Advanced Troubleshooting Tools

arek@arekdreyer.com

MacSysAdmin 2010

Troubleshooting Tools

- DNS
- Packet Analysis
- File Use Analysis
- DTrace
- `spindump`

DNS

- `mDNSResponder`
- `dsacheutil`
- /etc/hosts
- dns_fallback
- Dynamic DNS Update

mDNSResponder

- One True Source of DNS resolution
- *Except `DirectoryService` uses /etc/hosts

mDNSResponder

- `sudo killall ____ mDNSResponder`
  - `-USR1`
  - `-USR2`
  - `-INFO`
  - `-HUP`
- plain old kill

–USR1

- toggle additional logging
  - Warning and Notice
- `sudo syslog -c mDNSResponder -d`
  - All levels (Emergency - Debug)
- /var/log/system.log

–USR2

- packet logging
- /var/log/system.log

-INFO

- snapshot of internal state
- /var/log/system.log

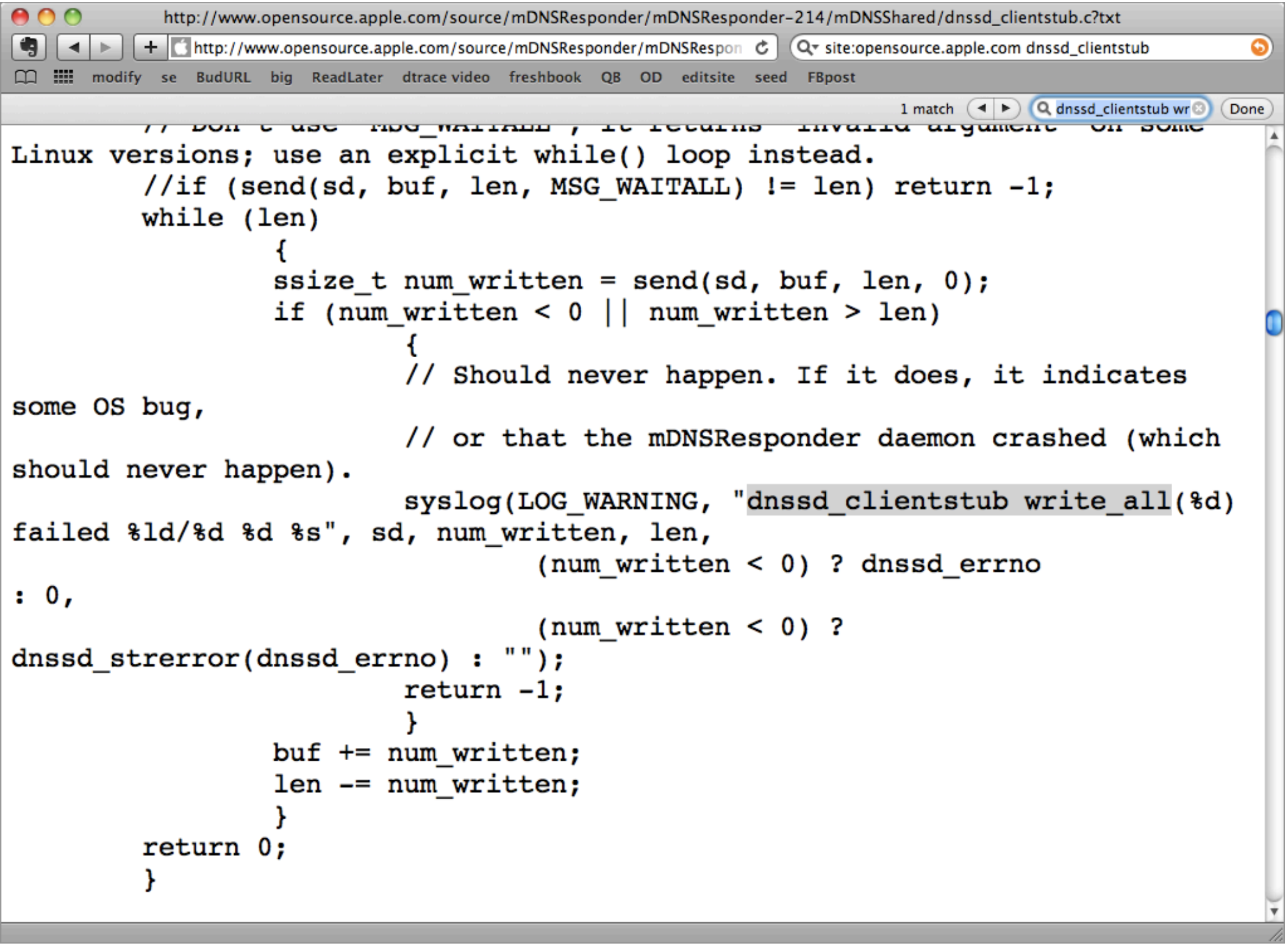
(No Signal)

