

### LABORATORIO DIDATTICO 3

#### Analizzatori di protocollo per WAN e analisi del protocollo PPP

Nelle reti di telecomunicazioni sia geografiche (*Wan, Wide Area Network*) sia locali (*LAN, Local Area Network*) è molto spesso utile avere a disposizione degli strumenti che eseguano un'analisi dei molti protocolli implementati (strati OSI 2÷7) e che siano in grado di produrre statistiche sugli errori e valutazioni sulla reale percentuale di utilizzo delle reti e delle connessioni.

A tale scopo si può utilizzare un *analizzatore di protocollo*.

Gli *analizzatori di protocollo per WAN*, sono strumenti hardware, dotati di software opportuno e interfacciati spesso con un PC per la presentazione dei risultati e la memorizzazione dei dati catturati, i quali sono inseriti in una connessione, per esempio tra un DTE e un DCE, come illustrato in FIGURA 1, e ne consentono l'analisi a tutti i livelli.

Va notato che il DTE è spesso un router e che lo strumento può supportare diversi tipi di interfaccia (V.24/V.28, V.35, ecc.) e deve poter analizzare diversi tipi di frame (HDLC, PPP, Frame Relay, ecc.) oltre a decodificare i protocolli degli strati OSI 3÷7 (tipicamente facenti parte della suite TCP/IP) trasportati (incapsulati) su interfacce e connessioni che possono essere differenti (linea dedicata, commutata, Frame Relay, ecc.).

Se usato come monitor di linea, l'analizzatore mostra il traffico scambiato nelle due direzioni (DTE⇒DCE e DCE⇒DTE); di solito, poi, questi strumenti integrano un *data tester* per consentire anche l'effettuazione del *BERT (Bit Error Rate Test)*.

In FIGURA 2 sono mostrate a titolo esemplificativo le possibilità offerte da uno di questi analizzatori, il Feline Parascope con software Feline WAN XL ([www.fetest.com](http://www.fetest.com)).

