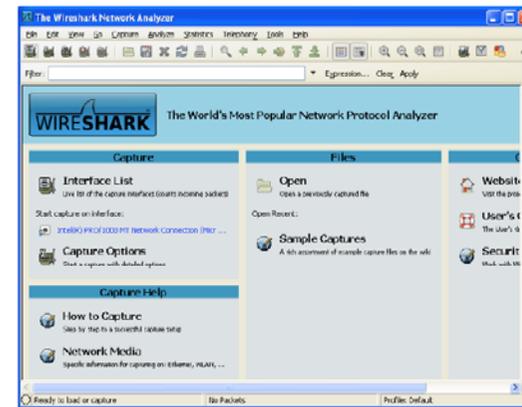


CSE 3214: Computer Network Protocols and Applications

– Network Monitoring & Protocol Analysis

Dr. Peter Lian, Professor
Department of Computer Science and Engineering
York University
Email: peterlian@cse.yorku.ca
Office: I012C Lassonde Building
Course website:
http://wiki.cse.yorku.ca/course_archive/2012-13/W/3214

Wireshark



Network Monitoring & Protocol Analysis

- Process of capturing network traffic and inspecting it closely to determine type and amount of data:
 - Traveling through your network, or
 - Arriving at your computer
- Network/protocol analysis is also known as “sniffing”

3

Network Analyzer

- Standalone hardware device or software installed on a computer – decodes data packets of common protocol and displays their content in human-readable format
- Network analyzers are either free and commercial
- Differences between network analyzers include:
 - Number of supported protocol decodes
 - Quality of packet decodes
 - User interface
 - Graphing and statistical capabilities

4

Network Analyzer Applications

- As an educational resource when learning about protocols
- Analyzing the operations of applications and protocols they rely upon
- Network intrusion detection
- Debugging in the development stage of network programming
- Reverse-engineering of protocols in order to write supporting programs

5

Common Network Analyzer

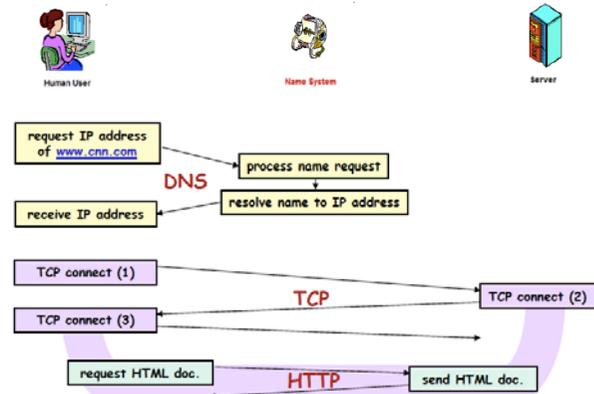
- Wireshark – freeware, runs on different platforms, decodes hundreds of protocols
- Snort, WinDump/TcpDump, Dsniff, etc.



6

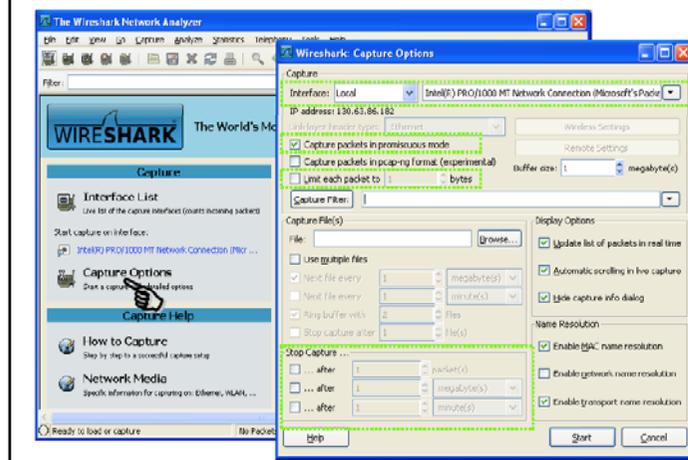
Wireshark Network Analyzer

Example: retrieval of www.cnn.com web page



7

Wireshark Network Analyzer



Wireshark Network Analyzer

Wireshark Display Window – captures traffic in three panes

SUMMARY
Displays one line summary for each captured packet:
1) time
2) source address
3) destination address
4) info about highest-layer protocol

DETAIL
Provides all the details for each of the layers contained inside the captured packet in a tree-like structure.

DATA
Displays the raw captured data both in hexadecimal and ASCII format.

Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------|----------------|----------|--------|-------------------|
| 213 | 3.001800000 | 192.168.1.100 | 192.168.1.100 | HTTP | 216 | GET /api/amzn.../ |
| 215 | 3.001800000 | 192.168.1.100 | 192.168.1.100 | HTTP | 133 | HTTP/1.1 200 OK |
| 216 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 453 | GET /images/001/ |
| 217 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 204 | GET /images/001/ |
| 218 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 219 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 220 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 221 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 222 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 223 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 224 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 225 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 226 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 227 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 228 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 229 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 230 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 231 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 232 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 233 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 234 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 235 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 236 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 237 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 238 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 239 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 240 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 241 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 242 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 243 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 244 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 245 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 246 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 247 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 248 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 249 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 250 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 251 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 252 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 253 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 254 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 255 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 256 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 257 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 258 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 259 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 260 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 261 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 262 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 263 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 264 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 265 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 266 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 267 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 268 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 269 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 270 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 271 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 272 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 273 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 274 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 275 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 276 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 277 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 278 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 279 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 280 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 281 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 282 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 283 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 284 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 285 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 286 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 287 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 288 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 289 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 290 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 291 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 292 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 293 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 294 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 295 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 296 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 297 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 298 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 299 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |
| 300 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | 440 | GET /images/001/ |

