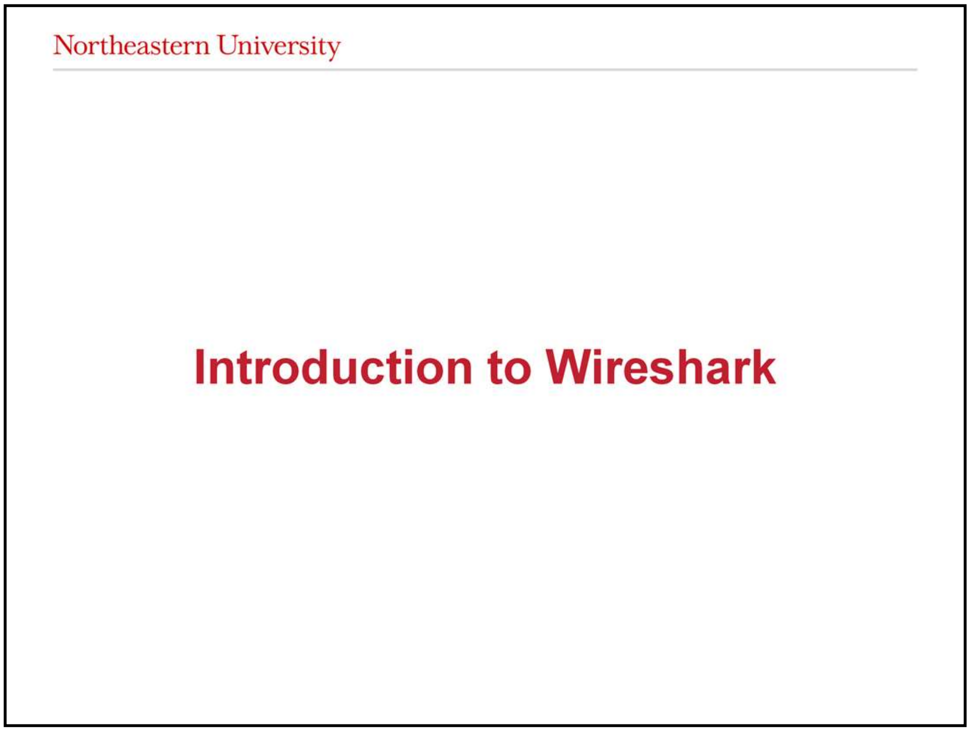
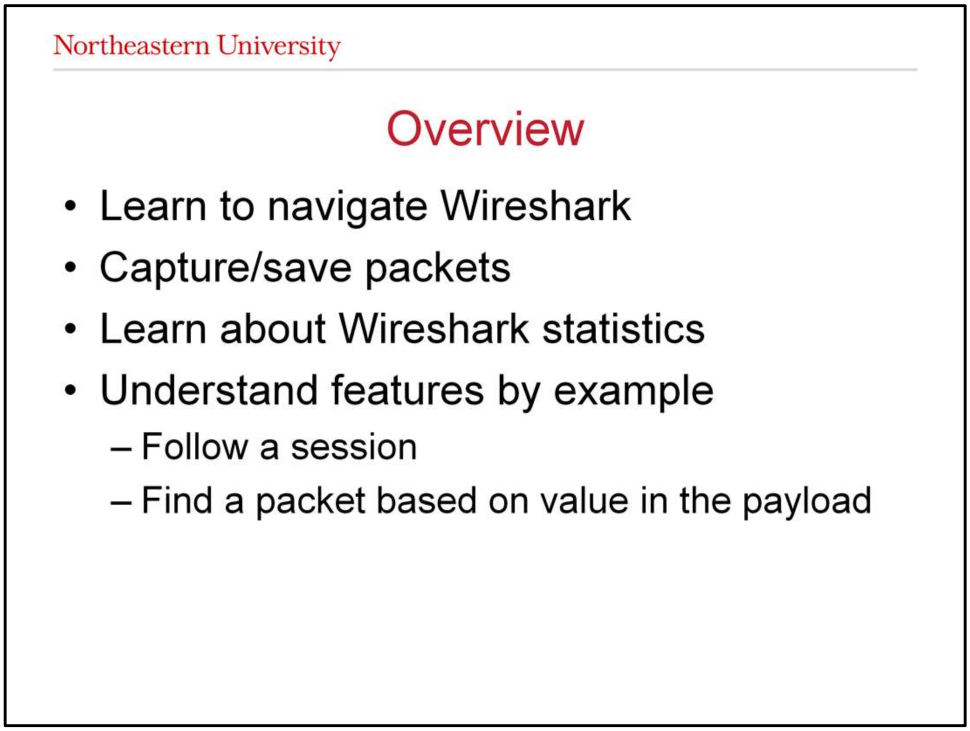
Northeastern



Northeastern University

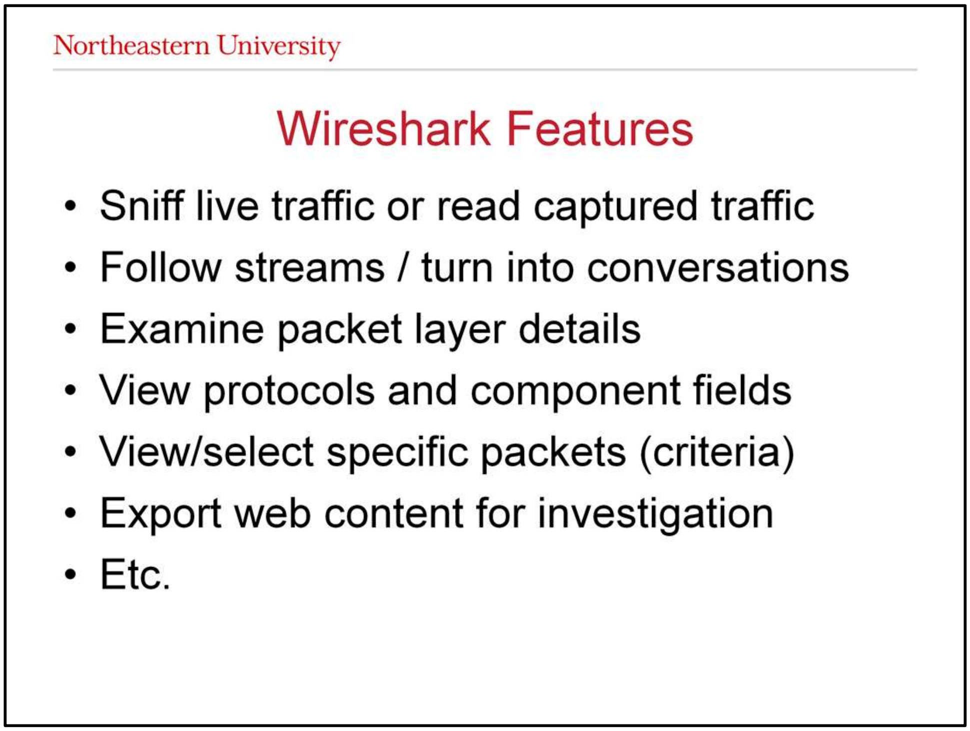
# Introduction to Wireshark

This slide intentionally left blank.



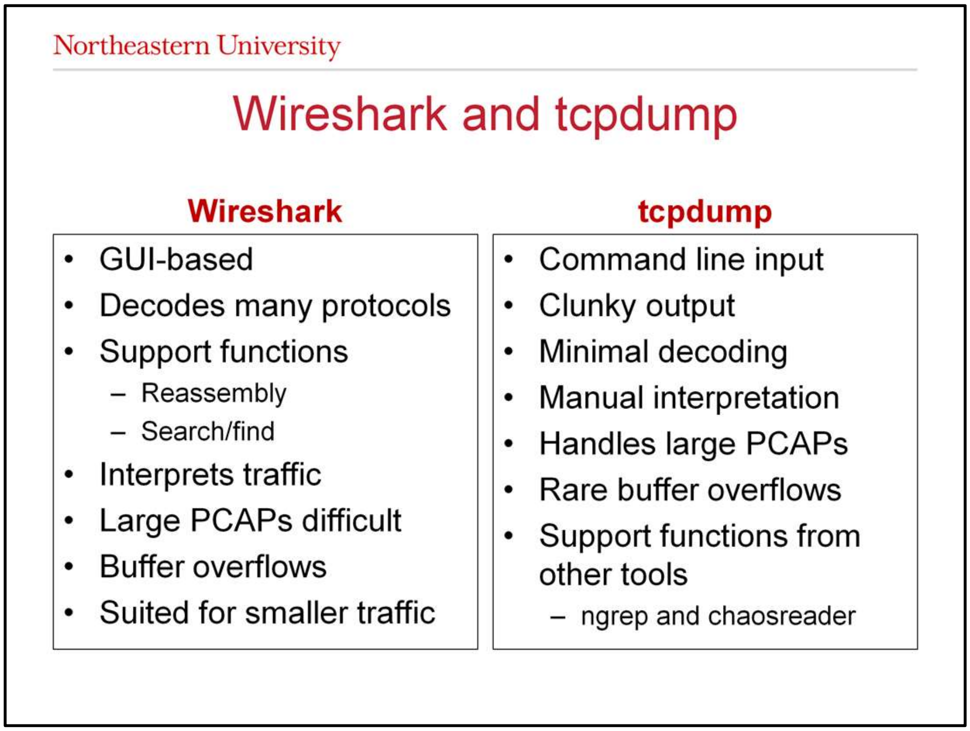
# Overview

- Learn to navigate Wireshark
- Capture/save packets
- Learn about Wireshark statistics
- Understand features by example
  - – Follow a session
  - – Find a packet based on value in the payload



## Wireshark Features

- Sniff live traffic or read captured traffic
- Follow streams / turn into conversations
- Examine packet layer details
- View protocols and component fields
- View/select specific packets (criteria)
- Export web content for investigation
- Etc.