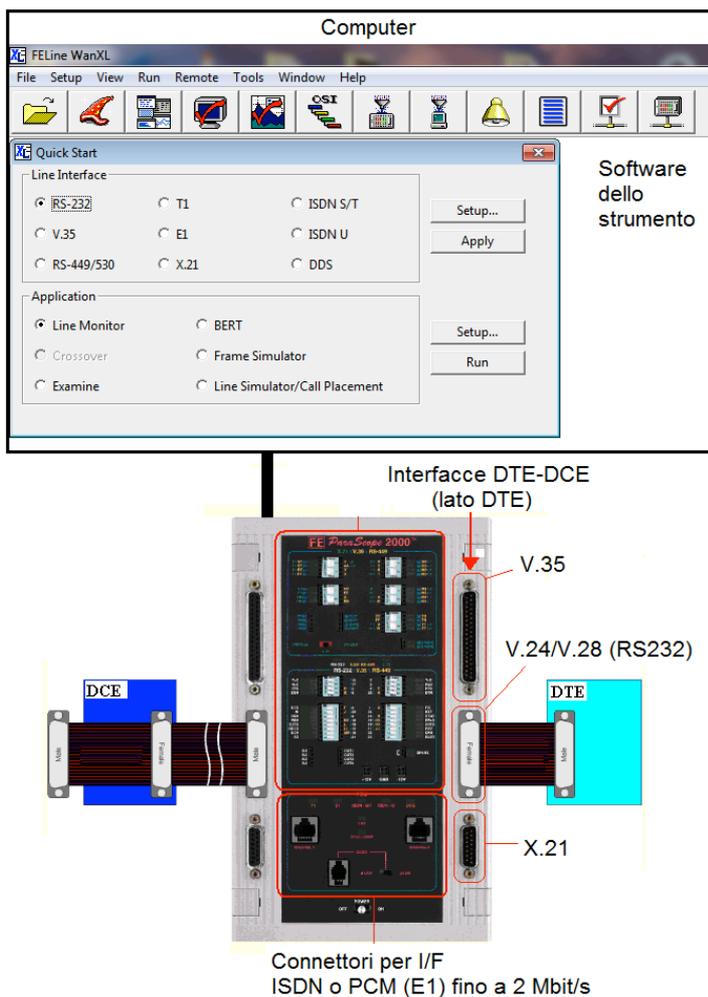


FIGURA 1 Esempio di analizzatore di protocollo per WAN

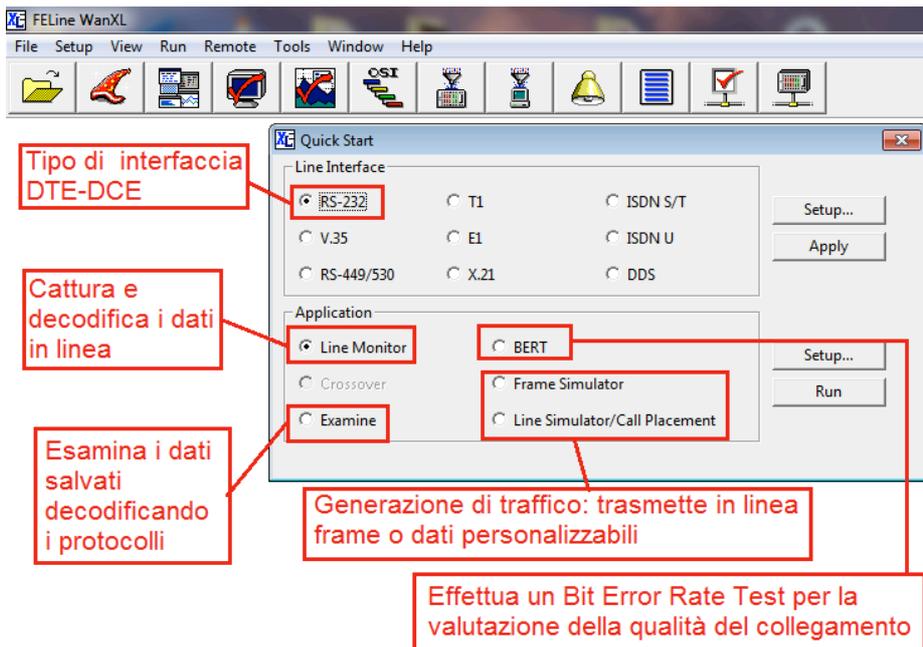


FIGURA 2 Esempio di possibilità offerte da un analizzatore di protocollo per Wan

A titolo esemplificativo si illustrano i passi per effettuare l'analisi di una connessione su linea dedicata, realizzata interconnettendo con due doppini (TX, RX) due DCE banda base, che mette in comunicazione due router (DTE) tramite cui si interconnettono due LAN. Come protocollo di linea si impiega il protocollo PPP (*encapsulation PPP*) per trasportare i protocolli della suite TCP/IP. L'interfaccia seriale dei router è di tipo V.24/V.28 (RS232) operante in sincrono. Come prima cosa si effettua la configurazione (*setup*) dello strumento per operare con l'interfaccia in oggetto (strato 1 OSI), FIGURA 3.

