Y36SPS
Proxy sniffer

Vojtěch Krása

krasav1@fel.cvut.cz

Proč proxy sever?

- Jediný možný způsob jak odchytit lokální komunikaci

Popis programu

- Open-source JpcapDumper + TCP Proxy server
- JpcapDumper – zobrazuje pakety zachycené pomocí Jpcap.
- Jpcap – knihovna k zachycení a posílání síťových paketů

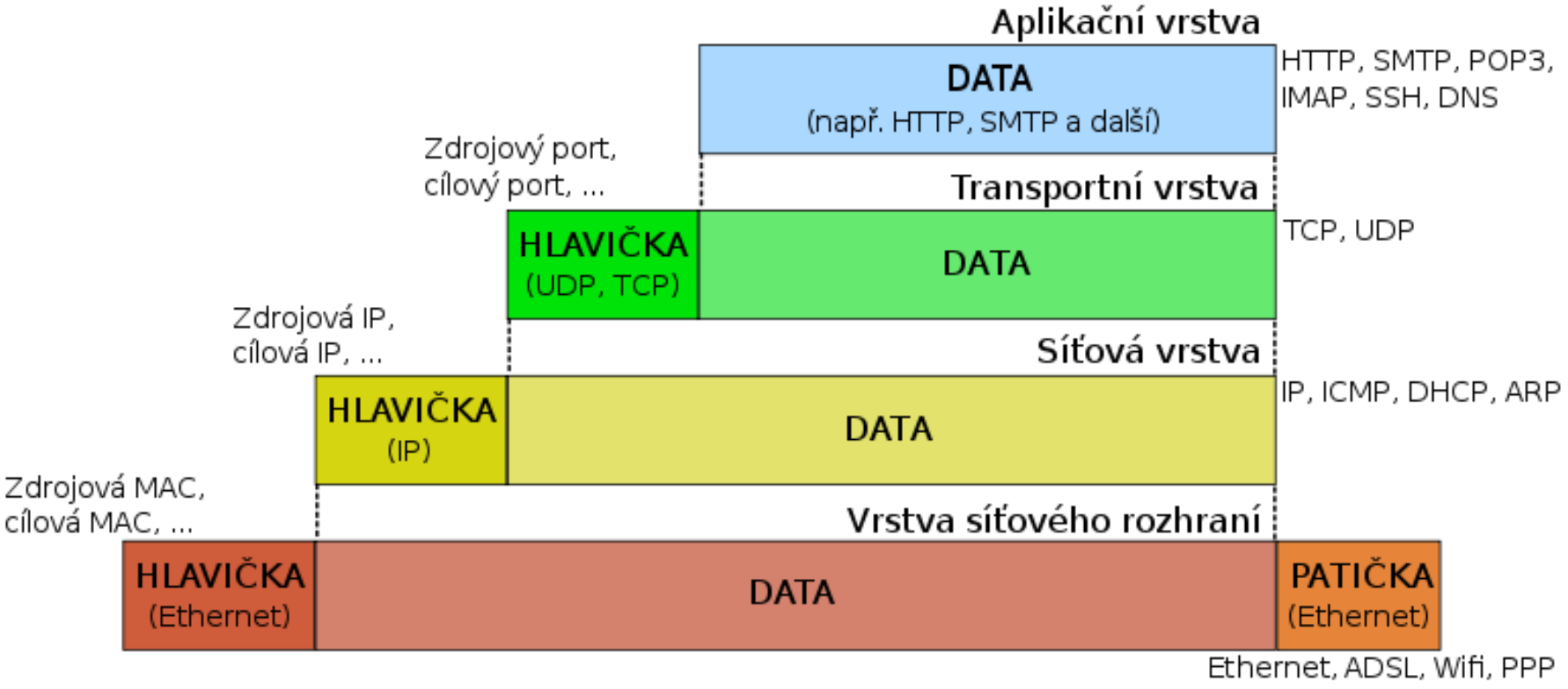
Jak to funguje

- JpcapDumper zavolá metodu proxyServer.processPacket(handler);
- Proxy pak volá handler.receiveMessage(packet)
- *handler je anonymní třída*