Northeastern University

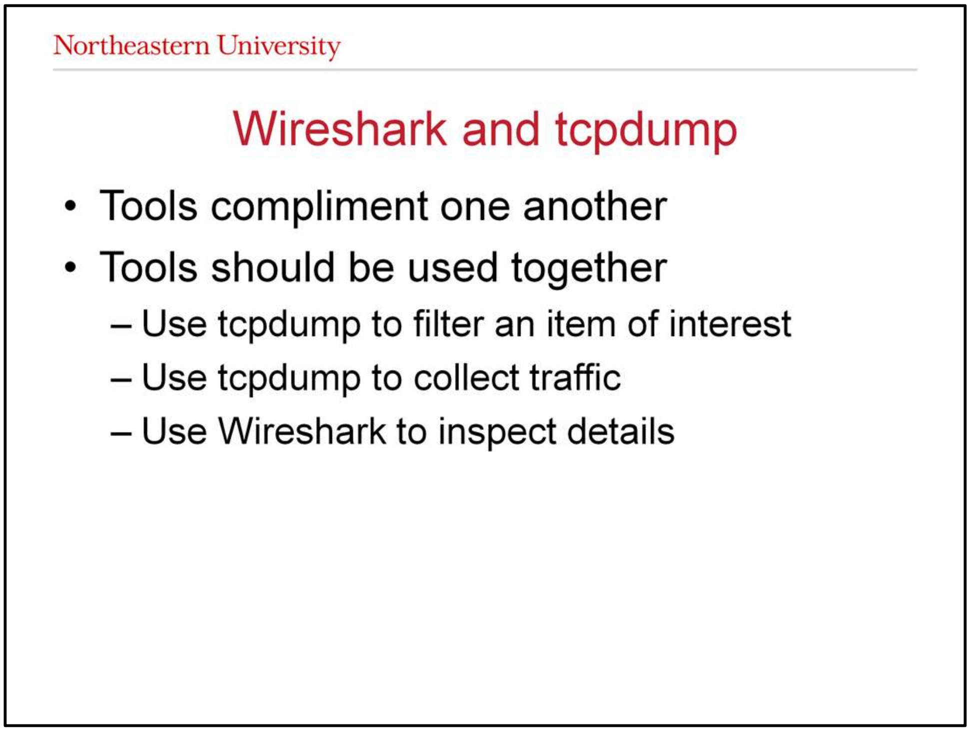
# Wireshark and tcpdump

**Wireshark**

- GUI-based
- Decodes many protocols
- Support functions
  - Reassembly
  - Search/find
- Interprets traffic
- Large PCAPs difficult
- Buffer overflows
- Suited for smaller traffic

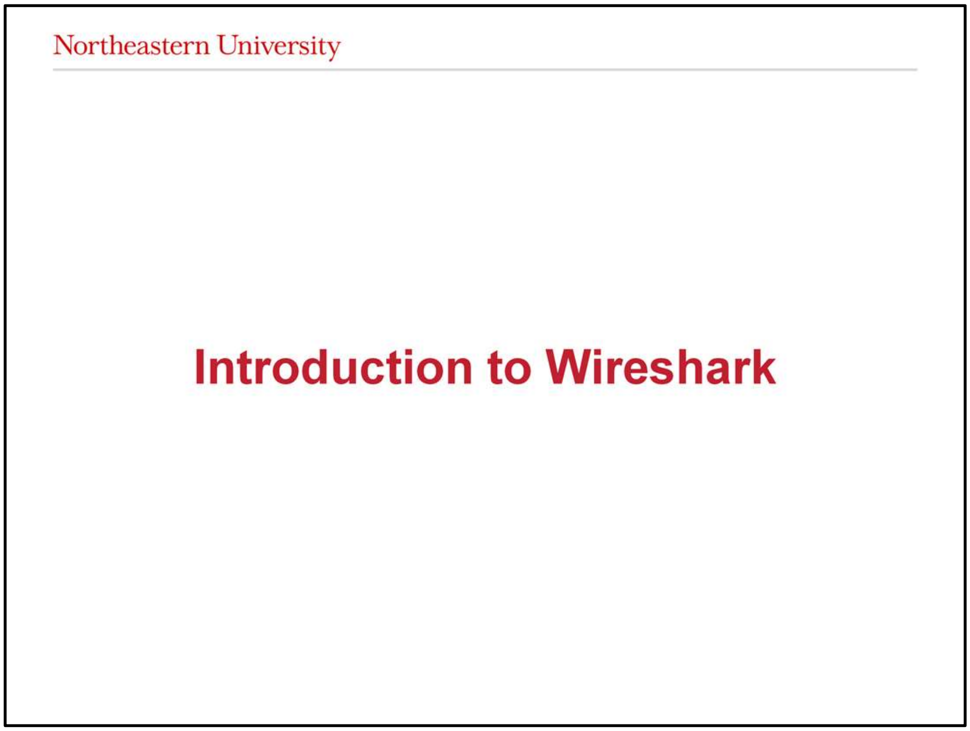
**tcpdump**

- Command line input
- Clunky output
- Minimal decoding
- Manual interpretation
- Handles large PCAPs
- Rare buffer overflows
- Support functions from other tools
  - ngrep and chaosreader

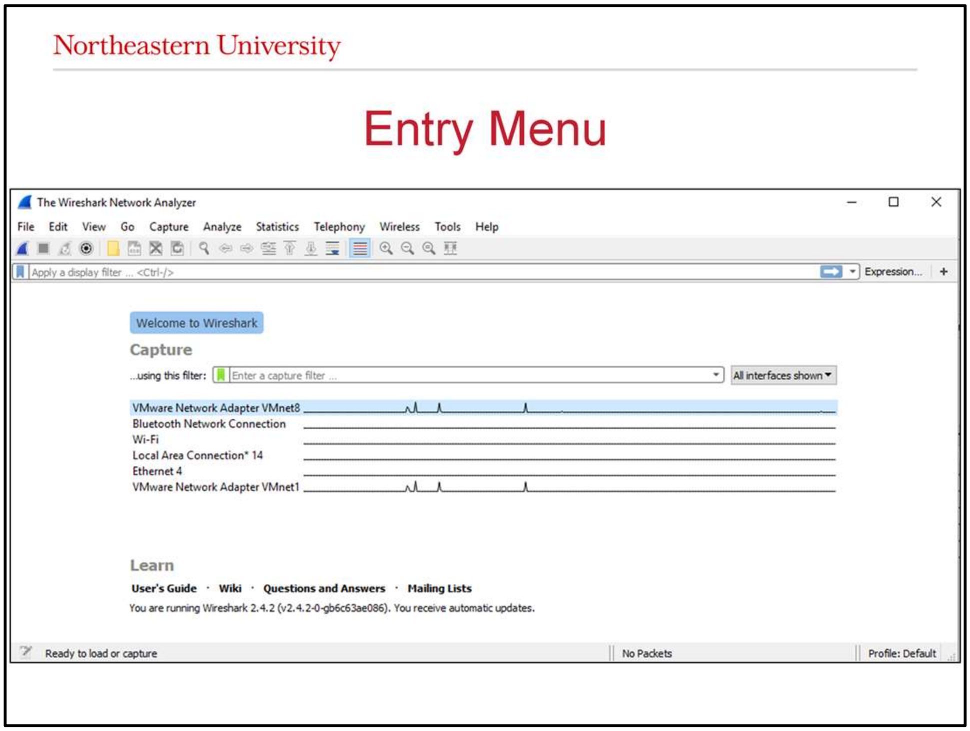


## Wireshark and tcpdump

- Tools compliment one another
- Tools should be used together
  - Use tcpdump to filter an item of interest
  - Use tcpdump to collect traffic
  - Use Wireshark to inspect details



# Introduction to Wireshark



Northeastern University

## Entry Menu

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

VMware Network Adapter VMnet8
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 14
Ethernet 4
VMware Network Adapter VMnet1

