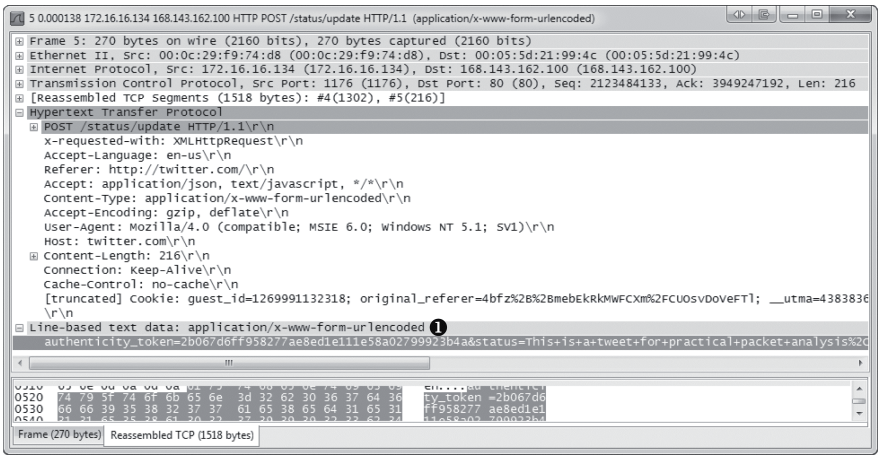
Zwróć uwagę na informację znajdującą się w polu *Line-based text data* (zob. rysunek 8.5). Podczas analizy tych danych zobaczysz pole o nazwie *Authenticity Token*, pod którym znajduje się pole *status* w adresie URL, zawierające następującą wartość:

```
This+is+a+tweet+for+practical+packet+analysis%2c+second+edition
```



Rysunek 8.5. Wiadomość serwisu Twitter w postaci zwykłego tekstu

Wartość pola *status* jest wiadomością serwisu Twitter, która została wysłana w postaci zwykłego, niezaszyfrowanego tekstu.

Jest to problem z punktu widzenia zapewnienia bezpieczeństwa, ponieważ niektóre osoby chronią swoje wiadomości i nie chcą, aby były one wyświetlane innym użytkownikom. To oczywiście nie oznacza, że każdy może odczytać wiadomość serwisu Twitter. Jednak użytkownik znajdujący się w tej samej sieci może przechwycić omówiony tutaj ruch sieciowy i poznać treść wiadomości.

Wiadomości bezpośrednie w serwisie Twitter

twitter_dm.pcap

Teraz zajmiemy się sytuacją, w której również występują pewne problemy związane z bezpieczeństwem: wiadomości bezpośrednie w serwisie Twitter pozwalające użytkownikom na przekazywanie sobie wiadomości prywatnych. Plik o nazwie *twitter_dm.pcap* zawiera dane przechwycone podczas przesyłania wspomnianych wiadomości w serwisie Twitter. Jak możesz zobaczyć na rysunku 8.6, wiadomości bezpośrednie wcale nie są aż tak bardzo prywatne.

Wyświetlony na rysunku 8.6 pakiet siódmy pokazuje, że treść wiadomości bezpośredniej ma postać zwykłego tekstu. Użyte jest dokładnie to samo pole *Line-based text data* ❶, z którym spotkaliśmy się podczas analizy danych w poprzednim pliku.