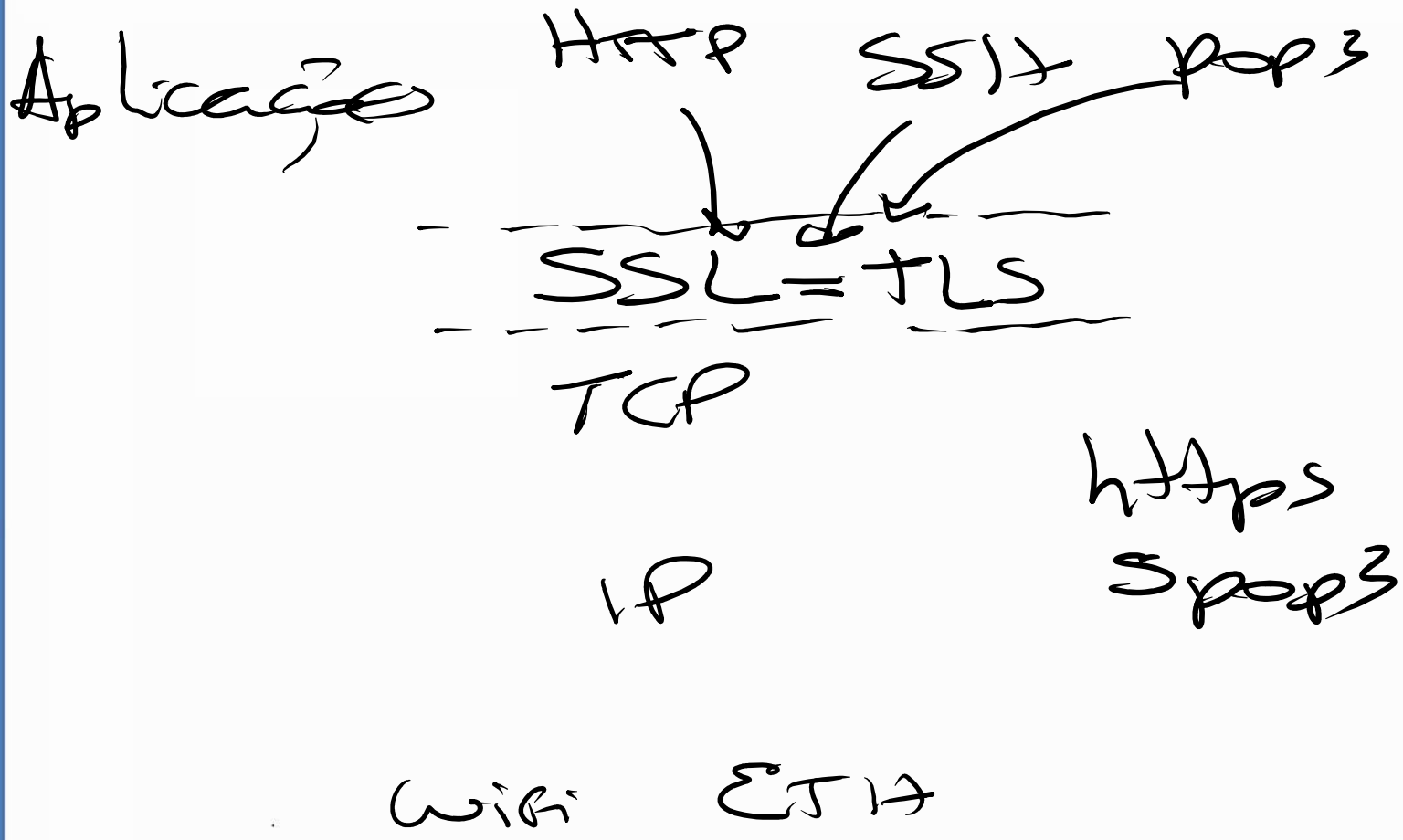


- Um URL autocertificado contendo um hash do nome e da chave pública do servidor

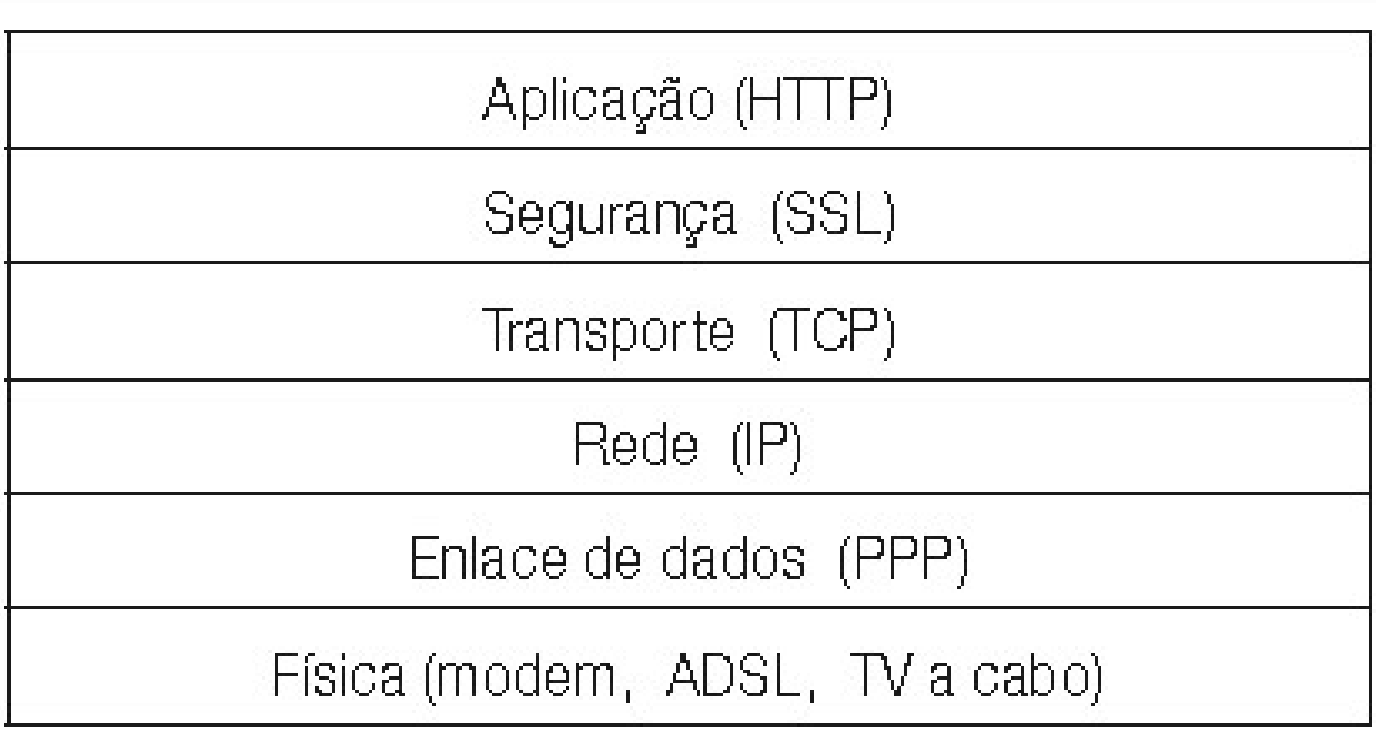
SSL – camada de soquetes seguros (1)

Conexão segura inclui:

- Negociação de parâmetro entre cliente e servidor
- Autenticação do servidor pelo cliente
- Comunicação secreta
- Proteção da integridade dos dados