Learn

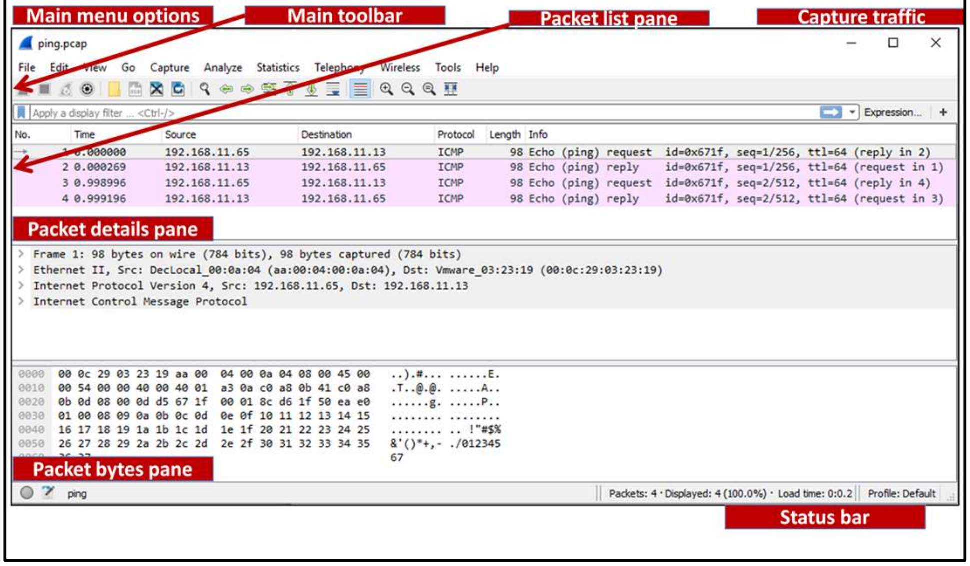
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.2 (v2.4.2-0-gb6c63ae086). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

The entry menu in Wireshark allows you to select options to configure capture interfaces, capture packets, or access the user's guide. If you have an Internet connection, there are additional online options that include accessing their website and downloading sample captures. There will also be a link to recently used packet captures. Some options will only be present and optional when a PCAP is loaded; otherwise the options may be grayed out.

# Main Menu



Main menu options

Main toolbar

Packet list pane

Capture traffic

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.11.65 | 192.168.11.13 | ICMP | 98 | Echo (ping) request  id=0x671f, seq=1/256, ttl=64 (reply in 2) |
| 2 | 0.000269 | 192.168.11.13 | 192.168.11.65 | ICMP | 98 | Echo (ping) reply    id=0x671f, seq=1/256, ttl=64 (request in 1) |
| 3 | 0.998996 | 192.168.11.65 | 192.168.11.13 | ICMP | 98 | Echo (ping) request  id=0x671f, seq=2/512, ttl=64 (reply in 4) |
| 4 | 0.999196 | 192.168.11.13 | 192.168.11.65 | ICMP | 98 | Echo (ping) reply    id=0x671f, seq=2/512, ttl=64 (request in 3) |

Packet details pane

```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: DecLocal_00:0a:04 (aa:00:04:00:0a:04), Dst: Vmware_03:23:19 (00:0c:29:03:23:19)
> Internet Protocol Version 4, Src: 192.168.11.65, Dst: 192.168.11.13
> Internet Control Message Protocol
```

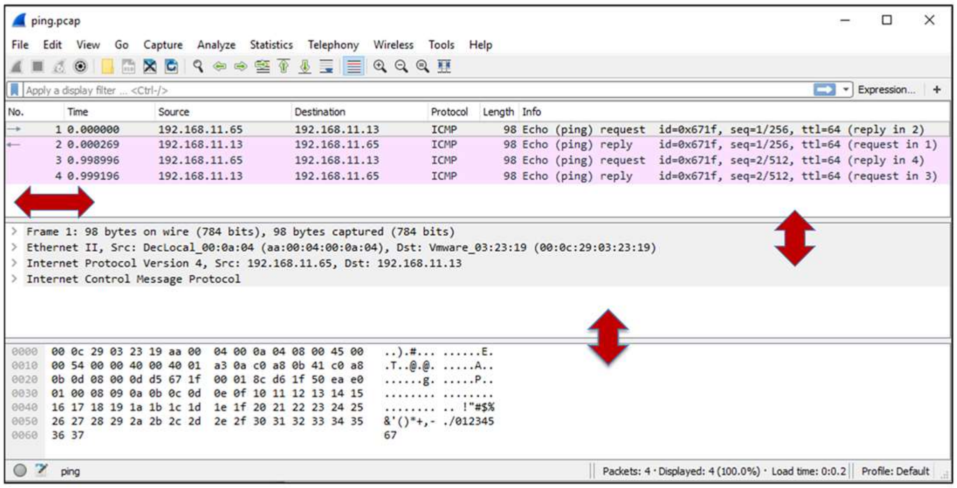
```
0000  00 0c 29 03 23 19 aa 00  04 00 0a 04 08 00 45 00   ..).#... ......E.
0010  00 54 00 00 40 00 40 01  a3 0a c0 a8 0b 41 c0 a8   .T..@.@. .....A..
0020  0b 0d 08 00 0d d5 67 1f  00 01 8c d6 1f 50 ea e0   ......g. .....P..
0030  01 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Packet bytes pane

```
ping                    Packets: 4 · Displayed: 4 (100.0%) · Load time: 0:0.2    Profile: Default
```

Status bar

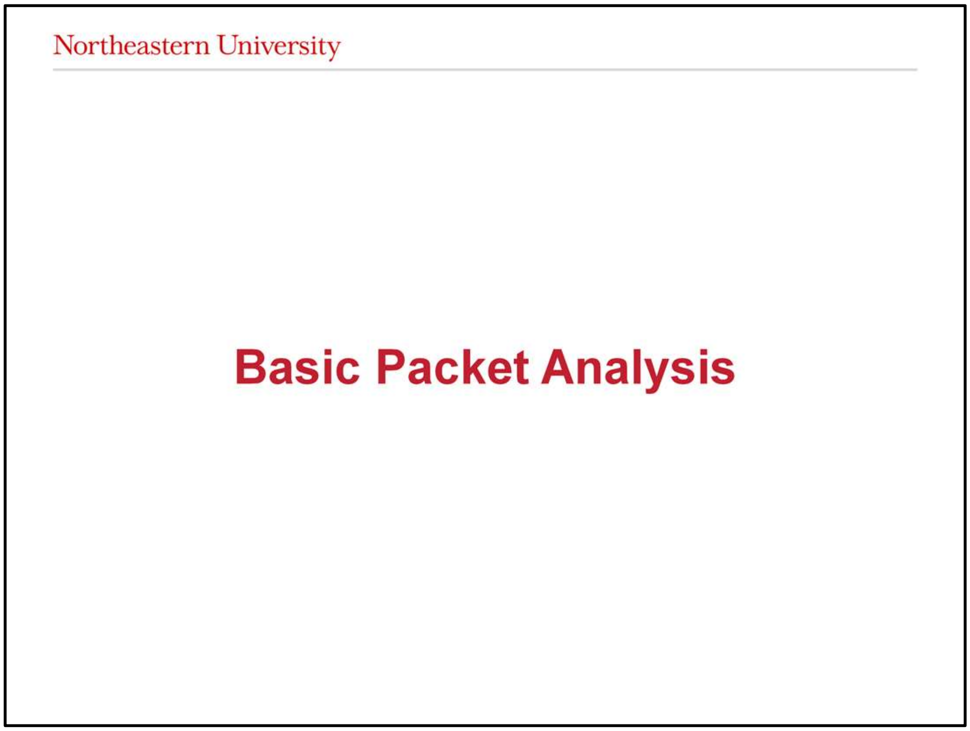
# Collapsing and Expanding Panes



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.11.65 | 192.168.11.13 | ICMP | 98 | Echo (ping) request id=0x671f, seq=1/256, ttl=64 (reply in 2) |
| 2 | 0.000269 | 192.168.11.13 | 192.168.11.65 | ICMP | 98 | Echo (ping) reply id=0x671f, seq=1/256, ttl=64 (request in 1) |
| 3 | 0.998996 | 192.168.11.65 | 192.168.11.13 | ICMP | 98 | Echo (ping) request id=0x671f, seq=2/512, ttl=64 (reply in 4) |
| 4 | 0.999196 | 192.168.11.13 | 192.168.11.65 | ICMP | 98 | Echo (ping) reply id=0x671f, seq=2/512, ttl=64 (request in 3) |

```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: DecLocal_00:0a:04 (aa:00:04:00:0a:04), Dst: Vmware_03:23:19 (00:0c:29:03:23:19)
> Internet Protocol Version 4, Src: 192.168.11.65, Dst: 192.168.11.13
> Internet Control Message Protocol
```