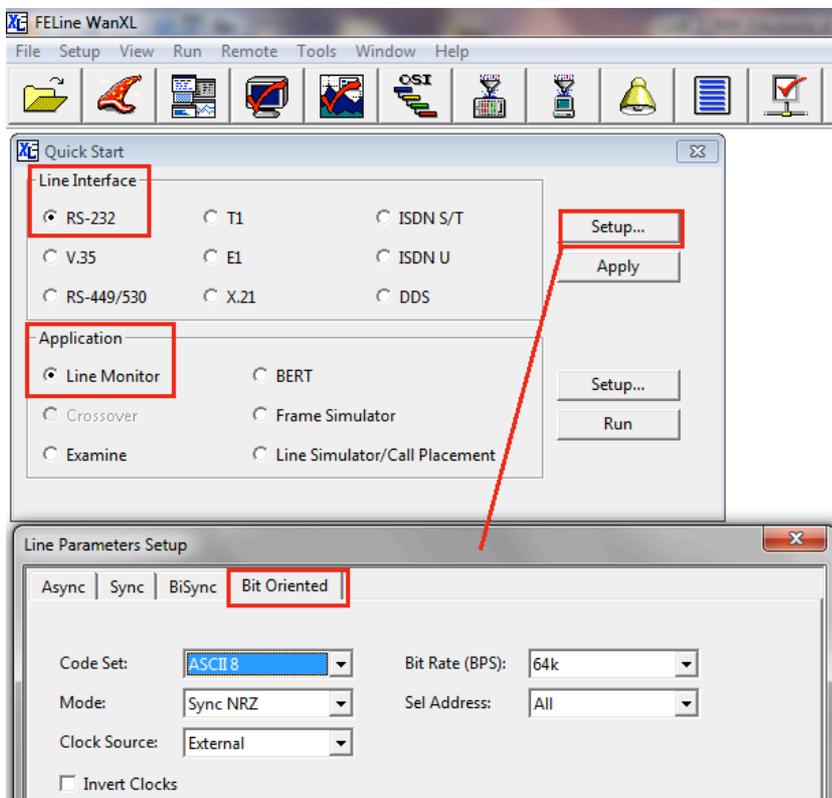


FIGURA 3 Configurazione dell'interfaccia

Si passa quindi alla scelta del protocollo di linea (*link protocol*, strato 2 OSI), selezionando il PPP (*Point to Point Protocol*), e i protocolli di livello superiore della suite TCP/IP che interessa analizzare (strati OSI 3÷7),

FIGURA 4. Si passa quindi alla configurazione (*setup*) dell'analizzatore di protocollo (applicazione *line monitor*) per definire le statistiche che interessano.

