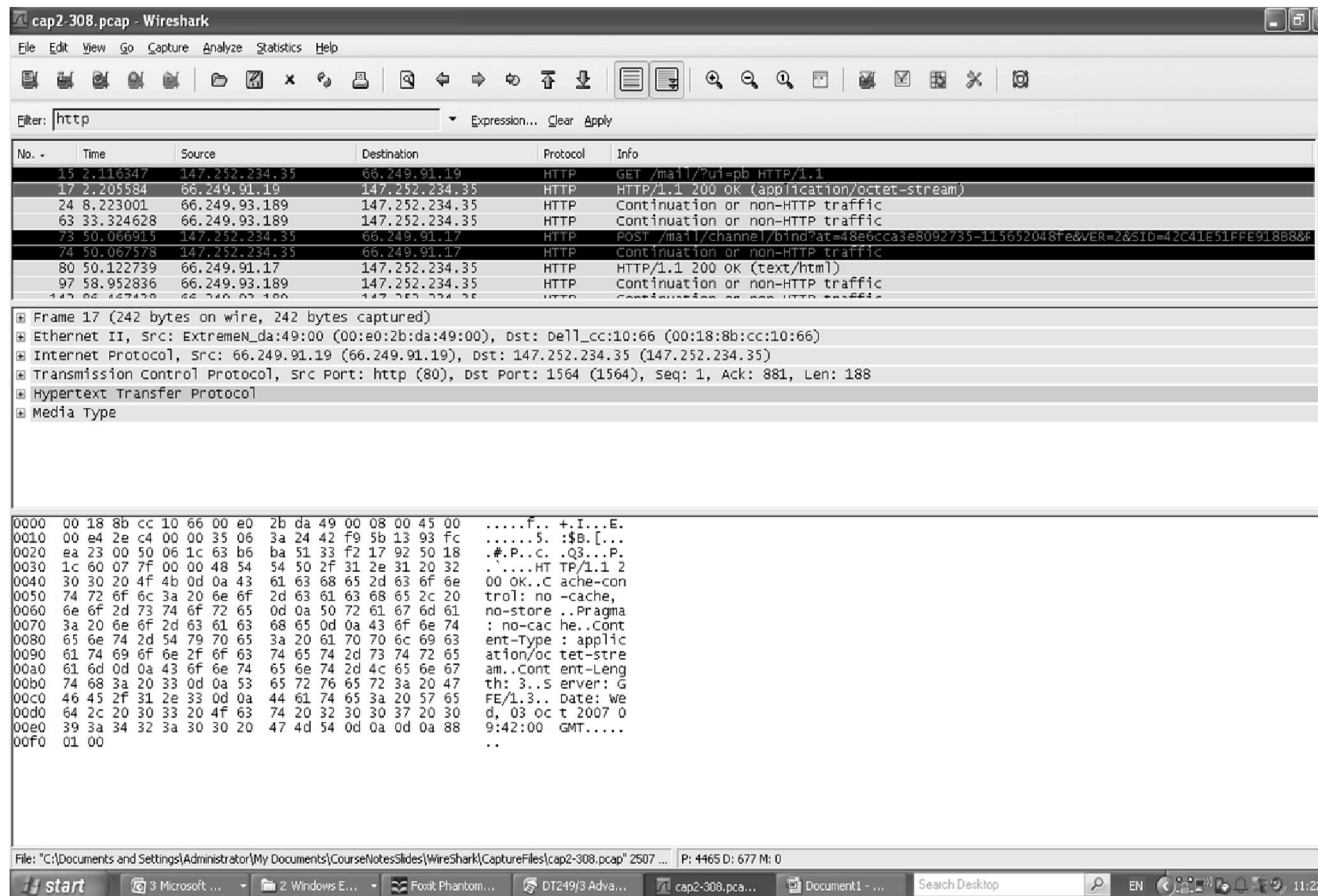


# Wireshark的 - 在工作协议

---

- 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 捕获。
  - 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 screenshot 2 - 整个 帧

cap2-308.pcap - Wireshark

Filter: http

No.	Time	Source	Destination	Protocol	Info
15	2.116347	147.252.234.35	66.249.91.19	HTTP	GET /mail/?ui=pb HTTP/1.1
17	2.205584	66.249.91.19	147.252.234.35	HTTP	HTTP/1.1 200 OK (application/octet-stream)
24	8.223001	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
63	33.324628	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
73	50.066915	147.252.234.35	66.249.91.17	HTTP	POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42c41e51f9e918b8&F
74	50.067578	147.252.234.35	66.249.91.17	HTTP	Continuation or non-HTTP traffic
80	50.122739	66.249.91.17	147.252.234.35	HTTP	HTTP/1.1 200 OK (text/html)
97	58.952836	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
147	66.467622	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic

