パケットキャプチャからのファイル抽出訓練

座学

訓練概要

- 目的
  - パケットキャプチャファイルから送受信ファイルを復元する技術を身に付けること
- 種別
  - ネットワーク
- 前提知識
  - HTTP、HTTPS、SMTP、FTP 等の各種プロトコル知識
- 習得技術
  - ネットワークツールの使い方（Wireshark）
- 対象
  - 防護隊員

目次

1. Export Objects機能を利用した抽出方法
2. 手動による抽出方法
3. HTTPSで暗号化された通信の復号方法

1. Export Objects機能を利用した抽出方法

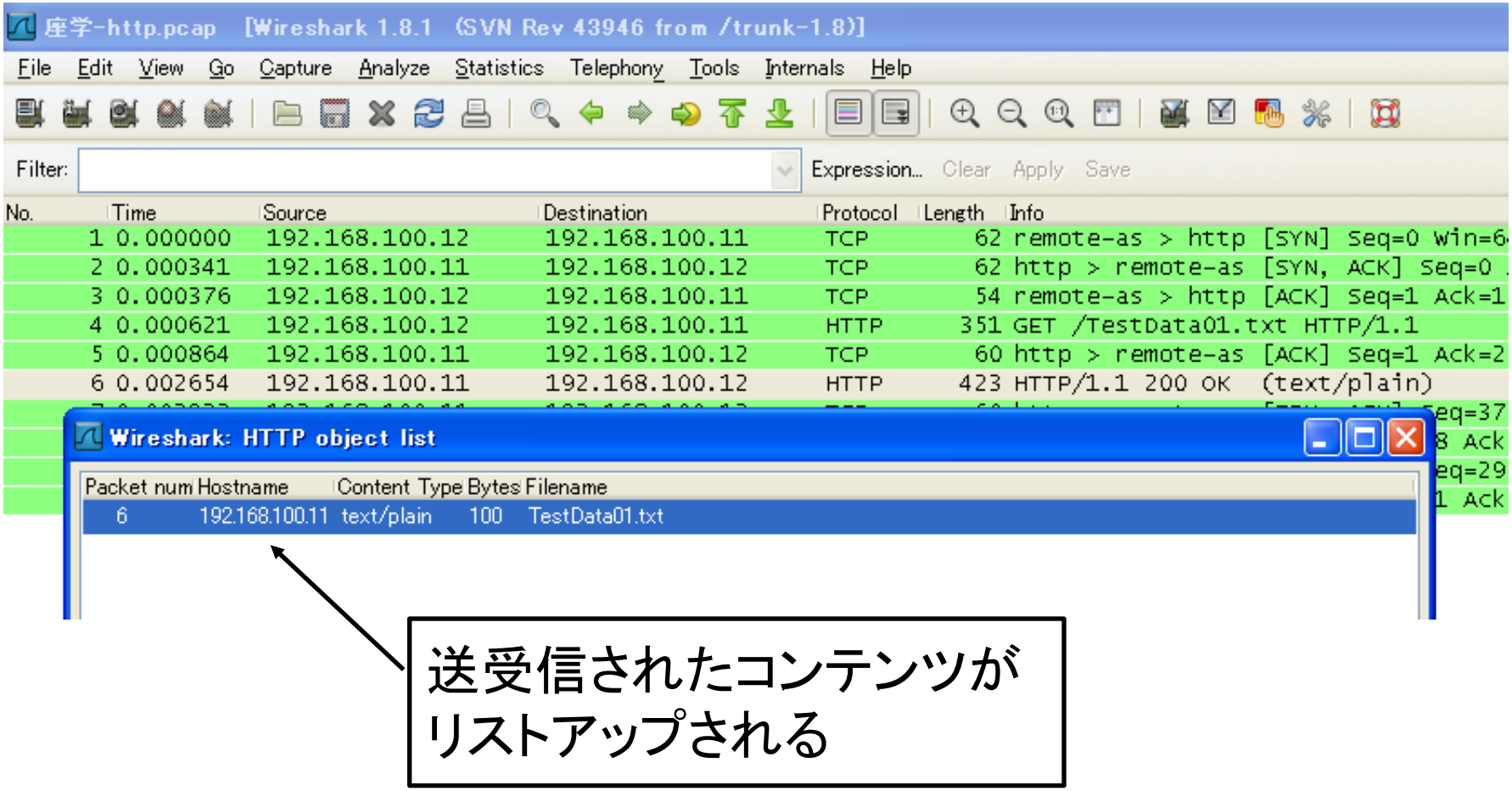
Export Objects機能

- Wireshark がもつ機能の一つ
- パケットキャプチャデータから、送受信したコンテンツを復元できる
- サポートしているプロトコルは下記の3つ
  - HTTP
  - DICOM
  - SMB