- `sudo killall mDNSResponder`
  - mDNSResponder dies
  - toggles are untoggled
- gets relaunched
  - except when it doens't

mDNSResponder dead

- I Killed mDNSResponder
- mDNSResponder didn't start again
- system.log said:

  dnssd_clientstub write_all failed
- dnssd_clientstub search in opensource




```
Linux versions; use an explicit while() loop instead.
        //if (send(sd, buf, len, MSG_WAITALL) != len) return -1;
        while (len)
                {
                ssize_t num_written = send(sd, buf, len, 0);
                if (num_written < 0 || num_written > len)
                        {
                        // Should never happen. If it does, it indicates
some OS bug,
                        // or that the mDNSResponder daemon crashed (which
should never happen).
                        syslog(LOG_WARNING, "dnssd_clientstub write_all(%d)
failed %ld/%d %d %s", sd, num_written, len,
                                (num_written < 0) ? dnssd_errno
: 0,
                                (num_written < 0) ?
dnssd_strerror(dnssd_errno) : "");
                        return -1;
                        }
                buf += num_written;
                len -= num_written;
                }
        return 0;
        }
```

–HUP

- So don't just kill it. Send a HUP.

see man page

- Fun question: why doesn't this work?
  - `man mdnsresponder`

dscacheutil

- `-q`
- `-cachedump`
- `-flushcache`

dscacheutil -q

- ```
  dscacheutil \
  -q host \
  -a name dc01.ssh22.com
  ```
- queries for answer
- adds positive result to cache
  ```

show host cache?

- Deprecated in 10.6:
  - `dscacheutil -cachedump -entries host`
- Use mDNSResponder -INFO instead

/etc/hosts

- What uses it
- What ignores it

Uses /etc/hosts

- Anything that uses mDNSResponder
  - Server Admin, Workgroup Manager
  - Safari
  - `dscacheutil -q host -a name a1.lan`
- `ping`
- `ssh`

Ignores /etc/hosts

- `host`
- `dig`
- `nslookup`

mDNSResponder and /etc/hosts/

- Add host to DNS service, /etc/hosts
  - assign different IP addresses
- dscacheutil -q host -a name a.ssh22.com
  - returns /etc/host answer
- remove from /etc/hosts
  - dscacheutil returns value from DNS

dns_fallback

- in edu.mit.Kerberos
- default: `dns_fallback = no`
- set to yes to use DNS SRV records
  - instead of Directory Service

Packet Analysis

- Capture
- Analyze

Capture Packets

- `tcpdump`
- Filtering out unwanted packets

interface: -i

- -ien0
- -ien l

packet size limit: -s

- -s0 no limit

write to a file: -w

- -w filename.pcap

don't checksum: -K

- checksum will be wrong anyway

don't resolve names: -n

- explicit port number not name
- explicit IP number not hostname

DS/DNS ports

Kerberos authentication	88
Kerberos password change	464
LDAP	389
LDAPS	636
SMB	137, 138, 139, 445
DNS	53
mDNS	5353

filter by port

- port name or port number
- combine with "||" or "or"
- `'port 88 || 464 || 389 || 137 || 138 || 139 || 445'`

filter by host

- host server01.ssh22.com

Put it all together

