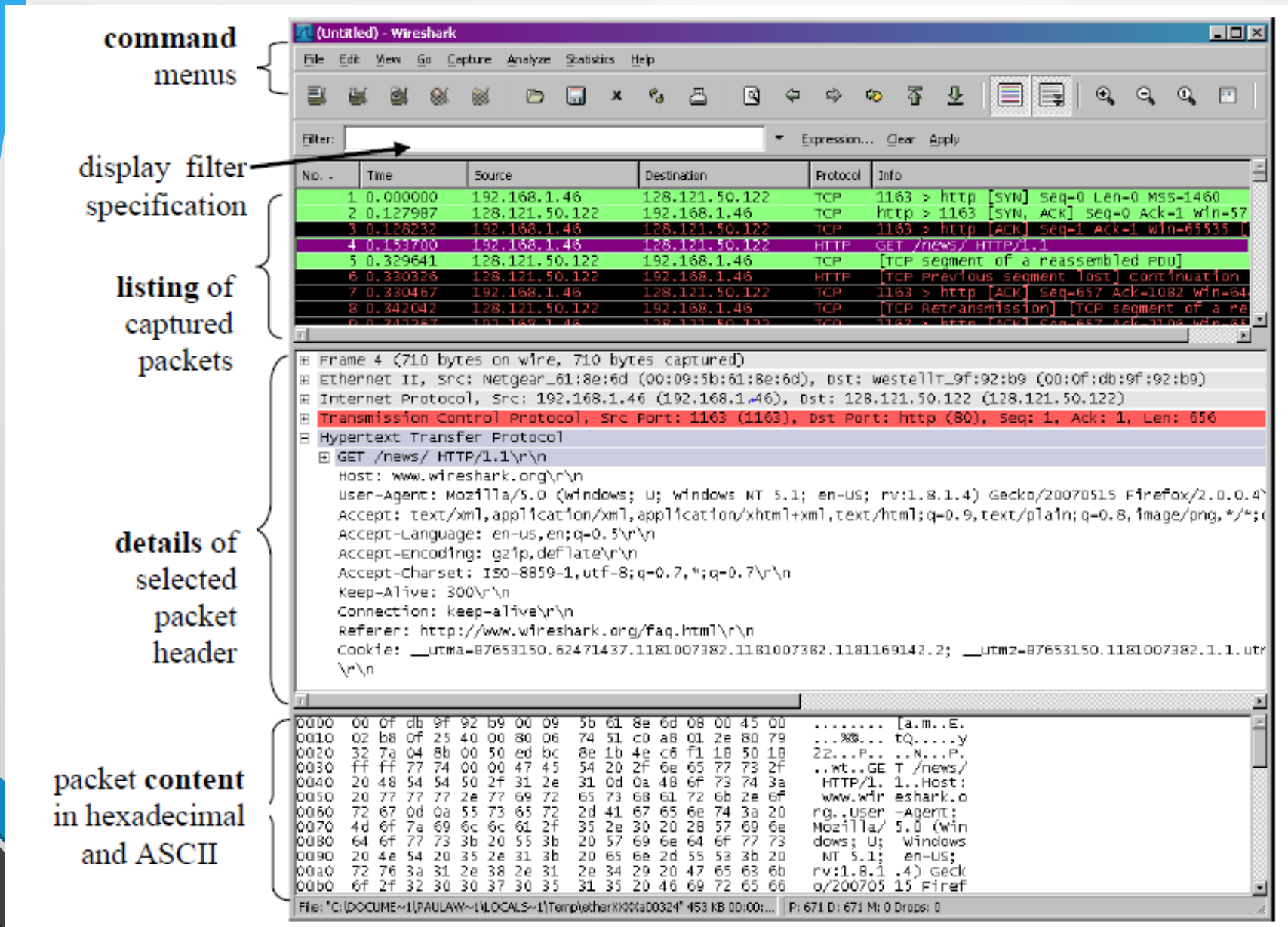
# Intrusion & Anomaly Detection

## Analysis Tools

Lisa Frye, Instructor
frye@kutztown.edu
Kutztown University

# Wireshark


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.1.46 128.121.50.122 TCP 1163 > http [SYN] Seq=0 Len=0 MSS=1460
2 0.127987 128.121.50.122 192.168.1.46 TCP http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
3 0.128232 192.168.1.46 128.121.50.122 TCP 1163 > http [ACK] Seq=1 Ack=1 Win=65535
4 0.153700 192.168.1.46 128.121.50.122 HTTP GET /news/ HTTP/1.1
5 0.329641 128.121.50.122 192.168.1.46 TCP [TCP segment of a reassembled PDU]
6 0.330326 128.121.50.122 192.168.1.46 HTTP [TCP Previous segment lost] Continuation
7 0.330467 192.168.1.46 128.121.50.122 TCP 1163 > http [ACK] Seq=657 Ack=1082 Win=64
8 0.342042 128.121.50.122 192.168.1.46 TCP [TCP Retransmission] [TCP segment of a re
Frame 4 (710 bytes on wire, 710 bytes captured)
Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: westellt_9f:92:b9 (00:0f:db:9f:92:b9)
Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
Hypertext Transfer Protocol
GET /news/ HTTP/1.1\r\n
Host: www.wireshark.org\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
Referer: http://www.wireshark.org/faq.html\r\n
Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
\r\n
0000 00 0f db 9f 92 b9 00 09 5b 61 8e 6d 08 00 45 00 ........ [a.m..E.
0010 02 b8 0f 25 40 00 80 06 74 51 c0 a8 01 2e 80 79 ...%@... tQ.....y
0020 32 7a 04 8b 00 50 ed bc 8e 1b 4e c6 f1 18 50 18 2z...P.. ..N...P.
0030 ff ff 77 74 00 00 47 45 54 20 2f 6e 65 77 73 2f ..wt..GE T /news/
0040 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1..Host:
0050 20 77 77 77 2e 77 69 72 65 73 68 61 72 6b 2e 6f www.wir eshark.o
0060 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 rg..User -Agent:
0070 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win
0080 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77 73 dows; U; Windows
0090 20 4e 54 20 35 2e 31 3b 20 65 6e 2d 55 53 3b 20 NT 5.1; en-US;
00a0 72 76 3a 31 2e 38 2e 31 2e 34 29 20 47 65 63 6b rv:1.8.1 .4) Geck
00b0 6f 2f 32 30 30 37 30 35 31 35 20 46 69 72 65 66 o/200705 15 Firef
File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherX%%a00324" 453 KB 00:00:...
P: 671 D: 671 M: 0 Drops: 0

# Wireshark Useful Options

- Edit / Mark packet
- Ignore packets – remove packets from view
- Display filters – filter packets displayed
- Capture filters – filter what is captured
- Statistics
- Conversations and endpoints list
- Flow graphs

# Wireshark Display Filters

- Types
  - Inclusion filtering
  - Exclusion filtering