```
0000  00 0c 29 03 23 19 aa 00  04 00 0a 04 08 00 45 00   ..).#... ......E.
0010  00 54 00 00 40 00 40 01  a3 0a c0 a8 0b 41 c0 a8   .T..@.@. .....A..
0020  0b 0d 08 00 0d d5 67 1f  00 01 8c d6 1f 50 ea e0   ......g. .....P..
0030  01 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

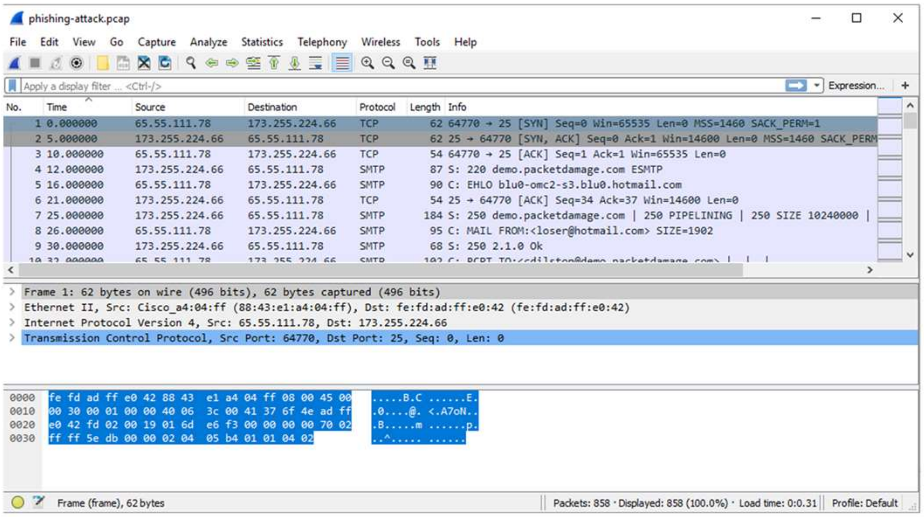


Northeastern University

## Basic Packet Analysis

Northeastern University

## Analysis of PCAP File

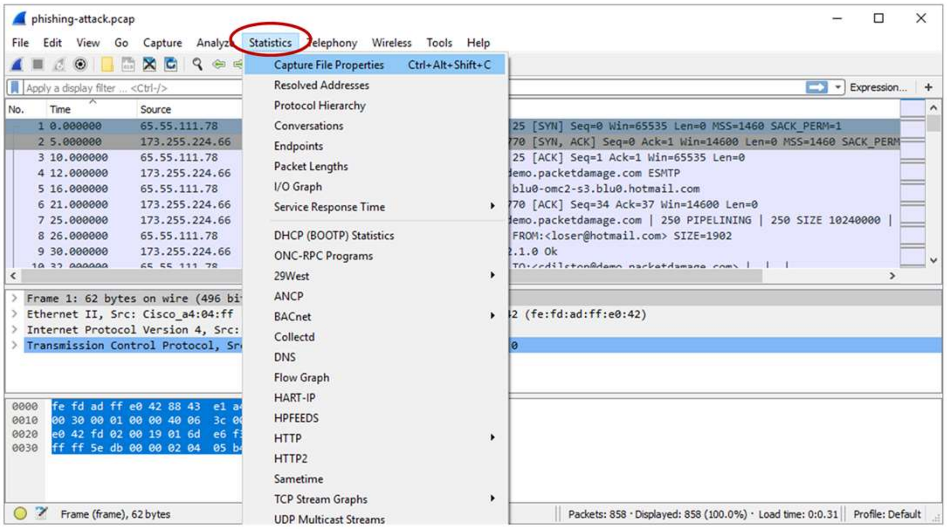

phishing-attack.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time         Source          Destination     Protocol  Length  Info
   1 0.000000     65.55.111.78    173.255.224.66  TCP       62 64770 → 25 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
   2 5.000000     173.255.224.66  65.55.111.78    TCP       62 25 → 64770 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM
   3 10.000000    65.55.111.78    173.255.224.66  TCP       54 64770 → 25 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   4 12.000000    173.255.224.66  65.55.111.78    SMTP      87 S: 220 demo.packetdamage.com ESMTP
   5 16.000000    65.55.111.78    173.255.224.66  SMTP      90 C: EHLO blu0-omc2-s3.blu0.hotmail.com
   6 21.000000    173.255.224.66  65.55.111.78    TCP       54 25 → 64770 [ACK] Seq=34 Ack=37 Win=14600 Len=0
   7 25.000000    173.255.224.66  65.55.111.78    SMTP     184 S: 250 demo.packetdamage.com | 250 PIPELINING | 250 SIZE 10240000 |
   8 26.000000    65.55.111.78    173.255.224.66  SMTP      95 C: MAIL FROM:<loser@hotmail.com> SIZE=1902
   9 30.000000    173.255.224.66  65.55.111.78    SMTP      68 S: 250 2.1.0 Ok
  10 32.000000    65.55.111.78    173.255.224.66  SMTP     102 C: RCPT TO:<cdilston@demo.packetdamage.com> | | |

> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: Cisco_a4:04:ff (88:43:e1:a4:04:ff), Dst: fe:fd:ad:ff:e0:42 (fe:fd:ad:ff:e0:42)
> Internet Protocol Version 4, Src: 65.55.111.78, Dst: 173.255.224.66
> Transmission Control Protocol, Src Port: 64770, Dst Port: 25, Seq: 0, Len: 0

0000  fe fd ad ff e0 42 88 43  e1 a4 04 ff 08 00 45 00   .....B.C ......E.
0010  00 30 00 01 00 00 40 06  3c 00 41 37 6f 4e ad ff   .0....@. <.A7oN..
0020  e0 42 fd 02 00 19 01 6d  e6 f3 00 00 00 00 70 02   .B.....m ......p.
0030  ff ff 5e db 00 00 02 04  05 b4 01 01 04 02         ..^..... ......

Frame (frame), 62 bytes    Packets: 858 · Displayed: 858 (100.0%) · Load time: 0:0.31    Profile: Default
```

Let’s walk through the basic review of a PCAP containing a potential phishing attack. An IPS or NetWitness packet capture alert identifies an HTTP session indicating a user visited a link in a phishing email that directed a user to download some malicious code. The alert is for the string “filename=pdf641.” This demo shows students how to review a packet capture and draw general traffic statistics from a packet capture file. This is the initial first step for any .pcap file an analyst is given and should be part of the initial report.

Northeastern University

# Statistics



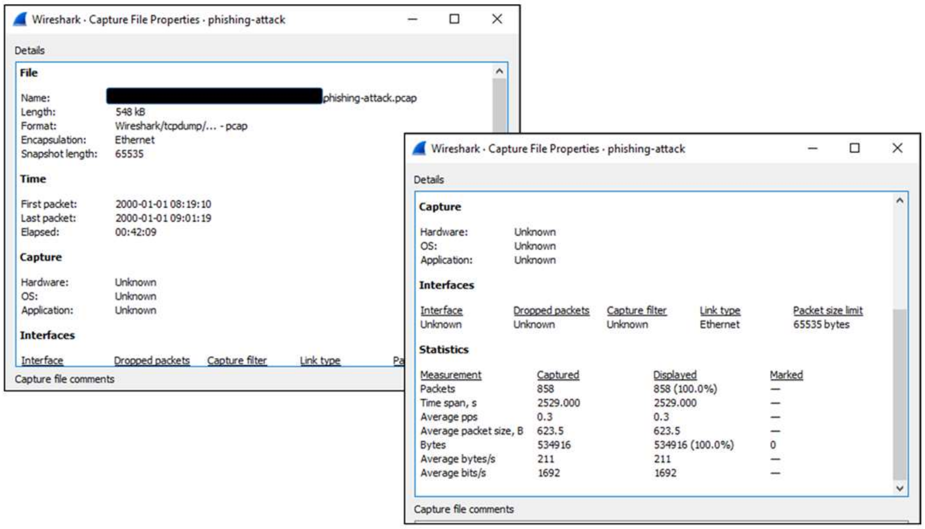
```
 1 0.000000    65.55.111.78      25 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
 2 5.000000    173.255.224.66    770 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM
 3 10.000000   65.55.111.78      25 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 4 12.000000   173.255.224.66    demo.packetdamage.com ESMTP
 5 16.000000   65.55.111.78      blu0-omc2-s3.blu0.hotmail.com
 6 21.000000   173.255.224.66    770 [ACK] Seq=34 Ack=37 Win=14600 Len=0
 7 25.000000   173.255.224.66    demo.packetdamage.com | 250 PIPELINING | 250 SIZE 10240000 |
 8 26.000000   65.55.111.78      FROM:<loser@hotmail.com> SIZE=1902
 9 30.000000   173.255.224.66    2.1.0 Ok

> Frame 1: 62 bytes on wire (496 bi
> Ethernet II, Src: Cisco_a4:04:ff        42 (fe:fd:ad:ff:e0:42)
> Internet Protocol Version 4, Src:
> Transmission Control Protocol, Sr       0