Frame 17 (242 bytes on wire, 242 bytes captured)

- Ethernet II, Src: ExtremeN\_da:49:00 (00:e0:2b:da:49:00), Dst: Dell\_cc:10:66 (00:18:8b:cc:10:66)
- Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
- Hypertext Transfer Protocol
- Media Type

0000 00 18 8b cc 10 66 00 e0 2b da 49 00 08 00 45 00 .....f..+I...E.  
0010 00 e4 2e c4 00 00 35 06 3a 24 42 f9 5b 13 93 fc .....5.:\$B.[...  
0020 ea 23 00 50 06 1c 63 b6 ba 51 33 f2 17 92 50 18 .#.P..c...Q3...P..  
0030 1c 60 07 7f 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2  
0040 30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d 63 6f 6e 00 OK...C ache-con  
0050 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 2c 20 trol: no -cache,  
0060 6e 6f 2d 73 74 6f 72 65 0d 0a 50 72 61 67 6d 61 no-store ..Pragma  
0070 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 43 6f 6e 74 : no-cac he...Cont  
0080 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic  
0090 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 ation/oct et-stre  
00a0 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 am..Cont ent-Leng  
00b0 74 68 3a 20 33 0d 0a 53 65 72 76 65 72 3a 20 47 th: 3..S erver: G  
00c0 46 45 2f 31 2e 33 0d 0a 44 61 74 65 3a 20 57 65 FE/1.3.. Date: we  
00d0 64 2c 20 30 33 20 4f 63 74 20 32 30 30 37 20 30 d, 03 Oc t 2007 0  
00e0 39 3a 34 32 3a 30 30 20 47 4d 54 0d 0a 0d 0a 88 9:42:00 GMT.....  
00f0 01 00 ..

Frame (frame), 242 bytes

P: 4465 D: 677 M: 0

start 3 Microsoft ... 2 Windows E... Wireshark.pdf ... DT249/3 Adva... cap2-308.pca... 2 Microsoft ... Search Desktop EN 11:30

## 小号 screenshot 3 - 中 HTTP 响应数据

The screenshot shows the Wireshark network protocol analyzer interface. The main display area shows a list of captured packets, with packet 17 selected. The packet list shows the following details:

No.	Time	Source	Destination	Protocol	Info
15	2.116347	147.252.234.35	66.249.91.19	HTTP	GET /mail/?ui=pb HTTP/1.1
17	2.205584	66.249.91.19	147.252.234.35	HTTP	HTTP/1.1 200 OK (application/octet-stream)
24	8.223001	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
63	33.324628	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
73	50.066915	147.252.234.35	66.249.91.17	HTTP	POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42C41E51FFE918B8&F
74	50.087578	147.252.234.35	66.249.91.17	HTTP	Continuation or non-HTTP traffic
80	50.122739	66.249.91.17	147.252.234.35	HTTP	HTTP/1.1 200 OK (text/html)
97	58.952836	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic

The packet details pane for Frame 17 (242 bytes on wire, 242 bytes captured) shows the following structure:

- Ethernet II, Src: ExtremeN\_da:49:00 (00:e0:2b:da:49:00), Dst: Dell\_cc:10:66 (00:18:8b:cc:10:66)
- Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
- Hypertext Transfer Protocol
- Media Type

The packet bytes pane shows the raw data of the HTTP response, including the status line and headers:

```
0000 00 18 8b cc 10 66 00 e0 2b da 49 00 08 00 45 00 .....f..+.I...E.
0010 00 e4 2e c4 00 00 35 06 3a 24 42 f9 5b 13 93 fc .....5. :$B.[...
0020 ea 23 00 50 06 1c 63 b6 ba 51 33 f2 17 92 50 18 .#.P..c..Q3...P.
0030 1c 60 07 7f 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d 63 6f 6e 00 OK..C ache-con
0050 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 2c 20 trol: no -cache,
0060 6e 6f 2d 73 74 6f 72 65 0d 0a 50 72 61 67 6d 61 no-store ..Pragma
0070 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 43 6f 6e 74 : no-cac he..Cont
0080 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic
0090 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 ation/oct et-stre
00a0 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 am..Cont ent-Leng
00b0 74 68 3a 20 33 0d 0a 53 65 72 76 65 72 3a 20 47 th: 3..S erver: G
00c0 46 45 2f 31 2e 33 0d 0a 44 61 74 65 3a 20 57 65 FE/1.3.. Date: we
00d0 64 2c 20 30 33 20 4f 63 74 20 32 30 30 37 20 30 d, 03 oc t 2007 0
00e0 39 3a 34 32 3a 30 30 20 47 4d 54 0d 0a 0d 0a 88 9:42:00 GMT.....
00f0 01 00 ..
```