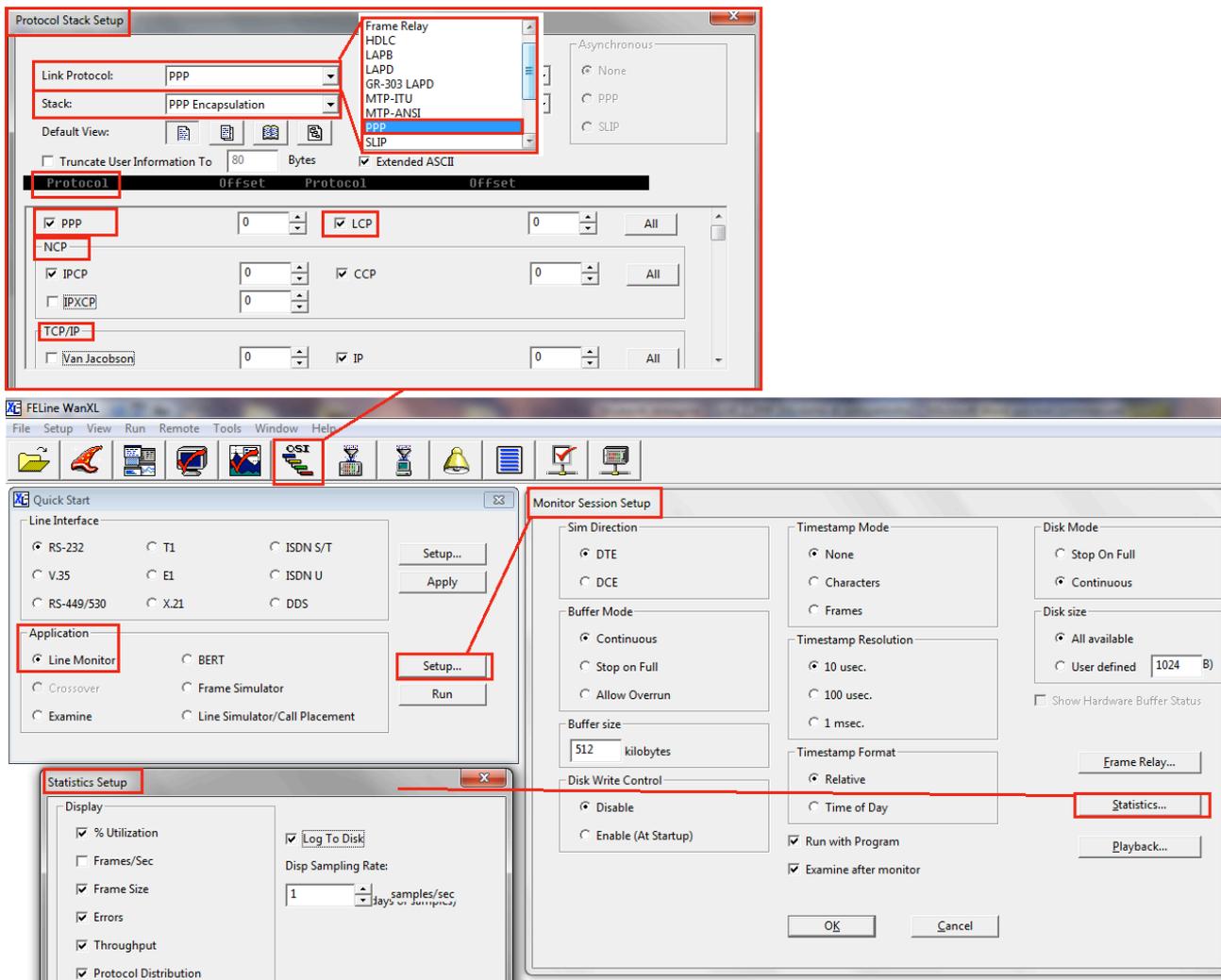


FIGURA 4 Esempio di configurazione di un analizzatore per l'analisi di frame PPP che trasportano i protocolli della suite TCP/IP.

Terminata la fase di configurazione, cliccando su *Run* si avvia la cattura dei dati in linea, i quali possono essere salvati in un file (*save as*) ed esaminati (menu *Examine*) successivamente.

L'esame può essere condotto praticamente su tutti gli strati OSI. Si possono infatti visualizzare, in esadecimale (o in formato carattere), tutti gli oggetti trasmessi in linea e ciò consente, per esempio, di verificare la struttura di un frame PPP, FIGURA 5.

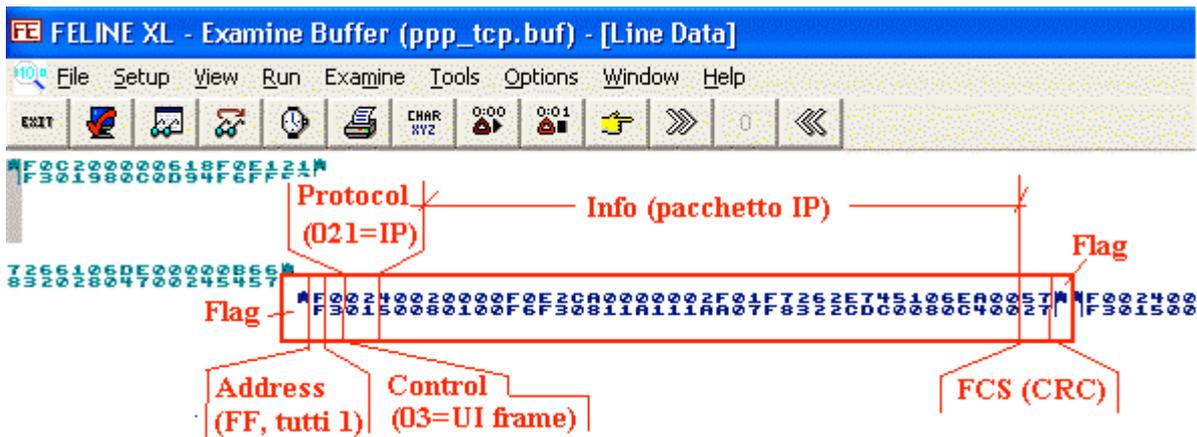


FIGURA 5 Esempio di visualizzazione dei dati trasmessi in linea: è evidenziata la struttura di un frame PPP (il contenuto dei campi è in formato esadecimale).

Si può quindi decidere di vedere un sommario (*summary*) della decodifica nei vari frame, FIGURA 6, che mostra esplicitamente, frame per frame (ogni riga è un frame), il contenuto degli header del protocollo di livello 2 e dei protocolli trasportati (l'IP con evidenziati gli indirizzi IP della sorgente e della destinazione, il TCP con evidenziate le porte sorgente e destinazione, da cui si evince che si sta utilizzando l'applicazione TCP/IP *Telnet*).