- ```
  sudo tcpdump –wCannotbind.pcap \
  –ien0 –s0 –K \
  'port 88 || 464 || 389 || 137 || 138
  || 139 || 445'
  ```
  ```

Analyze Capture Files

- Display at CLI
- Packet Analysis Software

tcpdump from file: -r

- tcpdump -r Cannotbind.pcap

Display data in ASCII

- -A: ASCII
- -X: ASCII and Hex
- tcpdump -A -r somefile.pcap

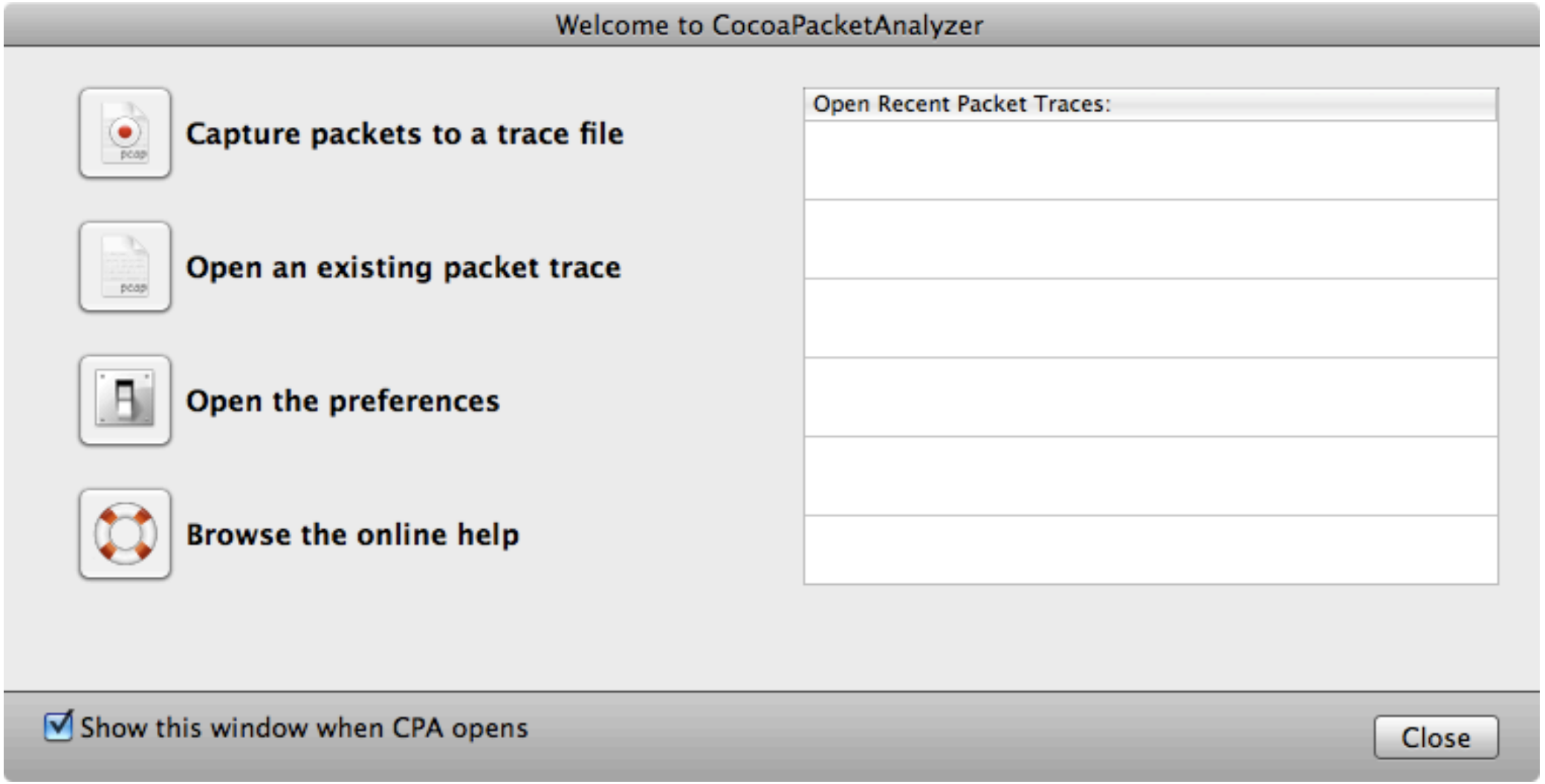