Export Objects機能を用いた抽出手順

1. キャプチャデータをWiresharkで開く
2. Export Objects機能を実行する
   - [File] -> [Export Objects] -> [HTTP]をクリック（HTTPの場合）
3. 該当のファイルを選択して [Save As] をクリック
4. ファイル名と保存場所を指定して [Save] をクリック

Export Objects機能を用いた抽出手順



2. 手動による抽出手順

Follow TCP Stream機能

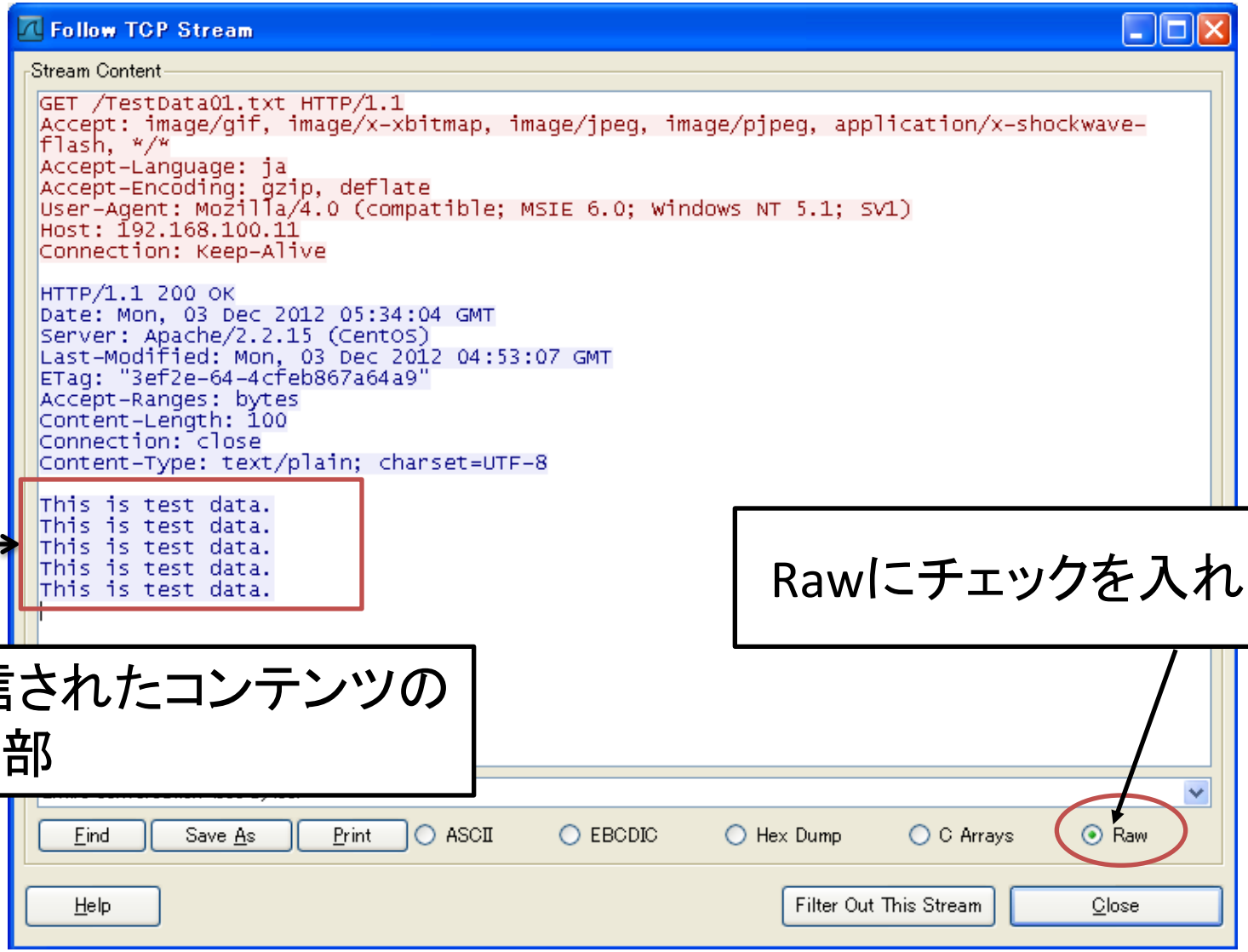
- Wiresharkがもつ機能の一つ
- 通信ストリームを再構築する機能
- [Save As] をクリックし、保存することで、通信ストリームをファイルに保存することが可能