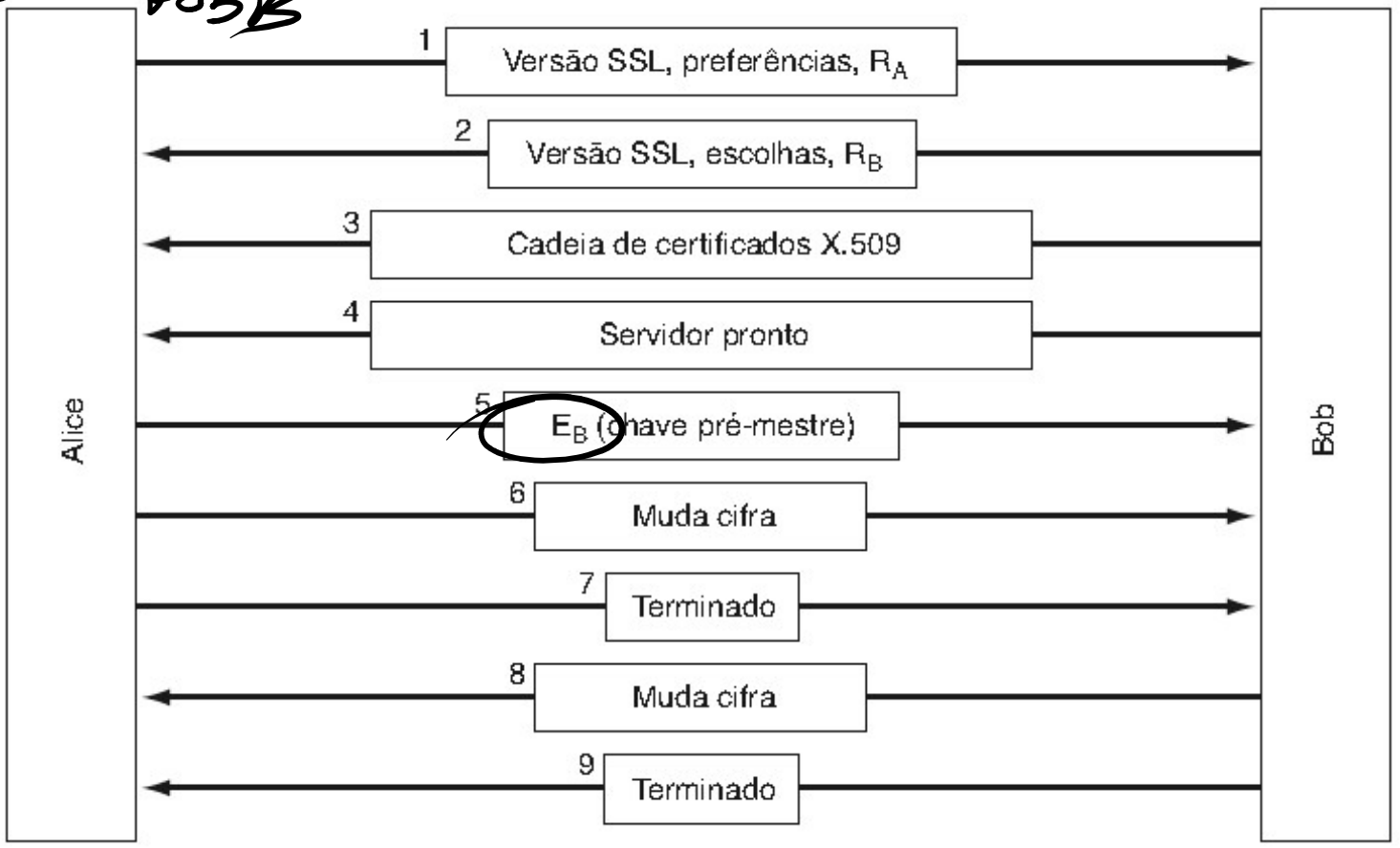


SSL – camada de soquetes seguros (2)