0000  fe fd ad ff e0 42 88 43  e1 a4
0010  00 30 00 01 00 00 40 06  3c 00
0020  e0 42 fd 02 00 19 01 6d  e6 f1
0030  ff ff 5e db 00 00 02 04  05 b4
```

Frame (frame), 62 bytes

Packets: 858 · Displayed: 858 (100.0%) · Load time: 0:0.31 | Profile: Default

There are many overview options to give a summary of the composition of a particular packet capture. We know there may be some HTTP and SMTP traffic, but that’s all we know so far with the information given. These summary statistics provide a decent starting point to understand the traffic contents.

# Property Statistics



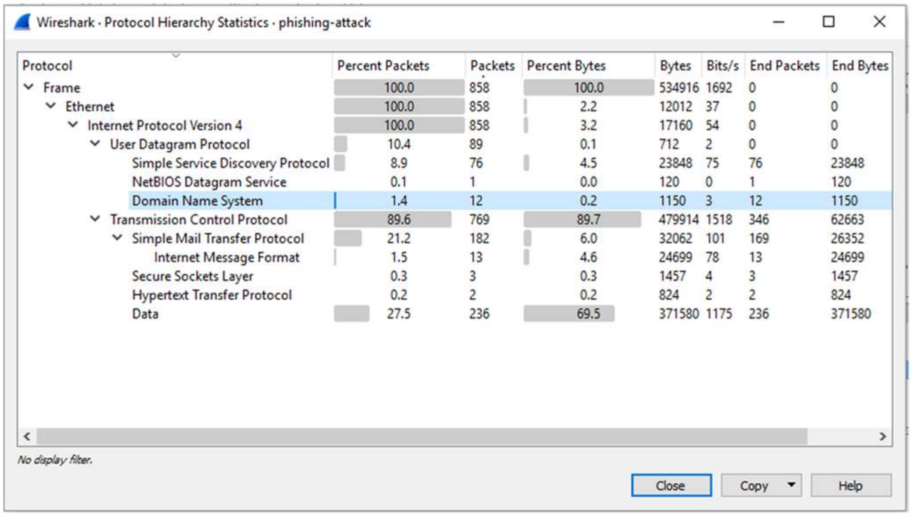
Wireshark · Capture File Properties · phishing-attack

```
Details

File

Name:              [redacted]phishing-attack.pcap
Length:            548 kB
Format:            Wireshark/tcpdump/... - pcap
Encapsulation:     Ethernet
Snapshot length:   65535

Time

First packet:      2000-01-01 08:19:10
Last packet:       2000-01-01 09:01:19
Elapsed:           00:42:09

Capture

Hardware:          Unknown
OS:                Unknown
Application:       Unknown

Interfaces

Interface          Dropped packets    Capture filter    Link type        Pa

Capture file comments
```

Wireshark · Capture File Properties · phishing-attack

```
Details

Capture

Hardware:          Unknown
OS:                Unknown
Application:       Unknown

Interfaces

Interface          Dropped packets    Capture filter    Link type        Packet size limit
Unknown            Unknown            Unknown           Ethernet         65535 bytes

Statistics

Measurement               Captured       Displayed          Marked
Packets                   858            858 (100.0%)       —
Time span, s              2529.000       2529.000           —
Average pps               0.3            0.3                —
Average packet size, B    623.5          623.5              —
Bytes                     534916         534916 (100.0%)    0
Average bytes/s           211            211                —
Average bits/s            1692           1692               —

Capture file comments
```

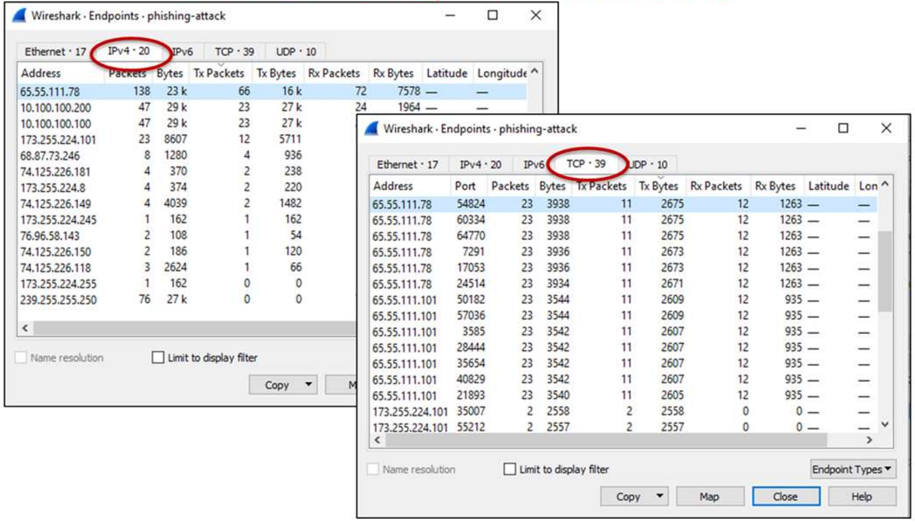
# Protocol Hierarchy Statistics



| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes |
|---|---|---|---|---|---|---|---|
| Frame | 100.0 | 858 | 100.0 | 534916 | 1692 | 0 | 0 |
| Ethernet | 100.0 | 858 | 2.2 | 12012 | 37 | 0 | 0 |
| Internet Protocol Version 4 | 100.0 | 858 | 3.2 | 17160 | 54 | 0 | 0 |
| User Datagram Protocol | 10.4 | 89 | 0.1 | 712 | 2 | 0 | 0 |
| Simple Service Discovery Protocol | 8.9 | 76 | 4.5 | 23848 | 75 | 76 | 23848 |
| NetBIOS Datagram Service | 0.1 | 1 | 0.0 | 120 | 0 | 1 | 120 |
| Domain Name System | 1.4 | 12 | 0.2 | 1150 | 3 | 12 | 1150 |
| Transmission Control Protocol | 89.6 | 769 | 89.7 | 479914 | 1518 | 346 | 62663 |
| Simple Mail Transfer Protocol | 21.2 | 182 | 6.0 | 32062 | 101 | 169 | 26352 |
| Internet Message Format | 1.5 | 13 | 4.6 | 24699 | 78 | 13 | 24699 |
| Secure Sockets Layer | 0.3 | 3 | 0.3 | 1457 | 4 | 3 | 1457 |
| Hypertext Transfer Protocol | 0.2 | 2 | 0.2 | 824 | 2 | 2 | 824 |
| Data | 27.5 | 236 | 69.5 | 371580 | 1175 | 236 | 371580 |

*No display filter.*

# IP/TCP Endpoint Statistics

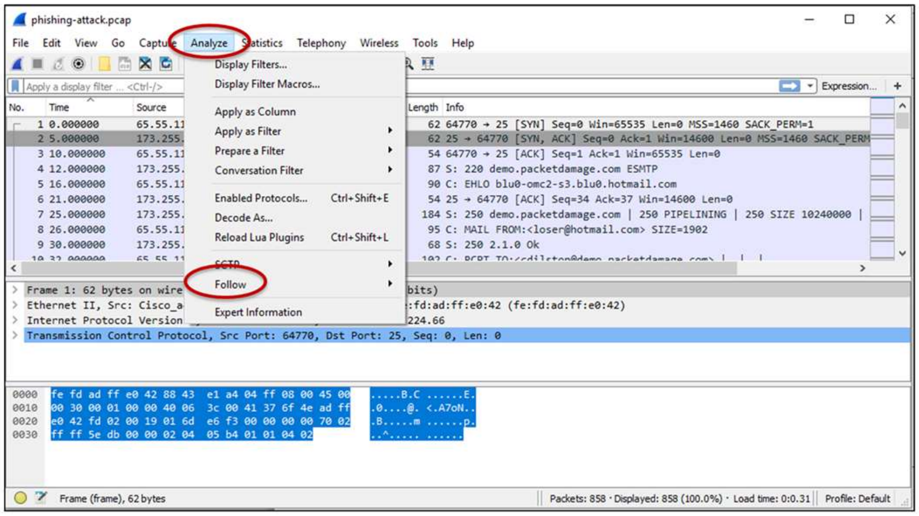


Wireshark · Endpoints · phishing-attack
Ethernet · 17
IPv4 · 20
IPv6
TCP · 39
UDP · 10
□ Name resolution
□ Limit to display filter
Copy
M

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Latitude | Longitude |
|---|---|---|---|---|---|---|---|---|
| 65.55.111.78 | 138 | 23 k | 66 | 16 k | 72 | 7578 | — | — |
| 10.100.100.200 | 47 | 29 k | 23 | 27 k | 24 | 1964 | — | — |
| 10.100.100.100 | 47 | 29 k | 23 | 27 k | | | | |
| 173.255.224.101 | 23 | 8607 | 12 | 5711 | | | | |
| 68.87.73.246 | 8 | 1280 | 4 | 936 | | | | |
| 74.125.226.181 | 4 | 370 | 2 | 238 | | | | |
| 173.255.224.8 | 4 | 374 | 2 | 220 | | | | |
| 74.125.226.149 | 4 | 4039 | 2 | 1482 | | | | |
| 173.255.224.245 | 1 | 162 | 1 | 162 | | | | |
| 76.96.58.143 | 2 | 108 | 1 | 54 | | | | |
| 74.125.226.150 | 2 | 186 | 1 | 120 | | | | |
| 74.125.226.118 | 3 | 2624 | 1 | 66 | | | | |
| 173.255.224.255 | 1 | 162 | 0 | 0 | | | | |
| 239.255.255.250 | 76 | 27 k | 0 | 0 | | | | |

| Address | Port | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Latitude | Lon |
|---|---|---|---|---|---|---|---|---|---|
| 65.55.111.78 | 54824 | 23 | 3938 | 11 | 2675 | 12 | 1263 | — | — |
| 65.55.111.78 | 60334 | 23 | 3938 | 11 | 2675 | 12 | 1263 | — | — |
| 65.55.111.78 | 64770 | 23 | 3938 | 11 | 2675 | 12 | 1263 | — | — |
| 65.55.111.78 | 7291 | 23 | 3936 | 11 | 2673 | 12 | 1263 | — | — |
| 65.55.111.78 | 17053 | 23 | 3936 | 11 | 2673 | 12 | 1263 | — | — |
| 65.55.111.78 | 24514 | 23 | 3934 | 11 | 2671 | 12 | 1263 | — | — |
| 65.55.111.101 | 50182 | 23 | 3544 | 11 | 2609 | 12 | 935 | — | — |
| 65.55.111.101 | 57036 | 23 | 3544 | 11 | 2609 | 12 | 935 | — | — |
| 65.55.111.101 | 3585 | 23 | 3542 | 11 | 2607 | 12 | 935 | — | — |
| 65.55.111.101 | 28444 | 23 | 3542 | 11 | 2607 | 12 | 935 | — | — |
| 65.55.111.101 | 35654 | 23 | 3542 | 11 | 2607 | 12 | 935 | — | — |
| 65.55.111.101 | 40829 | 23 | 3542 | 11 | 2607 | 12 | 935 | — | — |
| 65.55.111.101 | 21893 | 23 | 3540 | 11 | 2605 | 12 | 935 | — | — |
| 173.255.224.101 | 35007 | 2 | 2558 | 2 | 2558 | 0 | 0 | — | — |
| 173.255.224.101 | 55212 | 2 | 2557 | 2 | 2557 | 0 | 0 | — | — |

# Analyze a TCP Session