Analysis Software

- Free
- Commercial

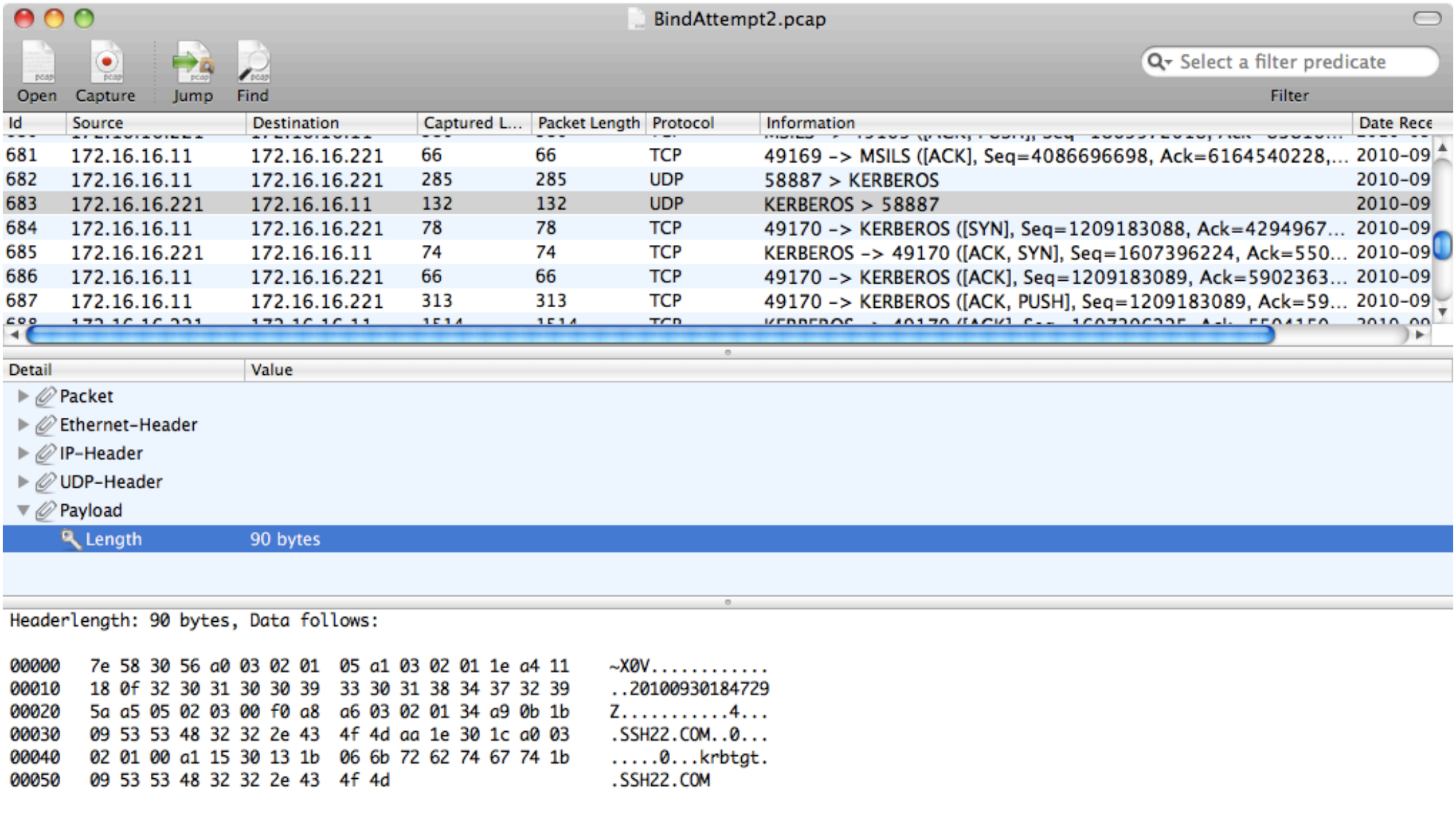
Free

- CocoaPacketAnalyzer
- WireShark
  - requires X11
