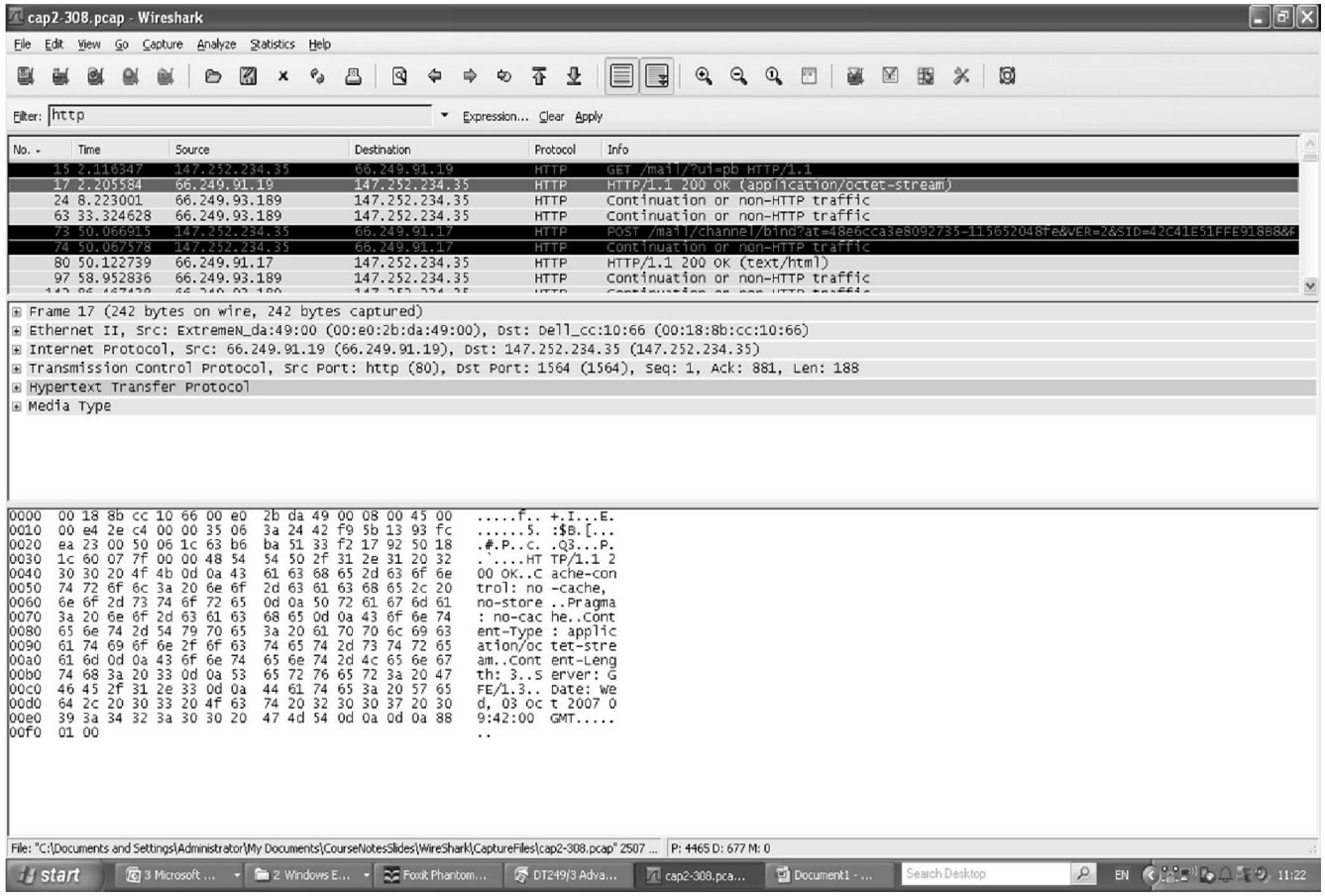
Wireshark的 - 在工作协议

- 该 *Wireshark的* 协议分析仪是用来捕获和分析 *帧* 从一个网络接口卡（NIC）d
- 下面滑动（截图1）示出了开口的屏幕，捕获的帧被突出显示：
  - 这里，过滤器已经被施加，从而只携带HTTP数据显示帧
- 屏幕包含三个子屏幕：
  - 顶层画面提供每个摘要信息 *帧* 抓获。
  - 中间屏幕提供表示组成部件（即TCP段报头，IP数据报头，以太网帧头等）的框架的击穿。
  - 下部屏幕示出了包括其数据字段中的整个帧如何在显示 *线（* 传输介质），即1和0（十六进制形式）。
- 从上面的屏幕包17将在下面的幻灯片，以便在展示被视为 *封装：*
  - 此帧包含一个HTTP 200 OK响应消息。