```
No.  Time          Source       Length Info
   1 0.000000      65.55.11         62 64770 → 25 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
   2 5.000000      173.255.         62 25 → 64770 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM
   3 10.000000     65.55.11         54 64770 → 25 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   4 12.000000     173.255.         87 S: 220 demo.packetdamage.com ESMTP
   5 16.000000     65.55.11         90 C: EHLO blu0-omc2-s3.blu0.hotmail.com
   6 21.000000     173.255.         54 25 → 64770 [ACK] Seq=34 Ack=37 Win=14600 Len=0
   7 25.000000     173.255.        184 S: 250 demo.packetdamage.com | 250 PIPELINING | 250 SIZE 10240000 |
   8 26.000000     65.55.11         95 C: MAIL FROM:<loser@hotmail.com> SIZE=1902
   9 30.000000     173.255.         68 S: 250 2.1.0 Ok
  10 32.000000     65.55.11        102 C: RCPT TO:<cdilston@demo.packetdamage.com> |  |  |
```

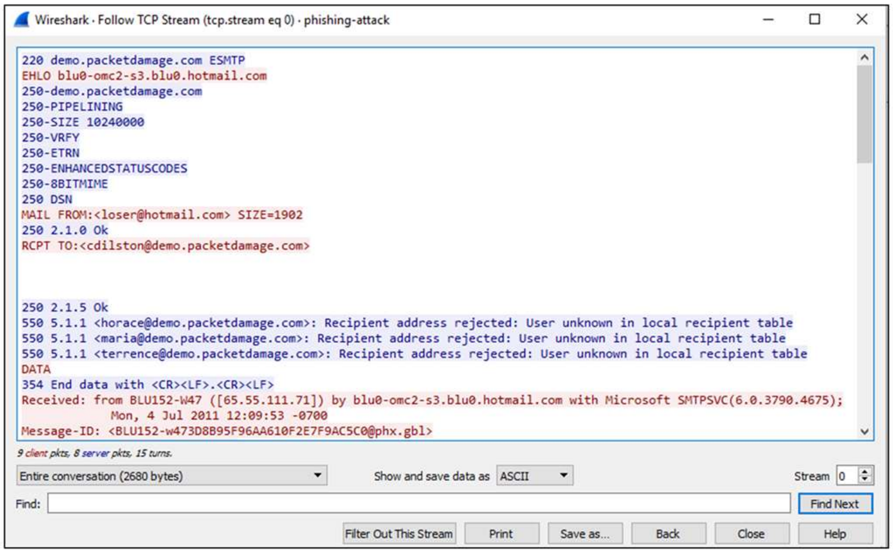
```
> Frame 1: 62 bytes on wire                       bits)
> Ethernet II, Src: Cisco_a                       :fd:ad:ff:e0:42 (fe:fd:ad:ff:e0:42)
> Internet Protocol Version                       224.66
> Transmission Control Protocol, Src Port: 64770, Dst Port: 25, Seq: 0, Len: 0
```

```
0000  fe fd ad ff e0 42 88 43  e1 a4 04 ff 08 00 45 00   .....B.C ......E.
0010  00 30 00 01 00 00 40 06  3c 00 41 37 6f 4e ad ff   .0....@. <.A7oN..
0020  e0 42 fd 02 00 19 01 6d  e6 f3 00 00 00 00 70 02   .B.....m ......p.
0030  ff ff 5e db 00 00 02 04  05 b4 01 01 04 02         ..^..... ......
```

Frame (frame), 62 bytes | Packets: 858 · Displayed: 858 (100.0%) · Load time: 0:0.31 | Profile: Default

Northeastern University

## TCP Session


Wireshark · Follow TCP Stream (tcp.stream eq 0) · phishing-attack

```
220 demo.packetdamage.com ESMTP
EHLO blu0-omc2-s3.blu0.hotmail.com
250-demo.packetdamage.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:<loser@hotmail.com> SIZE=1902
250 2.1.0 Ok
RCPT TO:<cdilston@demo.packetdamage.com>



250 2.1.5 Ok
550 5.1.1 <horace@demo.packetdamage.com>: Recipient address rejected: User unknown in local recipient table
550 5.1.1 <maria@demo.packetdamage.com>: Recipient address rejected: User unknown in local recipient table
550 5.1.1 <terrence@demo.packetdamage.com>: Recipient address rejected: User unknown in local recipient table
DATA
354 End data with <CR><LF>.<CR><LF>
Received: from BLU152-W47 ([65.55.111.71]) by blu0-omc2-s3.blu0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675);
            Mon, 4 Jul 2011 12:09:53 -0700
Message-ID: <BLU152-w473D8B95F96AA610F2E7F9AC5C0@phx.gbl>
```

9 client pkts, 8 server pkts, 15 turns.

Entire conversation (2680 bytes)

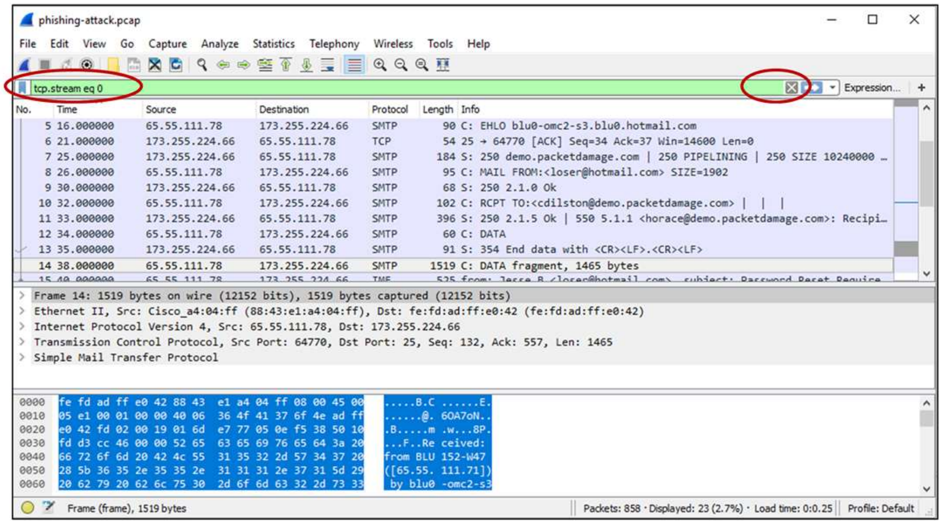
Show and save data as: ASCII

Stream: 0

Find:

Note: The blue highlights anything sent from the client to the server and red indicates anything sent from the server to the client.

# Make all Packets Available


phishing-attack.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

tcp.stream eq 0