- 使用方法
  - 該当パケットを右クリック -> Follow TCP Stream

2. 手動による抽出手順

1. キャプチャデータをWiresharkで開く
2. 目的のファイルを通信していたパケットを見つける
   - GET [ファイル名] などで検索する（HTTPの場合）
   - 検索機能 : [Edit] -> [Find Packet]
3. 上記2で見つけたパケットを右クリック -> [Follow TCP Stream]
4. 下部の [Raw] にチェックを入れる
5. データ部分をコピーし、エディタに貼り付けて保存する

2. 手動による抽出手順



送受信されたコンテンツのデータ部

Rawにチェックを入れる

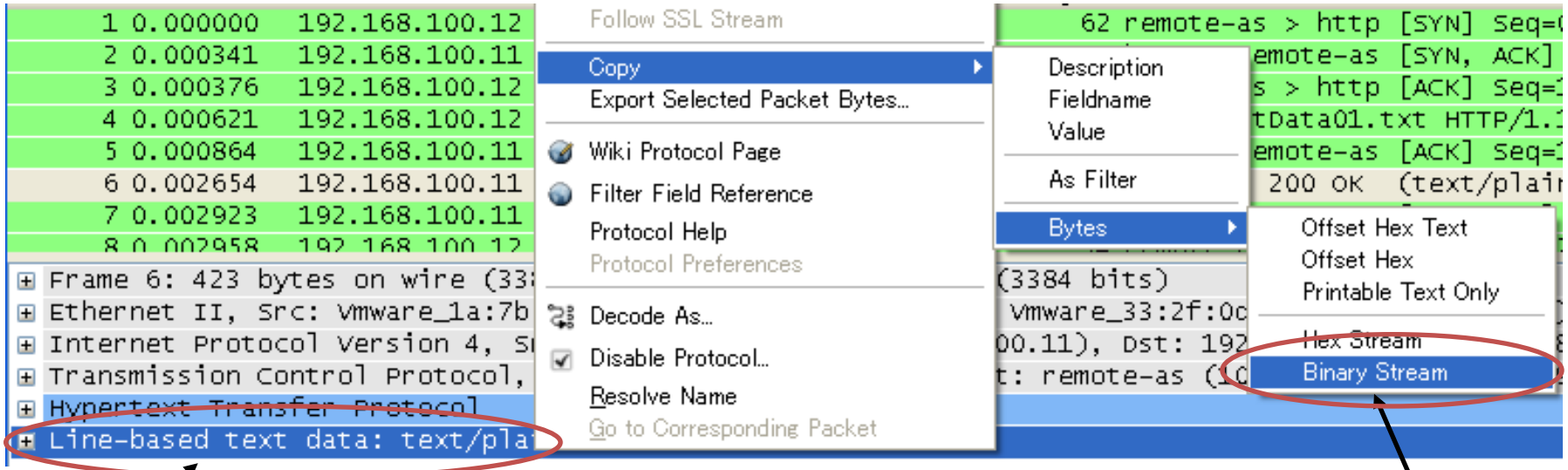
2. 手動による抽出手順

抽出するファイルがバイナリの場合

1. キャプチャデータをWiresharkで開く
2. 目的のファイルを通信していたパケットを見つける
   - HTTPであれば、「HTTP/1.0 200 OK」の後のサーバからのパケット
3. 「Packet Details」ウィンドウのデータ部を右クリック -> Copy -> Bytes -> Binary Stream をクリック
4. バイナリエディタ（BZなど）を起動し、貼り付けて保存