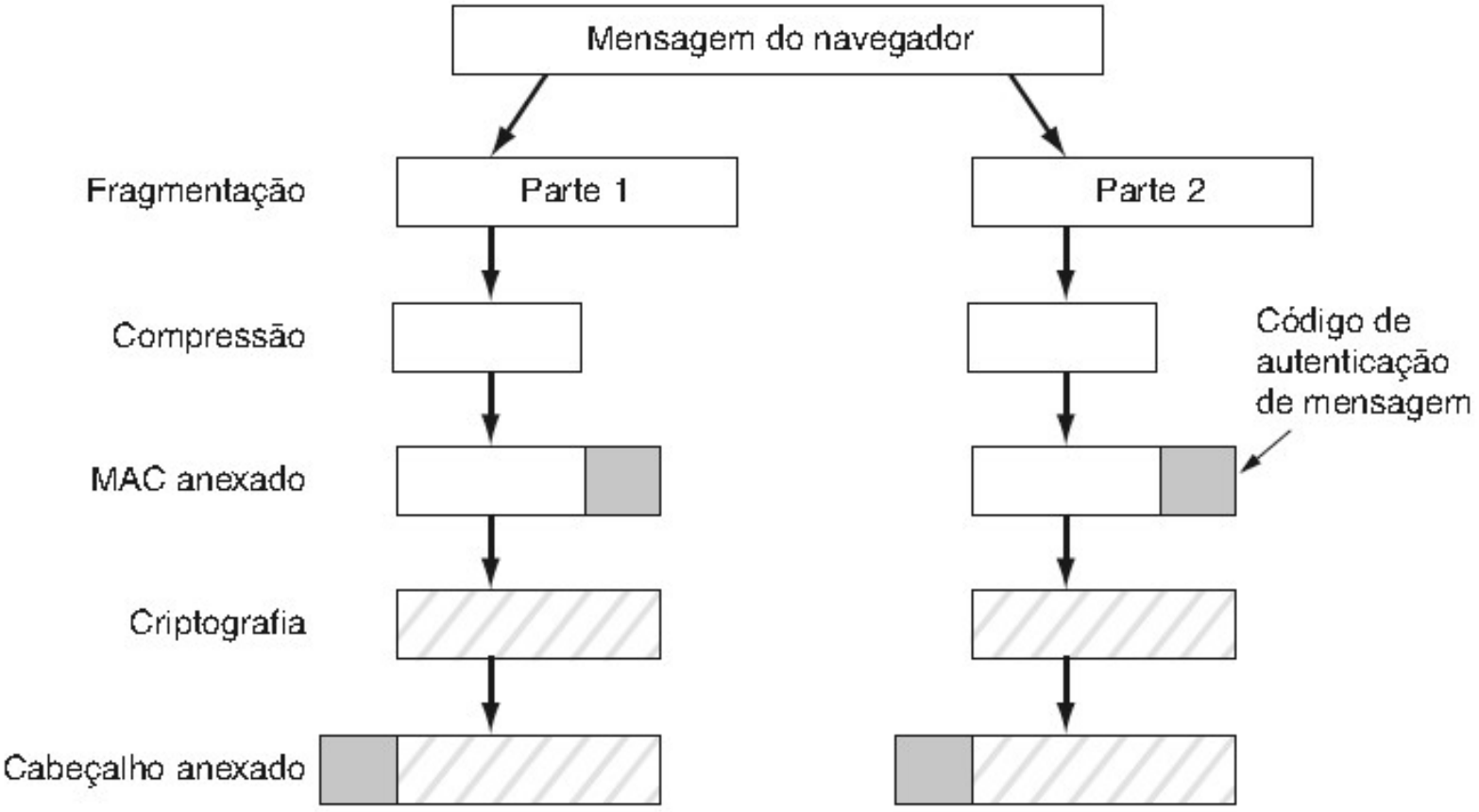
Camadas (e protocolos) para usuário doméstico navegando com SSL.