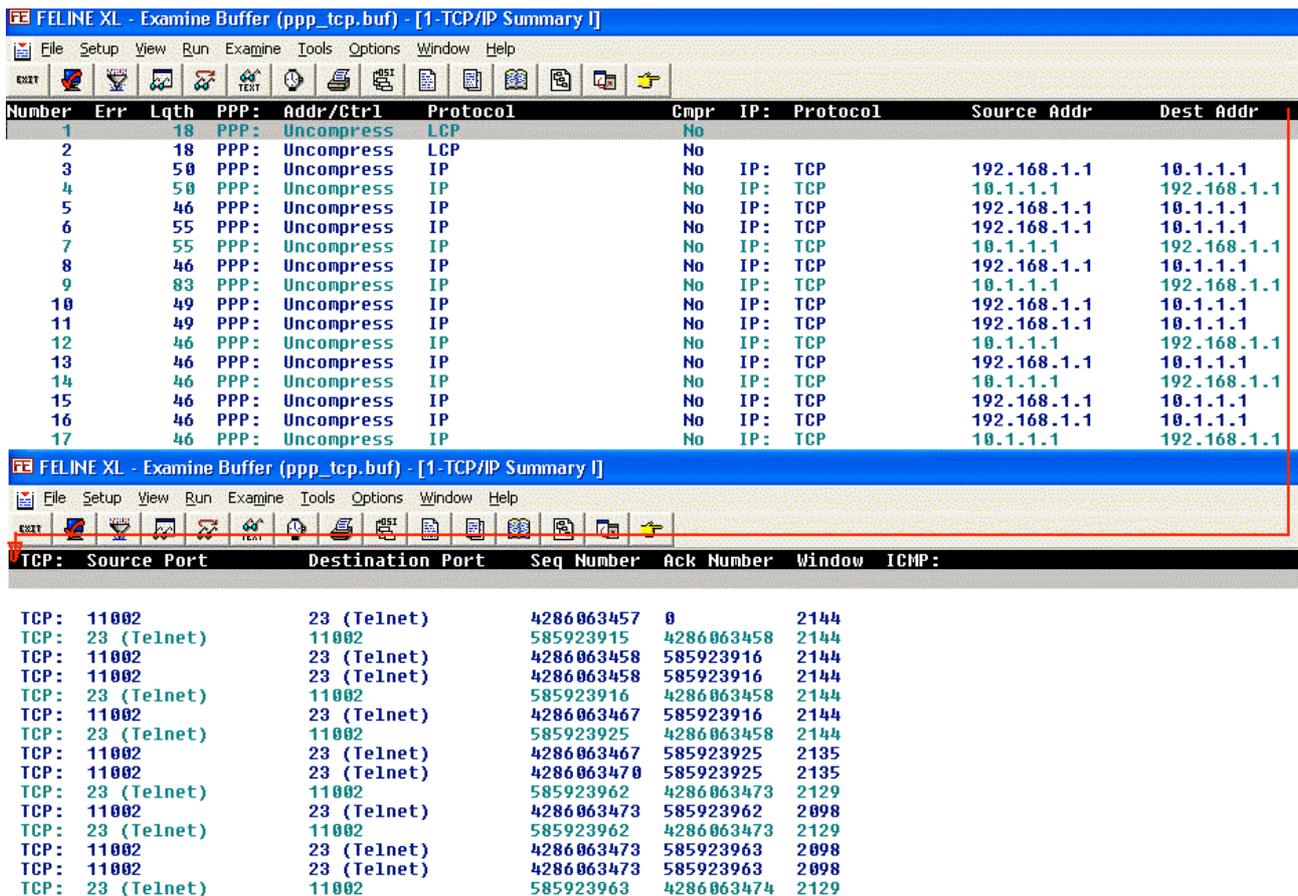


FIGURA 6 Esempio di sommario della decodifica di frame PPP. I frame sono numerati e se evidenzia la lunghezza; sono quindi mostrati i campi principali dei vari header dei protocolli trasportati nel frame.

Si può quindi analizzare nel dettaglio ogni singolo frame PPP, visualizzando la decodifica completa delle intestazioni<sup>1</sup> (*header*) sia del PPP sia delle PDU dei protocolli trasportati, che nell'esempio di FIGURA 7 sono in un frame PPP il protocollo LCP mentre nell'altro frame è l'IP (che a sua volta trasporta una PDU del protocollo ICMP, con cui si invia una *Echo Request* per il comando *ping*). Si possono anche visualizzare le effettive informazioni inviate, se sono in chiaro come quando si impiega l'applicazione *Telnet*, FIGURA 8.