Wireshark的 打开屏幕（截图1）



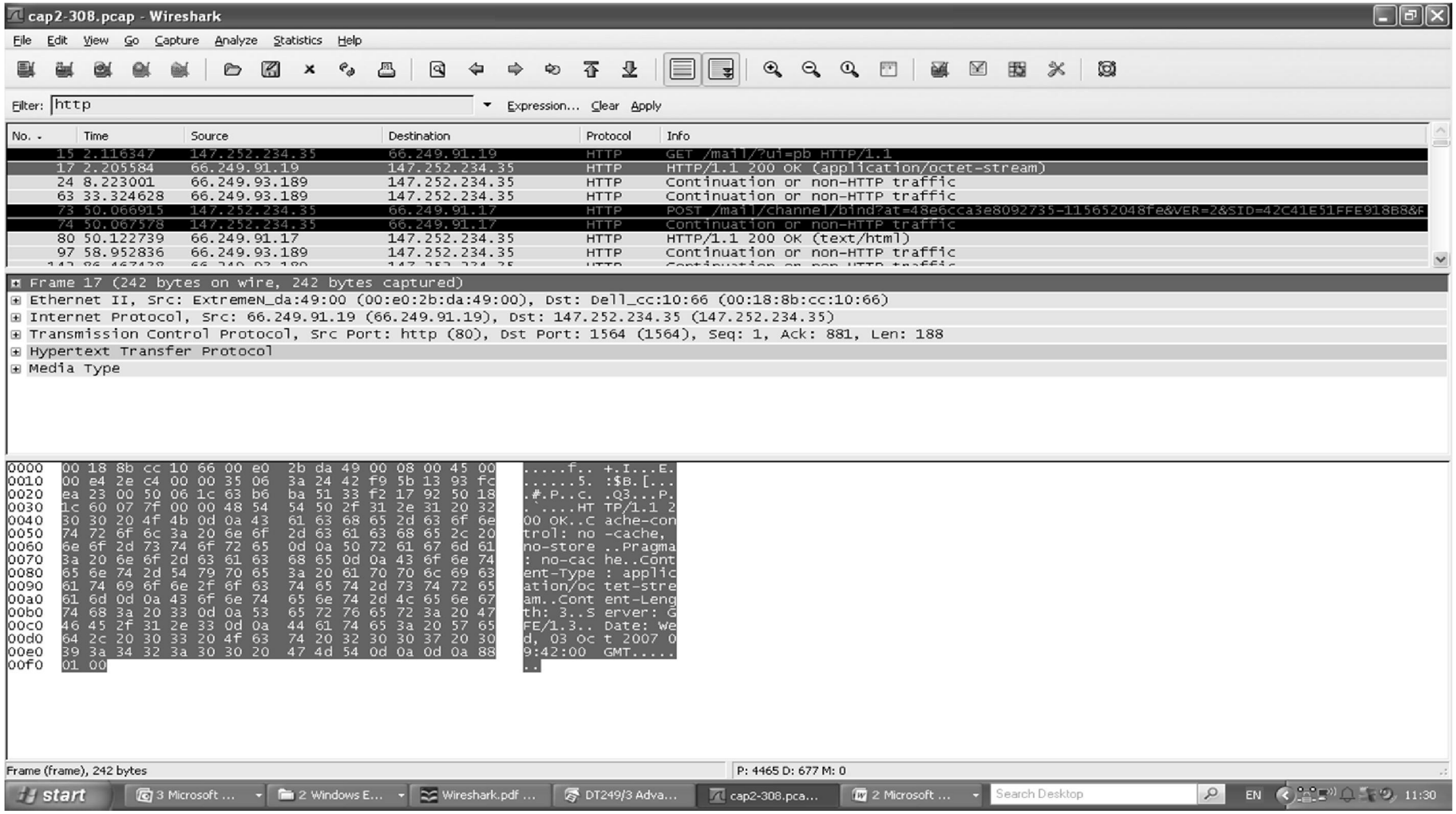
封装

- *封装* 是由此来自每个协议层的PDU被下一个协议层向下协议栈的有效载荷部分内进行的处理。例如：
  - HTTP请求/响应一个TCP内进行 *分割，*
  - 一个TCP段被一个IP内进行 *数据报，*
  - 一个IP报文的以太网内进行 *帧。*
- 下面的截图显示这一过程的例子：
  - 通过点击不同的组件头，中间屏幕与每个PDU报头类型（帧，IP和TCP）相关联的字节的位置可以看到突出底部屏幕上。