- Large monitor helps

CocoaPacketAnalyzer

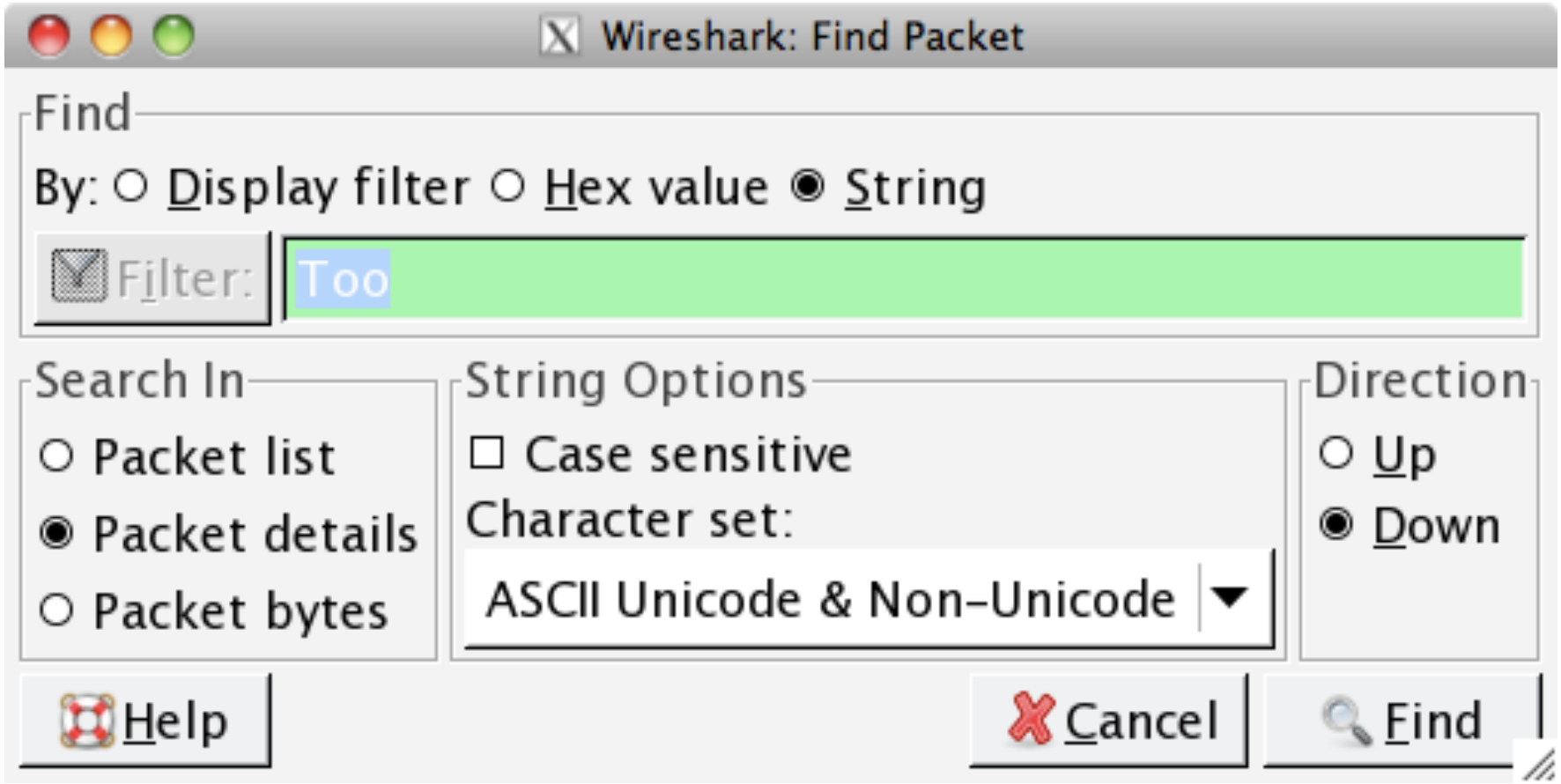


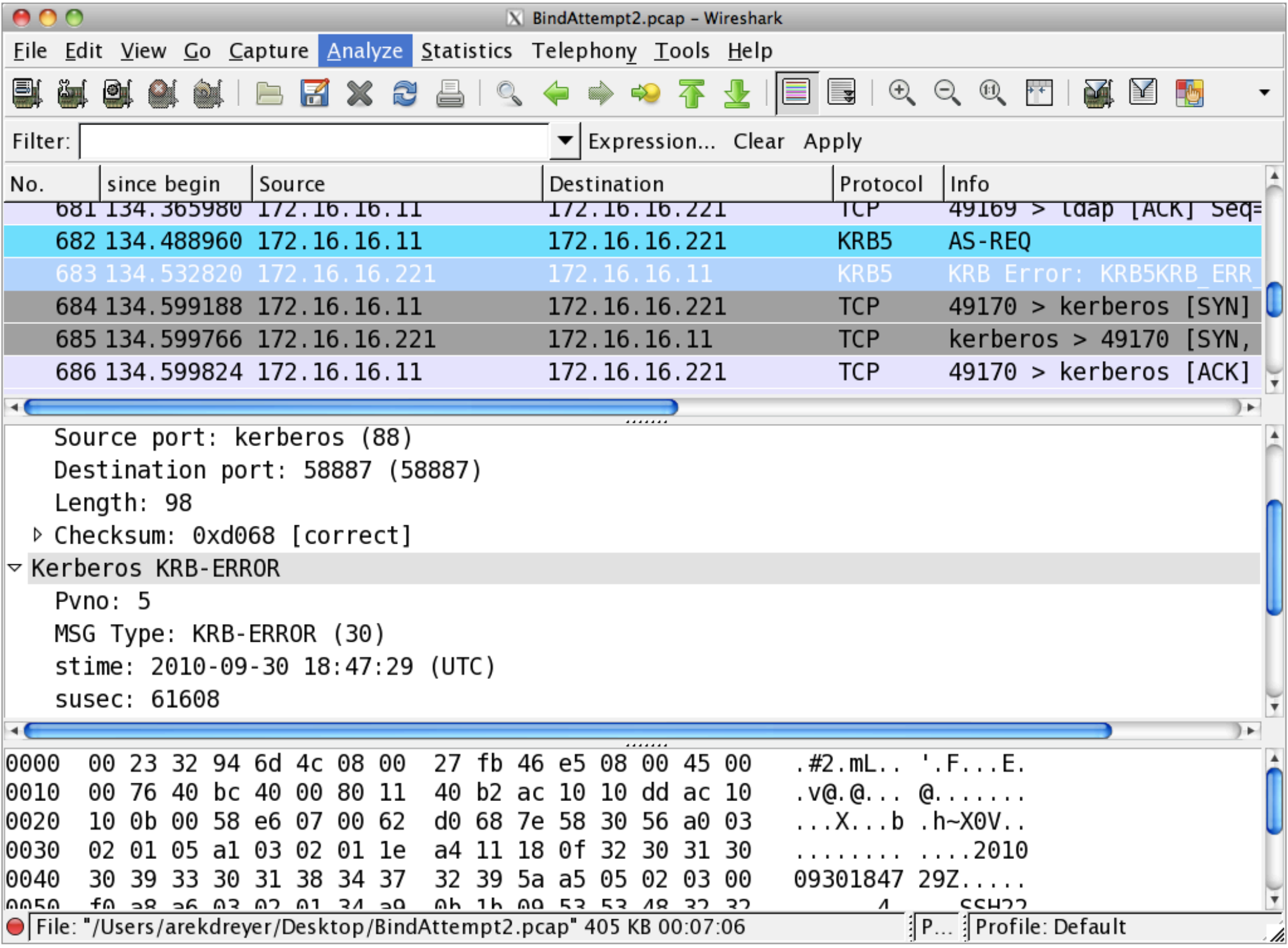