※サイズが大きいファイルの場合、
複数パケットに分割されている可能性がある

2. 手動による抽出手順



コピーする領域を
右クリック

バイナリとしてコピーする

3. HTTPSで暗号化された通信の復号方法

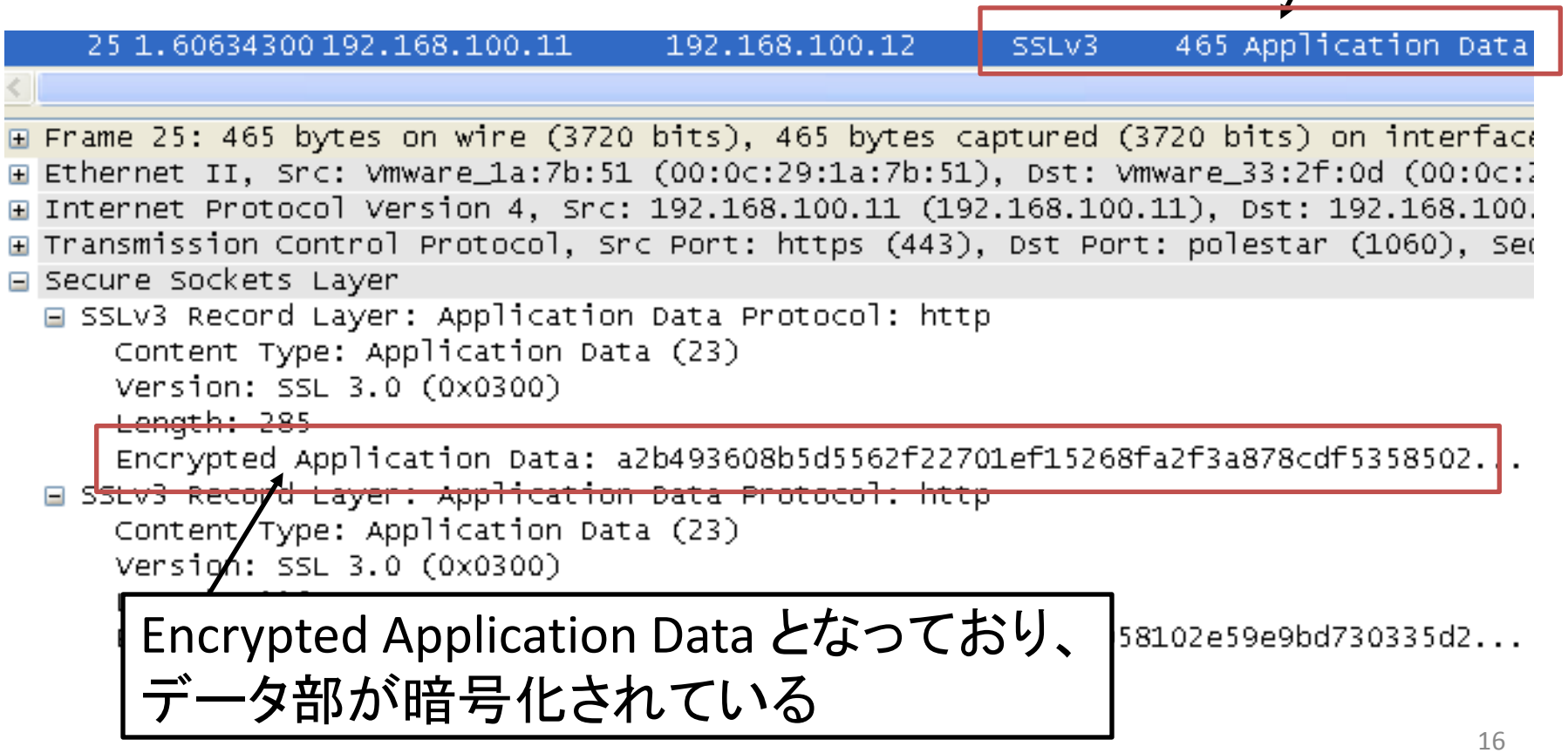
WiresharkのSSL復号機能

- Wiresharkには、SSLで暗号化された通信を復号する機能が実装されている
- 復号には通信先のSSLサーバ証明書の秘密鍵（PEM形式）が必要

  （本訓練では、事前に鍵を用意しています）
- マルウェアが行うHTTPS通信の調査に有用
  - 名前解決を細工して調査用HTTPSサーバに接続
  - 透過型プロキシ等を使って HTTPS通信を中継