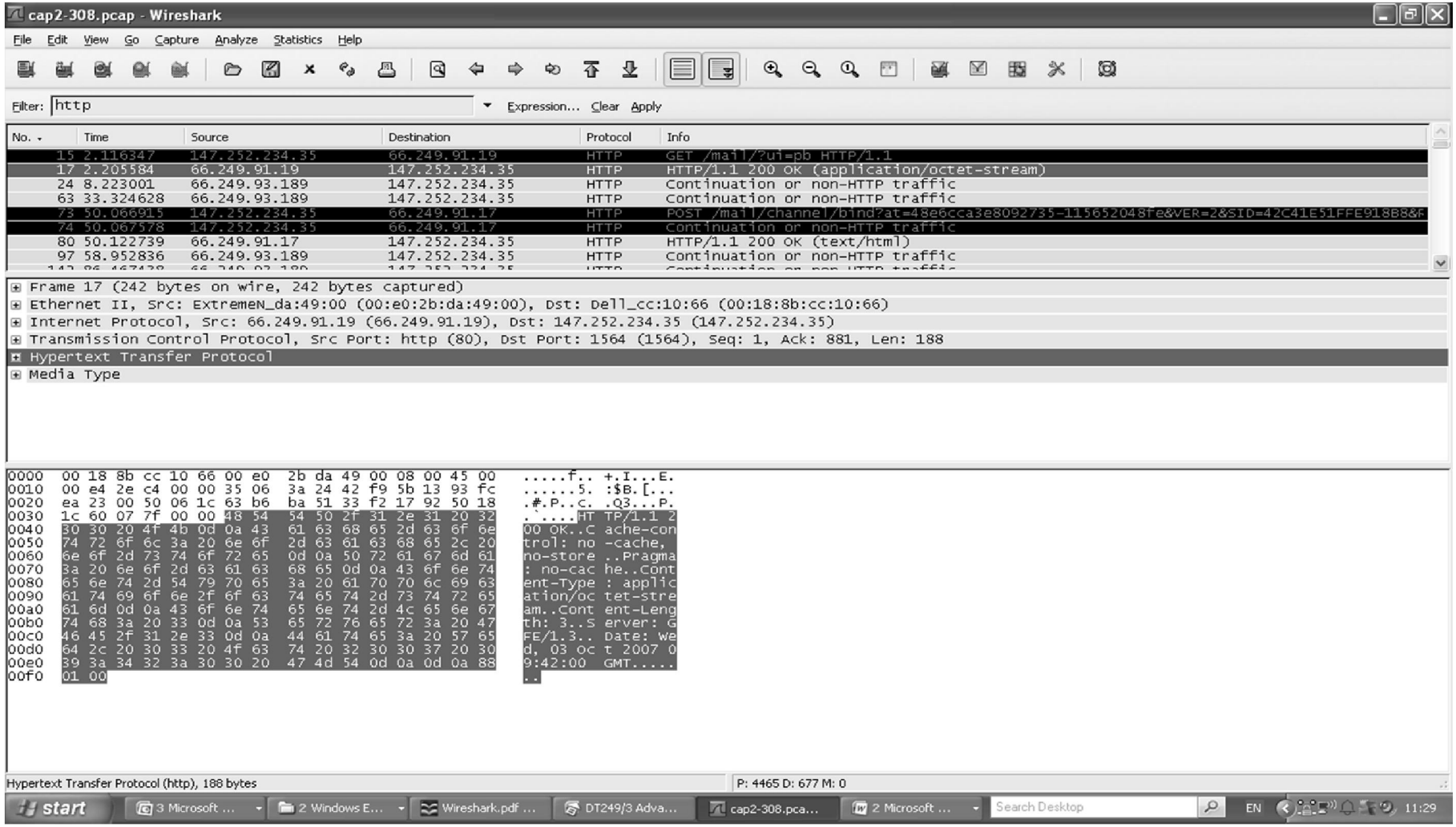
封装

- 请注意其中PDU头部出现的顺序：
  - 整个帧在屏幕截图2突出
    - 与所述帧相关联的所有字节在下部屏幕被突出正如人们所期望。
  - HTTP报头的数据在屏幕截图3突出
    - 与HTTP 200响应相关联的字节包括所述帧的所述最后部分
  - TCP报头的数据在屏幕截图4高亮显示
    - 与TCP分段报头相关联的字节先于HTTP响应数据
  - IP报头的数据在屏幕截图5突出
    - 与IP报头相关联的字节先于TCP段头
  - 帧头数据在屏幕截图6突出
    - 与所述帧报头相关联的字节先IP数据报头