# 小号 creenshot 4日 - TCP 段头

cap2-308.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: http Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
15	2.116347	147.252.234.35	66.249.91.19	HTTP	GET /mail/?ui=pb HTTP/1.1
17	2.205584	66.249.91.19	147.252.234.35	HTTP	HTTP/1.1 200 OK (application/octet-stream)
24	8.223001	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
63	33.324628	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
73	50.066915	147.252.234.35	66.249.91.17	HTTP	POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&ver=2&SID=42C41E51FFE918B8&P...
74	50.067578	147.252.234.35	66.249.91.17	HTTP	Continuation or non-HTTP traffic
80	50.122739	66.249.91.17	147.252.234.35	HTTP	HTTP/1.1 200 OK (text/html)
97	58.952836	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
143	66.467478	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic

Frame 17 (242 bytes on wire, 242 bytes captured)

Ethernet II, Src: Extremen\_da:49:00 (00:e0:2b:da:49:00), Dst: Dell\_cc:10:66 (00:18:8b:cc:10:66)

Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)

Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188

Hypertext Transfer Protocol

Media Type

```
0000 00 18 8b cc 10 66 00 e0 2b da 49 00 08 00 45 00 .....f..+.I...E.
0010 00 e4 2e c4 00 00 35 06 3a 24 42 f9 5b 13 93 fc .....5. :$B.[...
0020 ea 23 00 50 06 1c 63 b6 ba 51 33 f2 17 92 50 18 .#.P..c..Q3...P.
0030 1c 60 07 f7 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d 63 6f 6e 00 OK..C ache-con
0050 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 2c 20 trol: no -cache,
0060 6e 6f 2d 73 74 6f 72 65 0d 0a 50 72 61 67 6d 61 no-store ..Pragma
0070 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 43 6f 6e 74 : no-cac he..Cont
0080 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic
0090 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 ation/oct et-stre
00a0 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 am..Cont ent-Leng
00b0 74 68 3a 20 33 0d 0a 53 65 72 76 65 72 3a 20 47 th: 3..s erver: G
00c0 46 45 2f 31 2e 33 0d 0a 44 61 74 65 3a 20 57 65 FE/1.3.. Date: we
00d0 64 2c 20 30 33 20 4f 63 74 20 32 30 30 37 20 30 d, 03 Oc t 2007 0
00e0 39 3a 34 32 3a 30 30 20 47 4d 54 0d 0a 0d 0a 88 9:42:00 GMT.....
00f0 01 00 ..
```

Transmission Control Protocol (tcp), 20 bytes P: 4465 D: 677 M: 0

start 3 Microsoft ... 2 Windows E... Wireshark.pdf ... DT249/3 Adva... cap2-308.pca... 2 Microsoft ... Search Desktop EN 11:29

# 小号 creenshot 5日 - IP 数据报头

cap2-308.pcap - Wireshark

Filter: http

No.	Time	Source	Destination	Protocol	Info
15	2.116347	147.252.234.35	66.249.91.19	HTTP	GET /mail/?ui=pb HTTP/1.1
17	2.205584	66.249.91.19	147.252.234.35	HTTP	HTTP/1.1 200 OK (application/octet-stream)
24	8.223001	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
63	33.324628	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
73	50.066915	147.252.234.35	66.249.91.17	HTTP	POST /mail/channel/bind?at=48e6ccae8092/35-115652048fe&ver=2&sid=42c41e51ffe918b8&...
74	50.067578	147.252.234.35	66.249.91.17	HTTP	Continuation or non-HTTP traffic
80	50.122739	66.249.91.17	147.252.234.35	HTTP	HTTP/1.1 200 OK (text/html)
97	58.952836	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
143	66.467428	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic

Frame 17 (242 bytes on wire (242 bytes captured) on interface 0: Ethernet II, Src: ExtremeN\_da:49:00 (00:e0:2b:da:49:00), Dst: Dell\_cc:10:66 (00:18:8b:cc:10:66)

Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)

Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188

Hypertext Transfer Protocol

Media Type

0000 00 18 8b cc 10 66 00 e0 2b da 49 00 08 00 45 00 .....f..+.i...E.  
0010 00 e4 2e c4 00 00 35 06 3a 24 42 f9 8b 15 93 fc .....5. :5B.[...  
0020 ea 23 00 50 06 1c 63 b6 ba 51 33 f2 17 92 50 18 .P..c. .Q3...P.  
0030 1c 60 07 7f 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2  
0040 30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d 63 6f 6e 00 OK..C ache-con  
0050 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 2c 20 trol: no -cache,  
0060 6e 6f 2d 73 74 6f 72 65 0d 0a 50 72 61 67 6d 61 no-store ..Pragma  
0070 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 43 6f 6e 74 : no-cac he..Cont  
0080 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic  
0090 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 ation/oc tet-stre  
00a0 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 am..Cont ent-Leng  
00b0 74 68 3a 20 33 0d 0a 53 65 72 76 65 72 3a 20 47 th: 3..S erver: G  
00c0 46 45 2f 31 2e 33 0d 0a 44 61 74 65 3a 20 57 65 FE/1.3.. Date: we  
00d0 64 2c 20 30 33 20 4f 63 74 20 32 30 30 37 20 30 d, 03 Oc t 2007 0  
00e0 39 3a 34 32 3a 30 30 20 47 4d 54 0d 0a 0d 0a 88 9:42:00 GMT.....  
00f0 01 00 ..

Internet Protocol (ip), 20 bytes P: 4465 D: 677 M: 0



# 小号 screenshot 6日 - 以太网网络帧报头

cap2-308.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: http Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
15	2.116347	147.252.234.35	66.249.91.19	HTTP	GET /mail/?ui=pb HTTP/1.1
17	2.205584	66.249.91.19	147.252.234.35	HTTP	HTTP/1.1 200 OK (application/octet-stream)
24	8.223001	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
63	33.324628	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
73	50.066915	147.252.234.35	66.249.91.17	HTTP	POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42c41e51ffe918b8&...
74	50.067578	147.252.234.35	66.249.91.17	HTTP	Continuation or non-HTTP traffic
80	50.122739	66.249.91.17	147.252.234.35	HTTP	HTTP/1.1 200 OK (text/html)
97	58.952836	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic
143	86.467438	66.249.93.189	147.252.234.35	HTTP	Continuation or non-HTTP traffic

Frame 17 (242 bytes on wire, 242 bytes captured)

- Ethernet II, Src: ExtremeN\_da:49:00 (00:e0:2b:da:49:00), Dst: dell\_cc:10:66 (00:18:8b:cc:10:66)
- Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
- Hypertext Transfer Protocol
- Media Type

0000 00 18 8b cc 10 66 00 e0 2b da 49 00 08 00 45 00 .....f..+I...E.  
0010 00 e4 2e c4 00 00 35 06 3a 24 42 f9 5b 13 93 fc .....5.:\$B.[...  
0020 ea 23 00 50 06 1c 63 b6 ba 51 33 f2 17 92 50 18 .#.P..C..Q3...P.  
0030 1c 60 07 7f 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2  
0040 30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d 63 6f 6e 00 OK..C ache-con  
0050 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 2c 20 trol: no -cache,  
0060 6e 6f 2d 73 74 6f 72 65 0d 0a 50 72 61 67 6d 61 no-store ..Pragma  
0070 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 43 6f 6e 74 : no-cac he..Cont  
0080 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic  
0090 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 ation/oct et-stre  
00a0 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 am..Cont ent-Leng  
00b0 74 68 3a 20 33 0d 0a 53 65 72 76 65 72 3a 20 47 th: 3..s erver: G  
00c0 46 45 2f 31 2e 33 0d 0a 44 61 74 65 3a 20 57 65 FE/1.3.. Date: we  
00d0 64 2c 20 30 33 20 4f 63 74 20 32 30 30 37 20 30 d, 03 oc t 2007 0  
00e0 39 3a 34 32 3a 30 30 20 47 4d 54 0d 0a 0d 0a 88 9:42:00 GMT.....  
00f0 01 00 ..

Ethernet (eth), 14 bytes P: 4465 D: 677 M: 0

start 3 Microsoft ... 2 Windows E... Wireshark.pdf ... DT249/3 Adva... cap2-308.pca... 2 Microsoft ... Search Desktop EN 11:29