SSL – camada de soquetes seguros (3)



Versão simplificada do subprotocolo de estabelecimento de conexões SSL.

SSL – camada de soquetes seguros (4)



Transmissão de dados com SSL.

PUC Minas

Questões sociais

- Privacidade
- Liberdade de expressão
- Direitos autorais

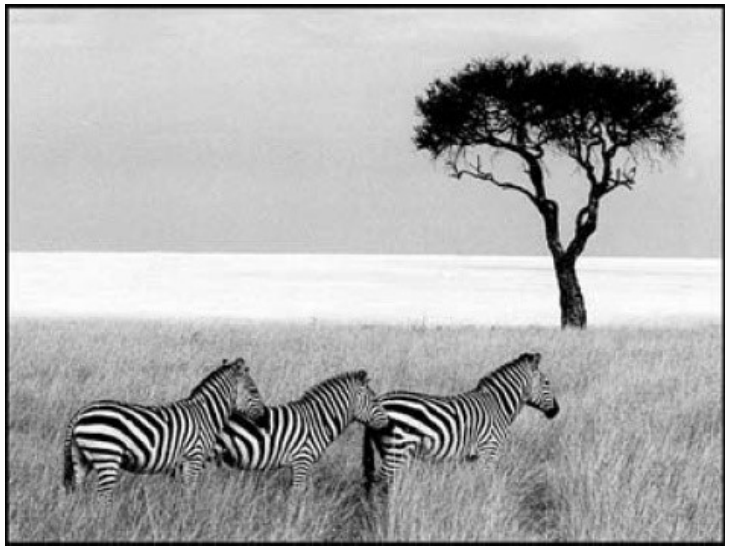
PUC Minas

Liberdade de expressão

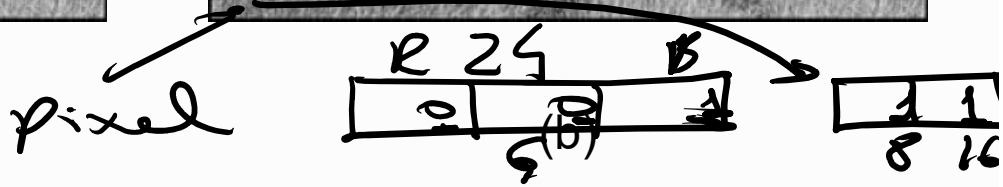
Possíveis materiais restritivos:

- Impróprio para crianças
- Ódio objetivando vários grupos
- Informações sobre democracia
- História que contradiz a versão do governo
- Manuais de atividades potencialmente ilegais

Liberdade de expressão (2)



(a)



(a) As três zebras e uma árvore.

(b) As três zebras, uma árvore, e o texto completo de cinco peças de William Shakespeare.