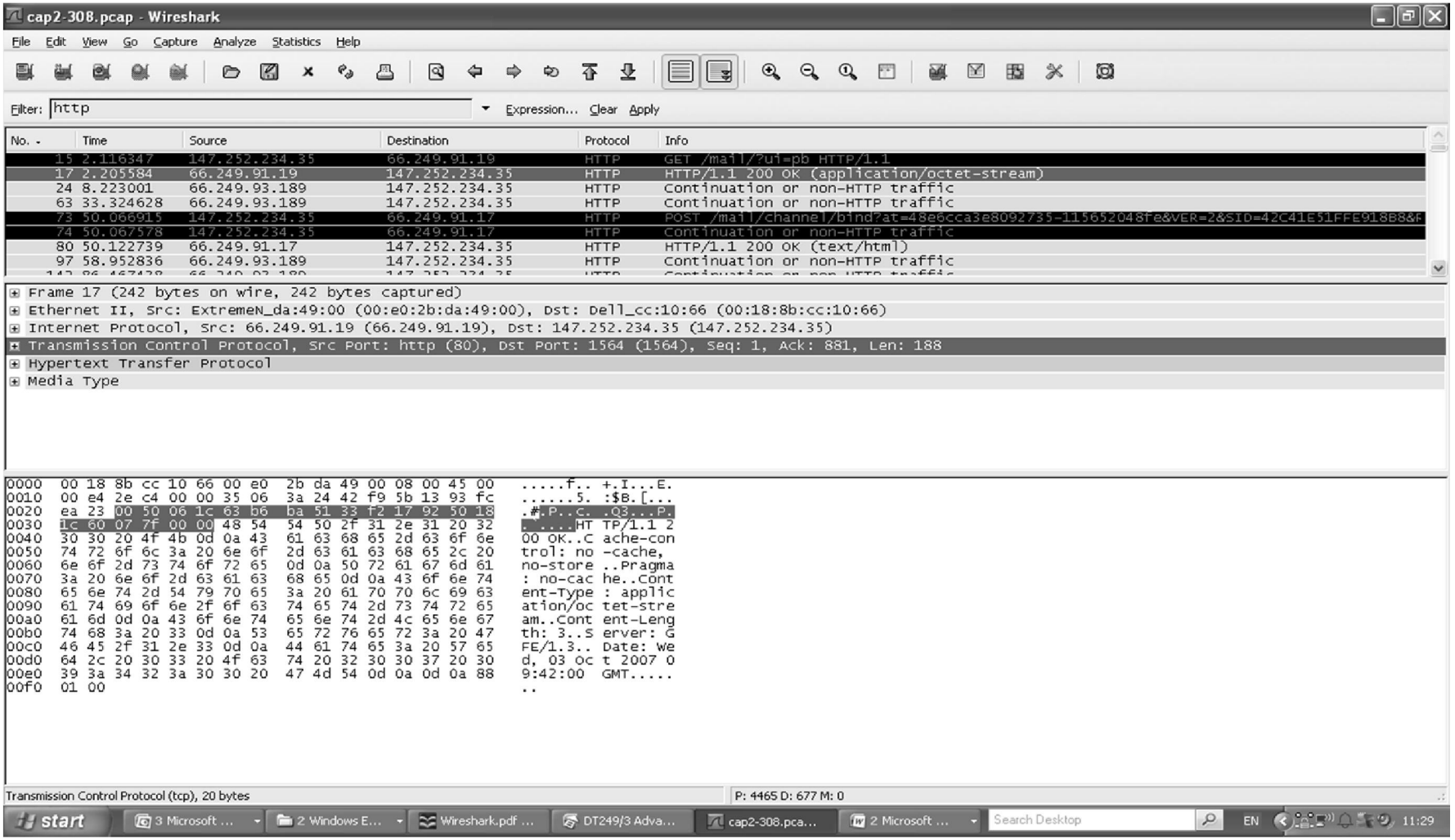
小号 creenshot 2 - 整个 *帧*



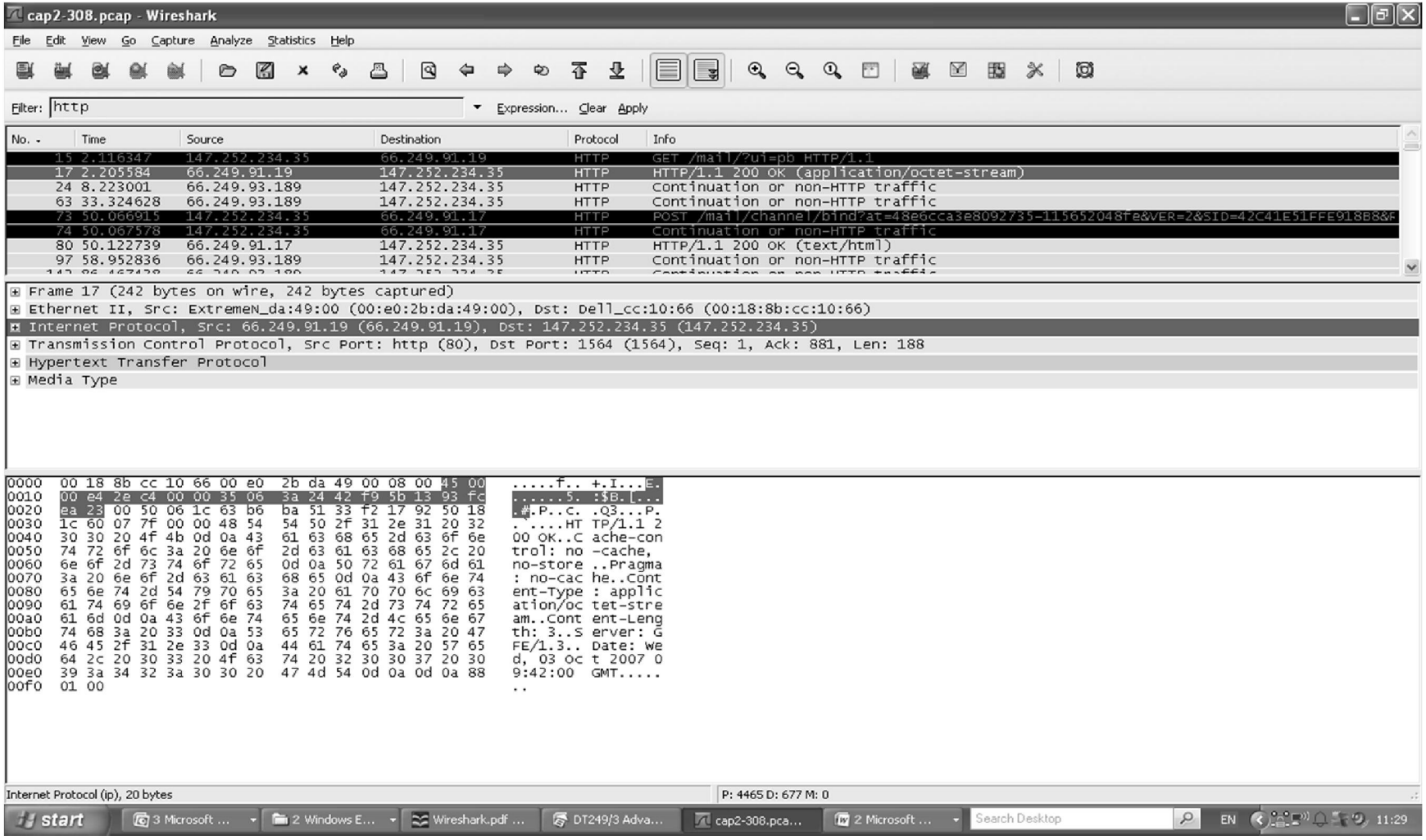
小号 creenshot 3 - 中 *HTTP* 响应数据



小号 creenshot 4日 - *TCP* 段头



小号 creenshot 5日 - *IP* 数据报头



小号 creenshot 6日 - *以太网络* 帧报头