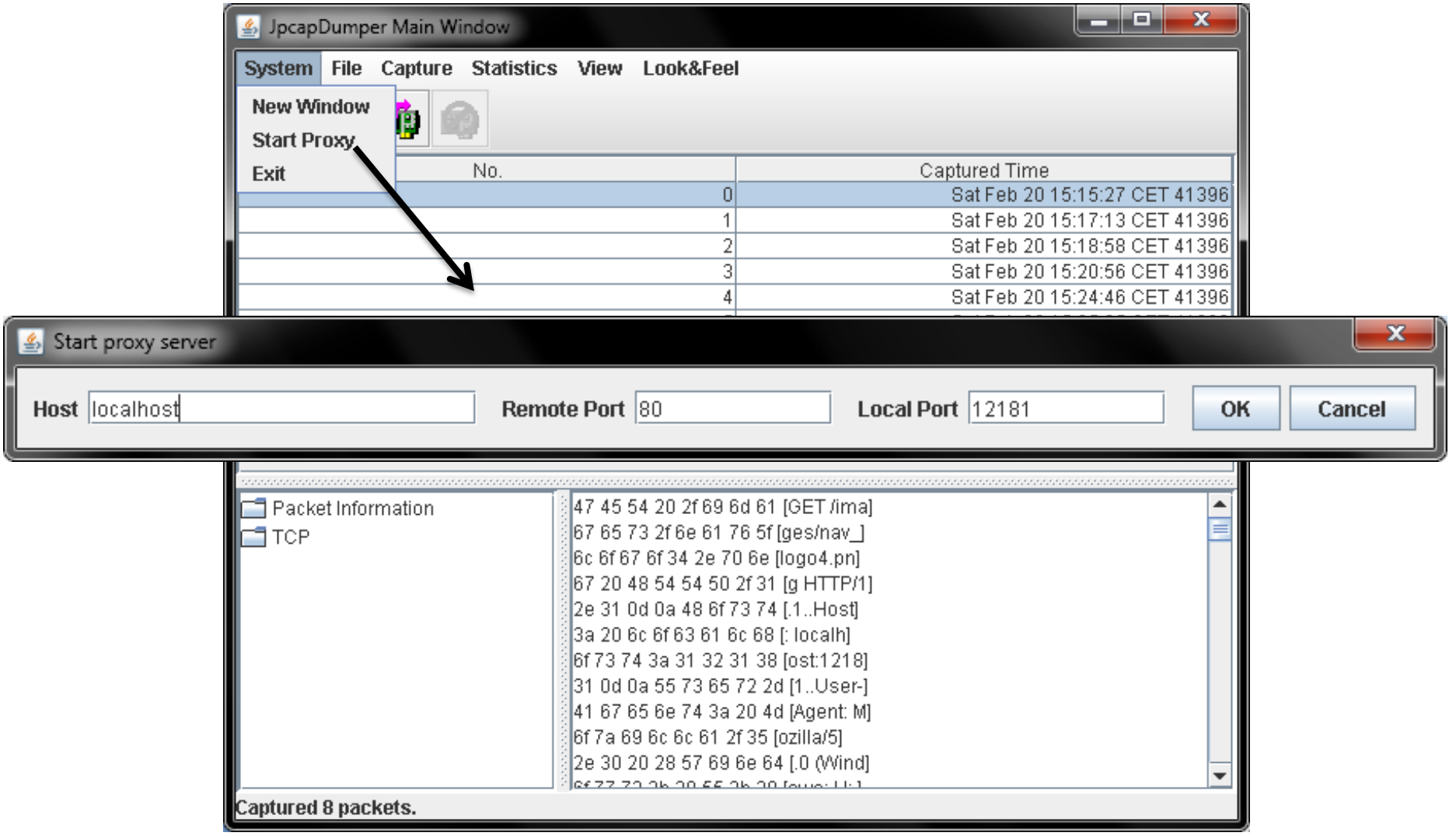
```
private PacketReceiver handler = new PacketReceiver() {
        public void receivePacket(Packet packet) {   …
        }
}
```

Nevýhody

- Java zobrazuje pouze aplikační vrstvu



GUI


JpcapDumper Main Window
System
File
Capture
Statistics
View
Look&Feel
New Window
Start Proxy
Exit
No.
Captured Time
0
Sat Feb 20 15:15:27 CET 41396
1
Sat Feb 20 15:17:13 CET 41396
2
Sat Feb 20 15:18:58 CET 41396
3
Sat Feb 20 15:20:56 CET 41396
4
Sat Feb 20 15:24:46 CET 41396
Start proxy server
Host
localhost
Remote Port
80
Local Port
12181
OK
Cancel
Packet Information
TCP
47 45 54 20 2f 69 6d 61 [GET /ima]
67 65 73 2f 6e 61 76 5f [ges/nav_]
6c 6f 67 6f 34 2e 70 6e [logo4.pn]
67 20 48 54 54 50 2f 31 [g HTTP/1]
2e 31 0d 0a 48 6f 73 74 [.1..Host]
3a 20 6c 6f 63 61 6c 68 [: localh]
6f 73 74 3a 31 32 31 38 [ost:1218]
31 0d 0a 55 73 65 72 2d [1..User-]
41 67 65 6e 74 3a 20 4d [Agent: M]
6f 7a 69 6c 6c 61 2f 35 [ozilla/5]
2e 30 20 28 57 69 6e 64 [.0 (Wind]
Captured 8 packets.

Děkuji za pozornost