The screenshot shows the 'Examine Buffer' window of Feline WanXL. It displays two PPP frames with their respective details:

**Frame 30 (18 bytes) was captured with no errors.**

- PPP:
  - Addr/Ctrl = Uncompress
  - Protocol = LCP
  - Compression = No
- LCP:
  - Code = Echo Reply
  - Identifier = 8
  - Length = 12
  - Magic Number = 843006
  - Data = 0000 0000

**Frame 31 (106 bytes) was captured with no errors.**

- PPP:
  - Addr/Ctrl = Uncompress
  - Protocol = IP
  - Compression = No
- IP:
  - Version = 4, IP Header Length (bytes) = 20
  - Time to Live = 255
  - Protocol = ICMP
  - Header Checksum = EE E3
  - Source Address = 192.168.1.1, Destination Address = 10.1.1.1
- ICMP:
  - Type = Echo
  - Code = 0

Red annotations in the image provide context:

- A red box highlights the LCP details in Frame 30.
- A red box highlights the IP and ICMP details in Frame 31.
- Red arrows point from the text 'Frame PPP che trasporta una PDU del protocollo LCP (con cui si verifica lo stato della linea)' to Frame 30.
- Red arrows point from the text 'Frame PPP che incapsula un pacchetto IP (il quale trasporta una PDU del protocollo ICMP)' to Frame 31.
- Red text labels 'Pacchetto IP' and 'PDU ICMP (Echo Request)' are placed next to the IP and ICMP sections respectively.

FIGURA 7 Esempio di decodifica di due frame PPP, uno nella fase LCP e uno che incapsula un pacchetto IP.

<sup>1</sup> L'analizzatore non mostra la decodifica dei campi non utilizzati o con contenuto fisso, che nel PPP sono il flag, l'address (FF esadecimale, tutti 1), il control (03 esadecimale fisso); anche il campo FCS (Frame Check Sequence), che contiene il CRC per la rivelazione d'errore, non viene decodificato.