復号前

SSLv3 Application Data となっており、
通信内容が分からない



Encrypted Application Data となっており、
データ部が暗号化されている

復号手順

1. キャプチャデータをWiresharkで開く
2. ツールバーの [Edit] -> [Preferences] -> [Protocols] -> [SSL]
3. [RSA keys list] の [Edit] をクリック
4. サーバの秘密鍵を登録する
   - 今回の訓練では、次ページの情報を入力する
5. [Apply] の後 [OK] をクリック
6. 下記を確認し、[Apply] の後 [OK] をクリック
   - [Reassemble SSL records …] => チェックあり
   - [Reassemble SSL Application …] => チェックなし
   - [Message Authentication Code …] => チェックなし
7. 一部のパケットが [SSLv3] から [HTTP] に復号されていることを確認する

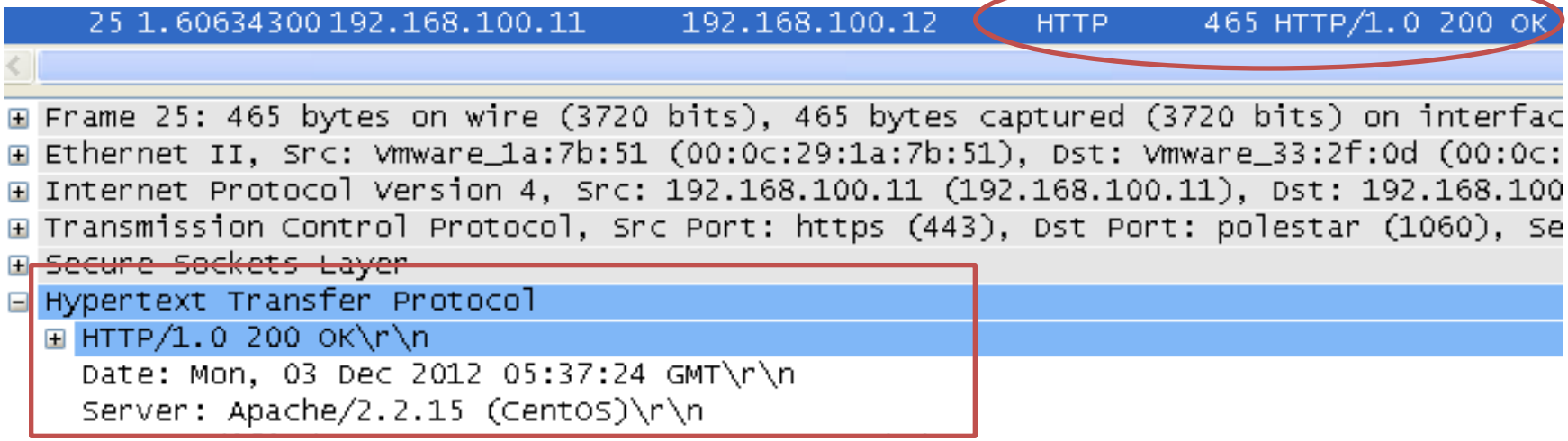
訓練用キャプチャデータの復号時に指定する情報

- 訓練用キャプチャデータのSSL復号時には、下記の内容を入力する

項目	入力値
IP address	192.168.100.11
Port	443
Protocol	http
Key File	C:¥server.key
Password	[なし]

復号後

SSLv3 から HTTP に変化している



SSLが復号され、通信内容が見えるようになった

Follow SSL Stream機能

- Wiresharkがもつ機能の一つ
- 復号した状態で通信ストリームを再構築する機能
- [Save As] をクリックし、保存することで、復号された通信ストリームをファイルに保存することが可能

- 使用方法
  - 該当パケットを右クリック -> Follow SSL Stream
  - SSL復号後に使用可能