Frame 550 (550 bytes) on interface (en0) (10/100/1000 Mbps Ethernet) captured on (en0) (10/100/1000 Mbps Ethernet) at 2013-01-15 10:10:10.000000000. Contains: Hypertext Transfer Protocol [64417 bytes] Do: chunked entity body (9046 bytes)

Wireshark Network Analyzer

ipconfig –all – reveals own MAC & IP address, and IP address of DNS & DHCP server

```

C:\Documents and Settings\marku\My Documents>ipconfig /all

Windows IP Configuration

Host Name . . . . . : marku
Primary Dns Suffix . . . . . : cs.yorku.ca
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cs.yorku.ca
                                     cs.yorku.ca
                                     yorku.ca

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : cs.yorku.ca
Description . . . . . : Intel(R) PRO/1000 MT Network Connecti
ion
Physical Address. . . . . : 00-0D-56-1F-4F-2E
Dhcp Enabled. . . . . : Yes
Autonomous Configuration Enabled . . . . . : Yes
IP Address. . . . . : 130.63.86.182
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 130.63.86.1
DHCP Server . . . . . : 130.63.86.28
DNS Servers . . . . . : 130.63.86.33
                                     130.63.169.241
Primary WINS Server . . . . . : 130.63.86.28
Lease Obtained. . . . . : Tuesday, January 05, 2010 5:28:22 AM
Lease Expires . . . . . : Tuesday, January 05, 2010 5:28:22 PM
    
```

Wireshark Network Analyzer

Wireshark Display Filter Feature

mythark.pc@ Wireshark

Filter: http

| No. | Time | Source | Destination | Protocol | Info |
|-----|-------------|---------------|----------------|----------|-------------------|
| 213 | 3.001800000 | 192.168.1.100 | 192.168.1.100 | HTTP | GET /api/amzn.../ |
| 215 | 3.001800000 | 192.168.1.100 | 192.168.1.100 | HTTP | HTTP/1.1 200 OK |
| 216 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 217 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 218 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 219 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 220 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 221 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 222 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 223 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 224 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 225 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 226 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 227 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 228 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 229 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 230 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 231 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 232 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 233 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 234 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 235 | 4.000000000 | 192.168.1.100 | 205.137.88.177 | HTTP | GET /images/001/ |
| 236 | | | | | |

Wireshark Network Analyzer

Wireshark Statistics Summary Feature

The screenshot shows the 'Wireshark Protocol Hierarchy - Statistics' window. It displays a tree view of protocols on the left and a table of statistics on the right. The table has columns for Protocol, % Packets, Packets Bytes, Pkts/s, and End Bytes. The 'IP' protocol is highlighted as the most frequent.

| Protocol | % Packets | Packets Bytes | Pkts/s | End Bytes |
|-------------------------------|---------------|------------------|--------|-----------|
| IP | 100.00% | 1927 1931194 | 1.117 | 0 |
| ICMP | 0.05% | 6 627 6061 | 0 | 0 |
| SSH (SSH-2) | 0.27% | 4 246 6060 | 4 | 240 |
| SSH (SSH-1) | 0.07% | 1 305 6060 | 0 | 0 |
| SSH (SSH-0) | 0.07% | 1 305 6060 | 1 | 287 |
| Address Resolution Protocol | 0.05% | 10 626 6061 | 10 | 684 |
| Internet Protocol | 0.02% (0.02%) | 150 106112 1.117 | 0 | 0 |
| User Datagram Protocol | 1.86% | 28 5818 6066 | 0 | 0 |
| Domain Name Service | 1.29% | 26 1625 6065 | 26 | 1625 |
| MIME (MIME) | 0.13% | 2 436 6068 | 0 | 0 |
| SMTP (SMTP) | 0.13% | 2 436 6068 | 0 | 0 |
| Internet Protocol | 0.13% | 2 436 6068 | 0 | 0 |
| Transmission Control Protocol | 0.72% | 142 102806 1.112 | 126 | 66120 |
| Hypertext Transfer Protocol | 16.32% | 246 14081 1.161 | 131 | 6314 |
| Line-based text data | 2.46% | 37 25627 6069 | 37 | 25627 |
| JPEG (JPEG) | 2.02% | 36 28094 6078 | 26 | 28095 |
| Compressed data | 2.19% | 33 19794 6022 | 33 | 19794 |
| Portable Network Graphics | 0.26% | 7 4911 6062 | 7 | 4911 |
| HTTP | 0.20% | 3 2098 6062 | 3 | 2098 |

13

Wireshark Network Analyzer

Wireshark Display Filter Feature

The screenshot shows the Wireshark interface with the 'Filter' field in the packet list pane. The filter expression is 'ip.addr == 192.168.1.102'. The packet list pane shows several packets, with the first one selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

Wireshark Installation

- www.wireshark.org

The screenshot shows the Wireshark website homepage. The main navigation bar includes 'Download Wireshark', 'Learn Wireshark', and 'Enhance Wireshark'. Below this, there are sections for 'News and Events', 'Wireshark Blog', and 'Enhance Wireshark'. The 'Wireshark Blog' section features an article titled 'Troubleshooting the hidden dangers of TCP's Nagle algorithm and delayed acknowledgement'.

15