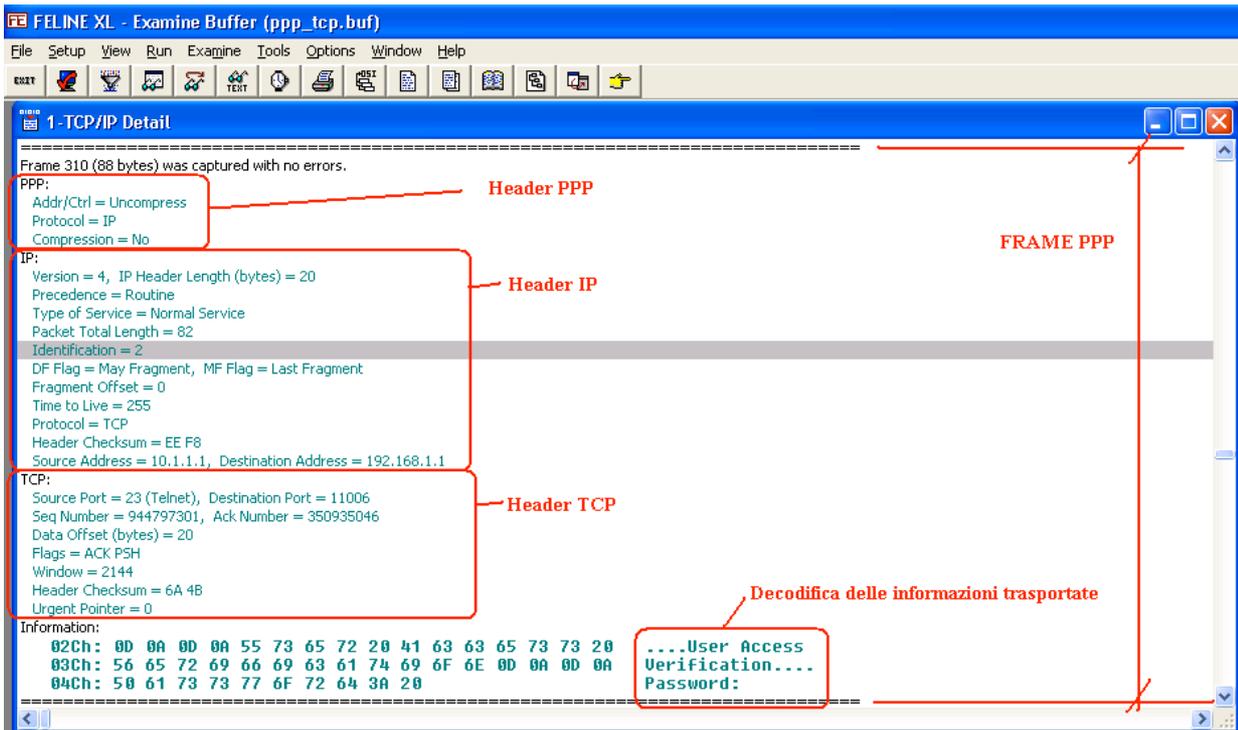


FIGURA 8 Esempio di decodifica completa di un frame PPP, che mostra gli header dei protocolli trasportati (IP e TCP) e le informazioni scambiate dai DTE (sia in esadecimale sia in formato carattere).

Infine, se sono state configurate, è possibile esaminare le statistiche relative al traffico sulla connessione (FIGURA 9) come: frame al secondo scambiati, i frame errati, la distribuzione della dimensione dei frame e la percentuale di utilizzo della connessione.

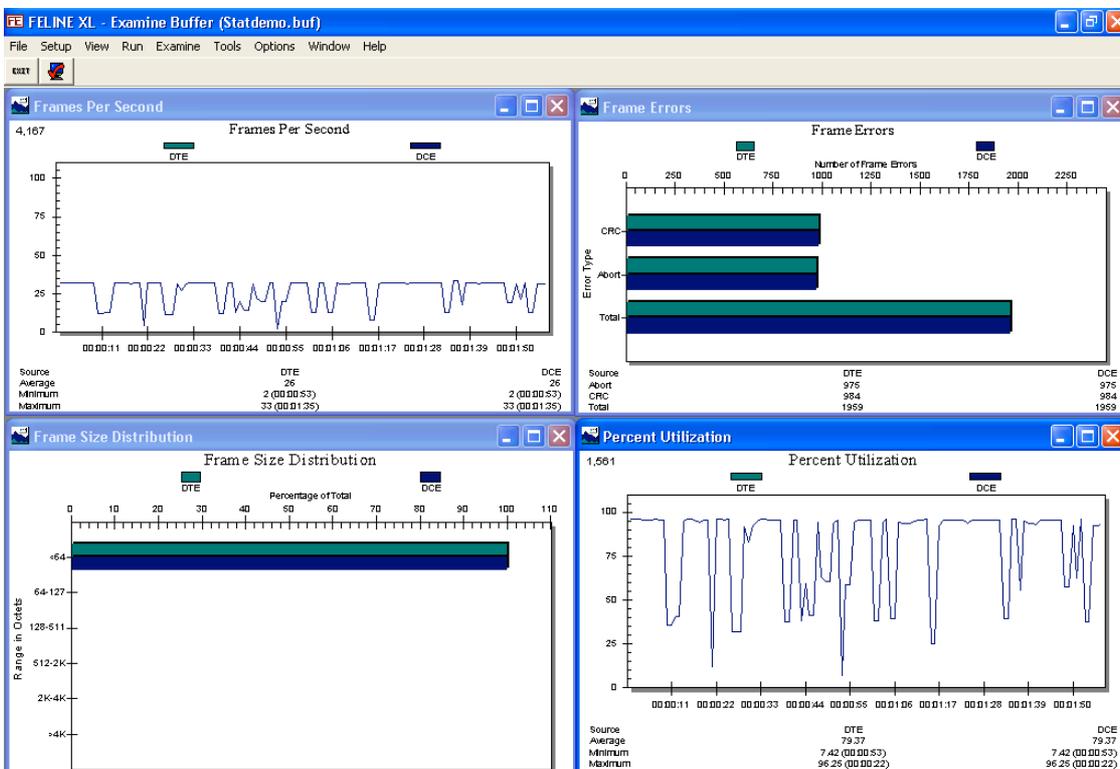


FIGURA 9 Esempio di statistiche di traffico.