```
No.  Time          Source           Destination      Protocol  Length  Info
   5 16.000000     65.55.111.78     173.255.224.66   SMTP        90 C: EHLO blu0-omc2-s3.blu0.hotmail.com
   6 21.000000     173.255.224.66   65.55.111.78     TCP         54 25 → 64770 [ACK] Seq=34 Ack=37 Win=14600 Len=0
   7 25.000000     173.255.224.66   65.55.111.78     SMTP       184 S: 250 demo.packetdamage.com | 250 PIPELINING | 250 SIZE 10240000 …
   8 26.000000     65.55.111.78     173.255.224.66   SMTP        95 C: MAIL FROM:<loser@hotmail.com> SIZE=1902
   9 30.000000     173.255.224.66   65.55.111.78     SMTP        68 S: 250 2.1.0 Ok
  10 32.000000     65.55.111.78     173.255.224.66   SMTP       102 C: RCPT TO:<cdilston@demo.packetdamage.com> |  |  |
  11 33.000000     173.255.224.66   65.55.111.78     SMTP       396 S: 250 2.1.5 Ok | 550 5.1.1 <horace@demo.packetdamage.com>: Recipi…
  12 34.000000     65.55.111.78     173.255.224.66   SMTP        60 C: DATA
  13 35.000000     173.255.224.66   65.55.111.78     SMTP        91 S: 354 End data with <CR><LF>.<CR><LF>
  14 38.000000     65.55.111.78     173.255.224.66   SMTP      1519 C: DATA fragment, 1465 bytes
  15 40.000000     65.55.111.78     173.255.224.66   IMF        525 from: Jesse B <loser@hotmail.com>, subject: Password Reset Require
```

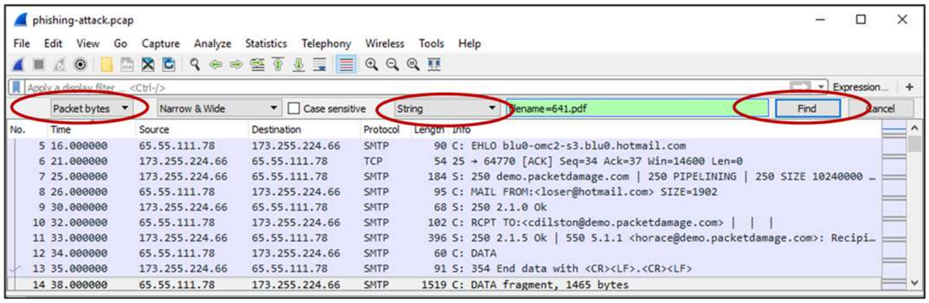
```
> Frame 14: 1519 bytes on wire (12152 bits), 1519 bytes captured (12152 bits)
> Ethernet II, Src: Cisco_a4:04:ff (88:43:e1:a4:04:ff), Dst: fe:fd:ad:ff:e0:42 (fe:fd:ad:ff:e0:42)
> Internet Protocol Version 4, Src: 65.55.111.78, Dst: 173.255.224.66
> Transmission Control Protocol, Src Port: 64770, Dst Port: 25, Seq: 132, Ack: 557, Len: 1465
> Simple Mail Transfer Protocol
```

```
0000  fe fd ad ff e0 42 88 43  e1 a4 04 ff 08 00 45 00   .....B.C ......E.
0010  05 e1 00 01 00 00 40 06  36 4f 41 37 6f 4e ad ff   ......@. 6OA7oN..
0020  e0 42 fd 02 00 19 01 6d  e7 77 05 0e f5 38 50 10   .B.....m .w...8P.
0030  fd d3 cc 46 00 00 52 65  63 65 69 76 65 64 3a 20   ...F..Re ceived: 
0040  66 72 6f 6d 20 42 4c 55  31 35 32 2d 57 34 37 20   from BLU 152-W47 
0050  28 5b 36 35 2e 35 35 2e  31 31 31 2e 37 31 5d 29   ([65.55. 111.71])
0060  20 62 79 20 62 6c 75 30  2d 6f 6d 63 32 2d 73 33    by blu0 -omc2-s3
```

Frame (frame), 1519 bytes    Packets: 858 · Displayed: 23 (2.7%) · Load time: 0:0.25    Profile: Default

Northeastern University

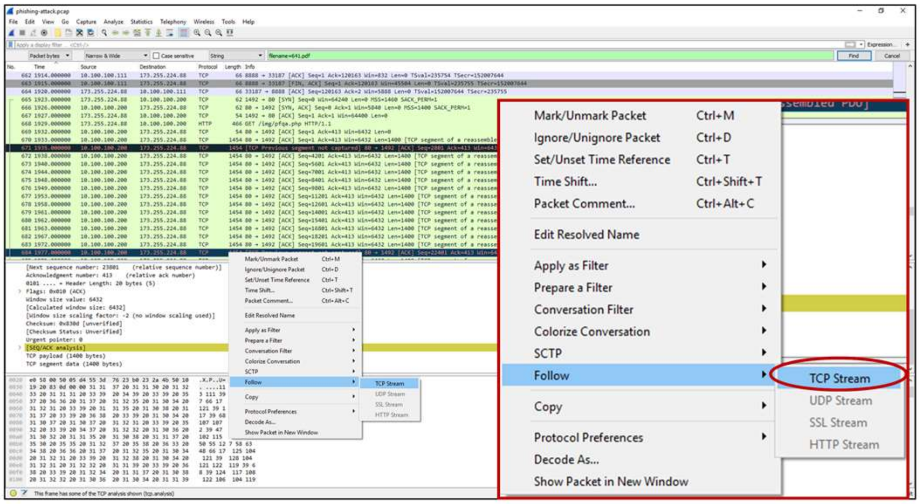
# Find a Packet


phishing-attack.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Find
Cancel

Packet bytes ▾ | Narrow & Wide ▾ | □ Case sensitive | String ▾ | filename=641.pdf