- Format
- Default set
- Create based on various properties

# Display Filter Examples

- All tcp traffic
- All http traffic
- Packets containing one of TCP analysis flags
- Packets with invalid IP header checksum
- HTTP GET request method
- TCP window size < 1460
- ICMP type 8
- TCP packets with ACK flag set but not SYN flag
- DNS/port 53 or HTTP traffic/port 80, from 192.168.0.105

# Wireshark Capture Filters

- Display or capture filters?
- Filter fields
  - Identifiier
  - Qualifiers
    - Type
    - Dir (direction)
    - Proto (protocol)

# Capture Filter Examples

- Traffic to 192.168.1.23
- Traffic to MAC 08:3f:3d:01:bc:18
- Traffic to or from KU network
- DNS traffic

# Wireshark Packet Colorization

- Highlight packets
- Predefined coloring rules
- Processed in order

# Wireshark Statistics

- Protocols
- Conversations
- Endpoints
- Traffic types
- Packets
- IP address
- Ports
- Etc.

# Wireshark Streams

- Follow communications streams
  - Reassemble communications
  - Conversation is colored
  - Right-click menu
- Can
  - Reassemble files
  - Re-create video streams

# Wireshark Miscellaneous

- Expert Information
- Graphs

# tcpdump

- Packet capture tool
- Backend to IDSs
- Stand alone

# tcpdump Example Output

- 17:13:09.088211 8:0:20:a8:73:54 0:4:dc:9e:1e:36 0800 102: 156.12.127.14.22 > 156.12.1.222.62425: P 3170556641:3170556689(48) ack 1792071674 win 49640 (DF)
- 17:13:09.088487 8:0:20:a8:73:54 0:4:dc:9e:1e:36 0800 137: 156.12.127.14.35760 > 156.12.1.142.514:  udp 95 (DF)
- 17:13:09.088624 8:0:20:a8:73:54 0:4:dc:9e:1e:36 0800 118: 156.12.127.14.22 > 156.12.1.222.62425: P 3170556689:3170556753(64) ack 1792071674 win 49640 (DF)
- 17:13:09.089130 8:0:20:a8:73:54 0:4:dc:9e:1e:36 0800 102: 156.12.127.14.22 > 156.12.1.222.62425: P 3170556753:3170556801(48) ack 1792071674 win 49640 (DF)
- 17:13:15.488598 0:4:dc:9e:1e:36 8:0:20:a8:73:54 0800 62: 156.12.3.30.2427 > 156.12.127.14.80: S 234874733l:234874733l(0) win 16384 <mss 1370,nop,nop,sackOK> (DF)

# tcpdump Output with HEX

- 17:13:09.088211 8:0:20:a8:73:54 0:4:dc:9e:1e:36 0800 102: 156.12.127.14.22 > 156.12.1.222.62425: P 3170556641:3170556689(48) ack 1792071674 win 49640 (DF)

  4500 0058 3d37 4000 3c06 4864 9c0c 7f0e

  9c0c 01de 0016 f3d9 bcfa dae1 6ad0 d7fa

  5018 c1e8 cfcd 0000 7df1 6ff9 29c2 8e75

  adf6 1467 6f70

- 17:13:09.088487 8:0:20:a8:73:54 0:4:dc:9e:1e:36 0800 137: 156.12.127.14.35760 > 156.12.1.142.514: udp 95 (DF)

  4500 007b b05e 4000 ff11 125e 9c0c 7f0e

  9c0c 018e 8bb0 0202 0067 01d4 3c35 353e

  4d61 7220 2032 2031 373a 3133 3a31 3620

  7072 696e 7464