```
No. Time        Source          Destination     Protocol Length Info
  5 16.000000   65.55.111.78    173.255.224.66  SMTP       90 C: EHLO blu0-omc2-s3.blu0.hotmail.com
  6 21.000000   173.255.224.66  65.55.111.78    TCP        54 25 → 64770 [ACK] Seq=34 Ack=37 Win=14600 Len=0
  7 25.000000   173.255.224.66  65.55.111.78    SMTP      184 S: 250 demo.packetdamage.com | 250 PIPELINING | 250 SIZE 10240000 …
  8 26.000000   65.55.111.78    173.255.224.66  SMTP       95 C: MAIL FROM:<loser@hotmail.com> SIZE=1902
  9 30.000000   173.255.224.66  65.55.111.78    SMTP       68 S: 250 2.1.0 Ok
 10 32.000000   65.55.111.78    173.255.224.66  SMTP      102 C: RCPT TO:<cdilston@demo.packetdamage.com> |  |  |
 11 33.000000   173.255.224.66  65.55.111.78    SMTP      396 S: 250 2.1.5 Ok | 550 5.1.1 <horace@demo.packetdamage.com>: Recipi…
 12 34.000000   65.55.111.78    173.255.224.66  SMTP       60 C: DATA
 13 35.000000   173.255.224.66  65.55.111.78    SMTP       91 S: 354 End data with <CR><LF>.<CR><LF>
 14 38.000000   65.55.111.78    173.255.224.66  SMTP     1519 C: DATA fragment, 1465 bytes
```

# Follow the Session


phishing-attack.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Packet bytes
Narrow & Wide
□ Case sensitive
String
Find
Cancel
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream

filename=641.pdf

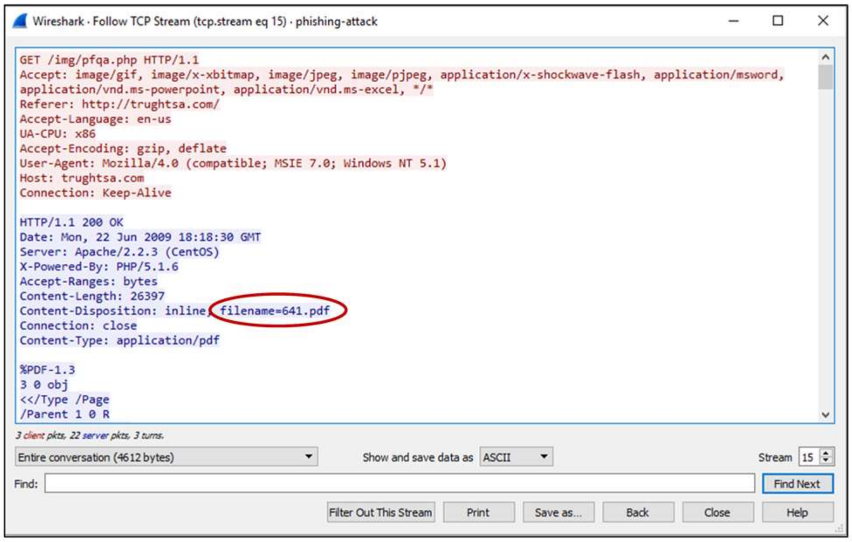
```
No.  Time            Source           Destination      Protocol  Length  Info
662 1914.000000   10.100.100.111   173.255.224.88   TCP         66 8888 → 33187 [ACK] Seq=1 Ack=120163 Win=832 Len=0 TSval=235754 TSecr=152007644
663 1915.000000   10.100.100.111   173.255.224.88   TCP         66 8888 → 33187 [FIN, ACK] Seq=1 Ack=120163 Win=45504 Len=0 TSval=235755 TSecr=152007644
664 1920.000000   173.255.224.88   10.100.100.111   TCP         66 33187 → 8888 [ACK] Seq=120163 Ack=2 Win=5888 Len=0 TSval=152007644 TSecr=235755
665 1923.000000   173.255.224.88   10.100.100.200   TCP         62 1492 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
666 1926.000000   10.100.100.200   173.255.224.88   TCP         62 80 → 1492 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400 SACK_PERM=1
667 1927.000000   173.255.224.88   10.100.100.200   TCP         54 1492 → 80 [ACK] Seq=1 Ack=1 Win=64400 Len=0
668 1929.000000   173.255.224.88   10.100.100.200   HTTP       466 GET /img/pfqa.php HTTP/1.1
669 1932.000000   10.100.100.200   173.255.224.88   TCP         54 80 → 1492 [ACK] Seq=1 Ack=413 Win=6432 Len=0
670 1933.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=1 Ack=413 Win=6432 Len=1400 [TCP segment of a reassemble
671 1935.000000   10.100.100.200   173.255.224.88   TCP       1454 [TCP Previous segment not captured] 80 → 1492 [ACK] Seq=2801 Ack=413 Win=643
672 1938.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=4201 Ack=413 Win=6432 Len=1400 [TCP segment of a reassem
673 1940.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=5601 Ack=413 Win=6432 Len=1400 [TCP segment of a reassem
674 1944.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=7001 Ack=413 Win=6432 Len=1400 [TCP segment of a reassem
675 1948.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=8401 Ack=413 Win=6432 Len=1400 [TCP segment of a reassem
676 1949.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=9801 Ack=413 Win=6432 Len=1400 [TCP segment of a reassem
677 1953.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=11201 Ack=413 Win=6432 Len=1400 [TCP segment of a reasse
678 1958.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=12601 Ack=413 Win=6432 Len=1400 [TCP segment of a reasse
679 1961.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=14001 Ack=413 Win=6432 Len=1400 [TCP segment of a reasse
680 1962.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=15401 Ack=413 Win=6432 Len=1400 [TCP segment of a reasse
681 1963.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=16801 Ack=413 Win=6432 Len=1400 [TCP segment of a reasse
682 1967.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=18201 Ack=413 Win=6432 Len=1400 [TCP segment of a reasse
683 1972.000000   10.100.100.200   173.255.224.88   TCP       1454 80 → 1492 [ACK] Seq=19601 Ack=413 Win=6432 Len=1400 [TCP segment of a reasse
684 1977.000000   10.100.100.200   173.255.224.88   TCP                                  80 → 1492 [ACK] Seq=22401 Ack=413 Win=64
```

```
    [Next sequence number: 23801    (relative sequence number)]
    Acknowledgment number: 413    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 6432
    [Calculated window size: 6432]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x830d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (1400 bytes)
    TCP segment data (1400 bytes)
```

```
0020  e0 58 00 50 05 d4 55 3d  76 23 b0 23 2a 4b 50 10   .X.P..U=
0030  19 20 83 0d 00 00 31 31  37 20 31 31 30 20 31 32   . ....11
0040  33 20 31 31 31 20 33 39  20 34 39 20 33 39 20 35   3 111 39
0050  37 20 36 36 20 31 37 20  31 32 35 20 31 30 34 20   7 66 17
0060  31 32 31 20 33 39 20 31  31 35 20 31 30 38 20 31   121 39 1
0070  31 37 20 33 39 20 36 38  20 33 39 20 31 30 34 20   17 39 68
0080  31 30 37 20 31 30 37 20  31 32 31 20 33 39 20 35   107 107
0090  32 20 33 39 20 34 37 20  31 32 32 20 31 30 36 20   2 39 47
00a0  31 30 32 20 31 31 35 20  31 30 38 20 31 31 37 20   102 115
00b0  35 30 20 35 35 20 31 32  37 20 35 38 20 36 33 20   50 55 12 7 58 63
00c0  34 38 20 36 36 20 31 37  20 31 32 35 20 31 30 34   48 66 17  125 104
00d0  20 31 32 31 20 33 39 20  31 32 38 20 31 30 34 20    121 39  128 104
00e0  31 32 31 20 31 32 32 20  31 31 39 20 33 39 20 36   121 122  119 39 6
00f0  38 20 33 39 20 31 32 34  20 31 31 37 20 31 30 38   8 39 124  117 108
0100  20 31 32 32 20 31 30 36  20 31 30 34 20 31 31 39    122 106  104 119
```

This frame has some of the TCP analysis shown (tcp.analysis)

# Session Reconstruction



Wireshark · Follow TCP Stream (tcp.stream eq 15) · phishing-attack

```
GET /img/pfqa.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword,
application/vnd.ms-powerpoint, application/vnd.ms-excel, */*
Referer: http://trughtsa.com/
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Host: trughtsa.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 22 Jun 2009 18:18:30 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Accept-Ranges: bytes
Content-Length: 26397
Content-Disposition: inline; filename=641.pdf
Connection: close
Content-Type: application/pdf

%PDF-1.3
3 0 obj
<</Type /Page
/Parent 1 0 R
```

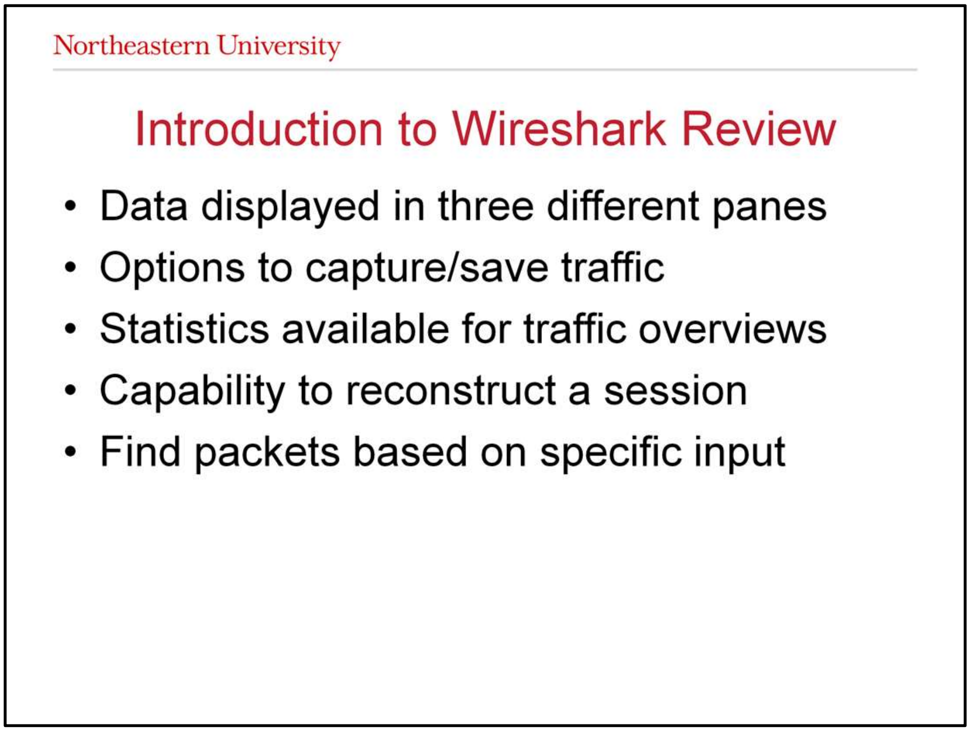
3 client pkts, 22 server pkts, 3 turns.

Entire conversation (4612 bytes)

Show and save data as: ASCII

Stream: 15

Find:



Northeastern University

## Introduction to Wireshark Review

- Data displayed in three different panes
- Options to capture/save traffic
- Statistics available for traffic overviews
- Capability to reconstruct a session
- Find packets based on specific input

References:

- http://www.wireshark.org/docs
- http://wiki.wireshark.org

Northeastern