CocoaPacketAnalyzer

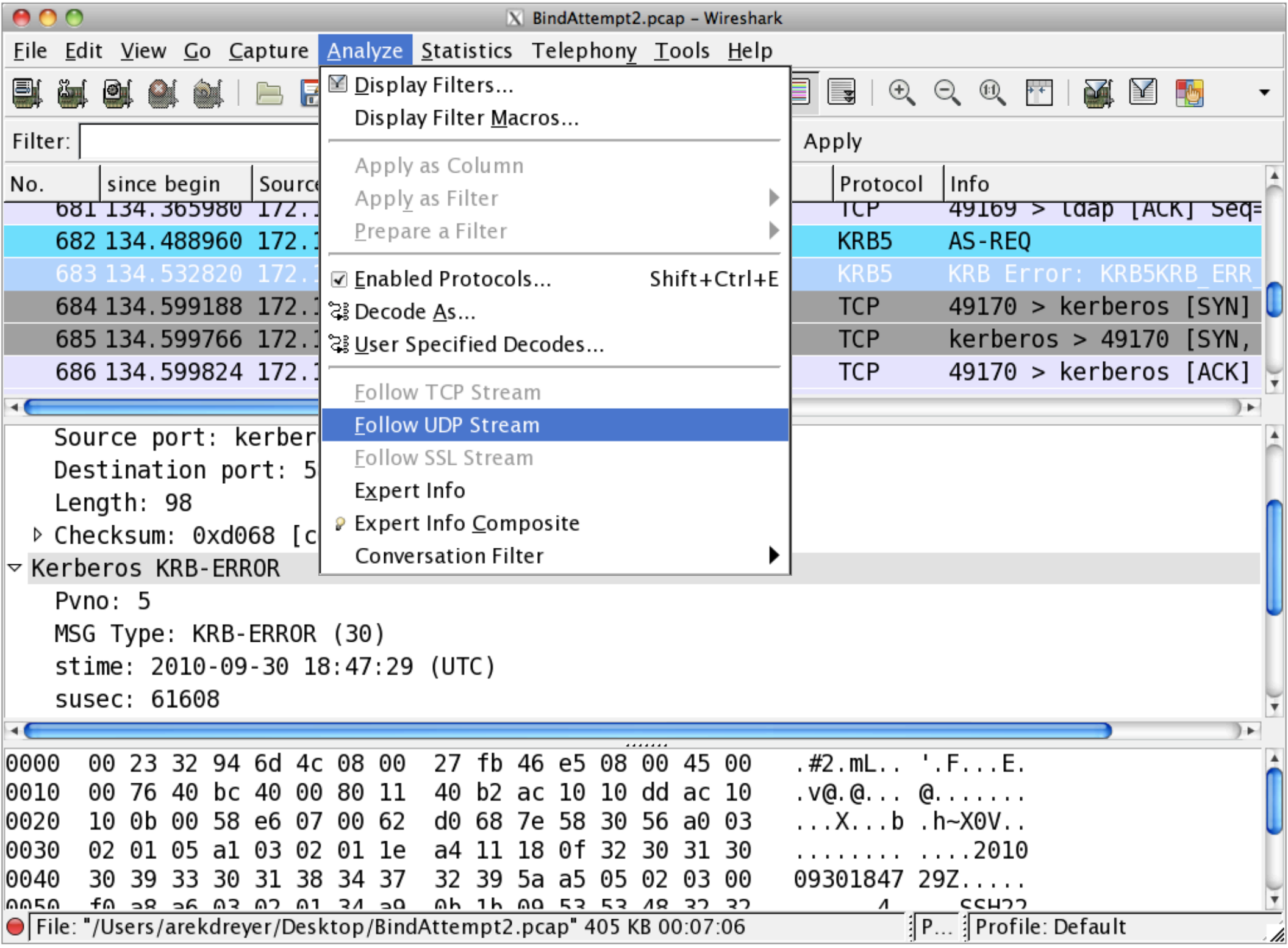


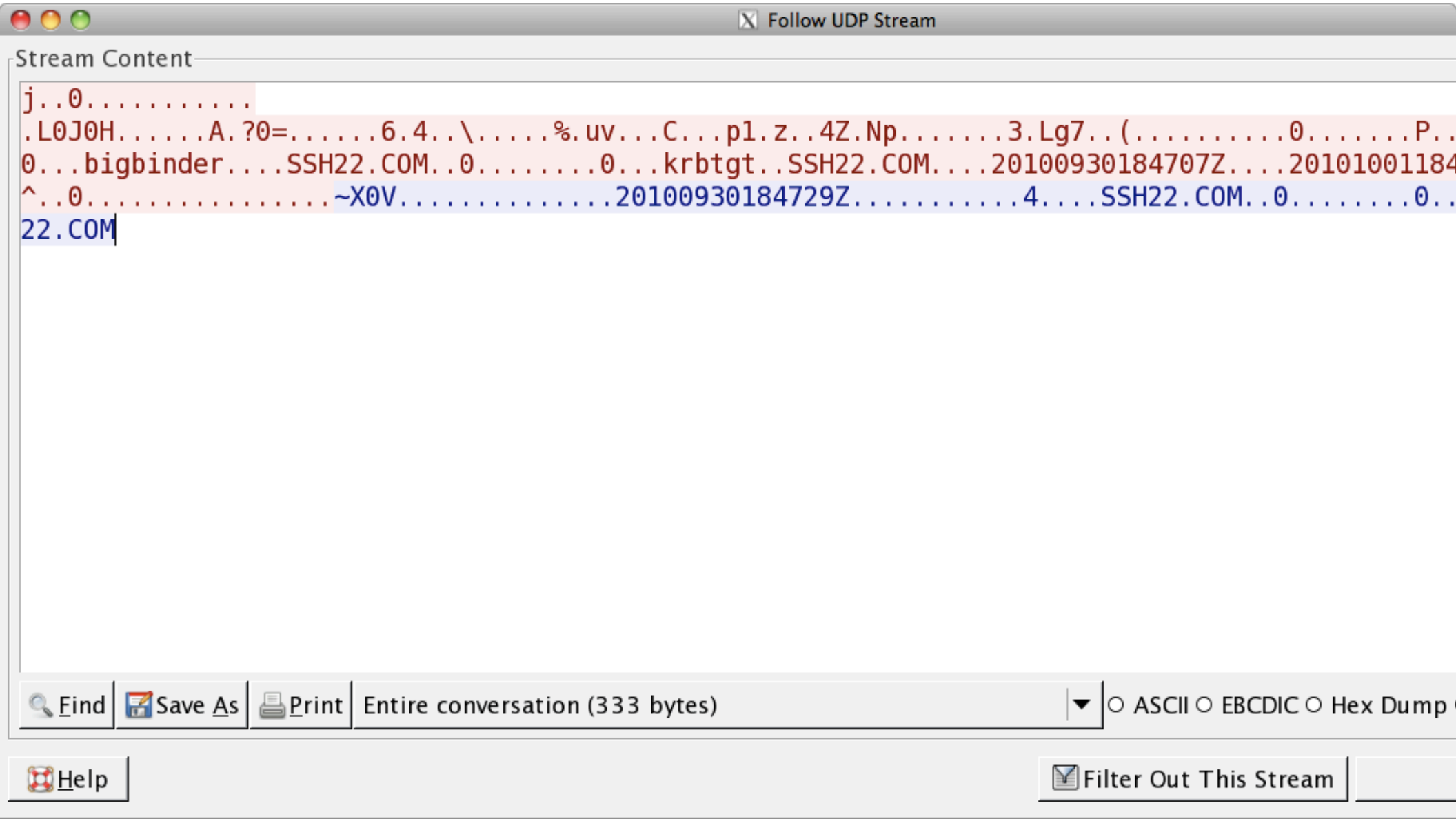
Wireshark Features

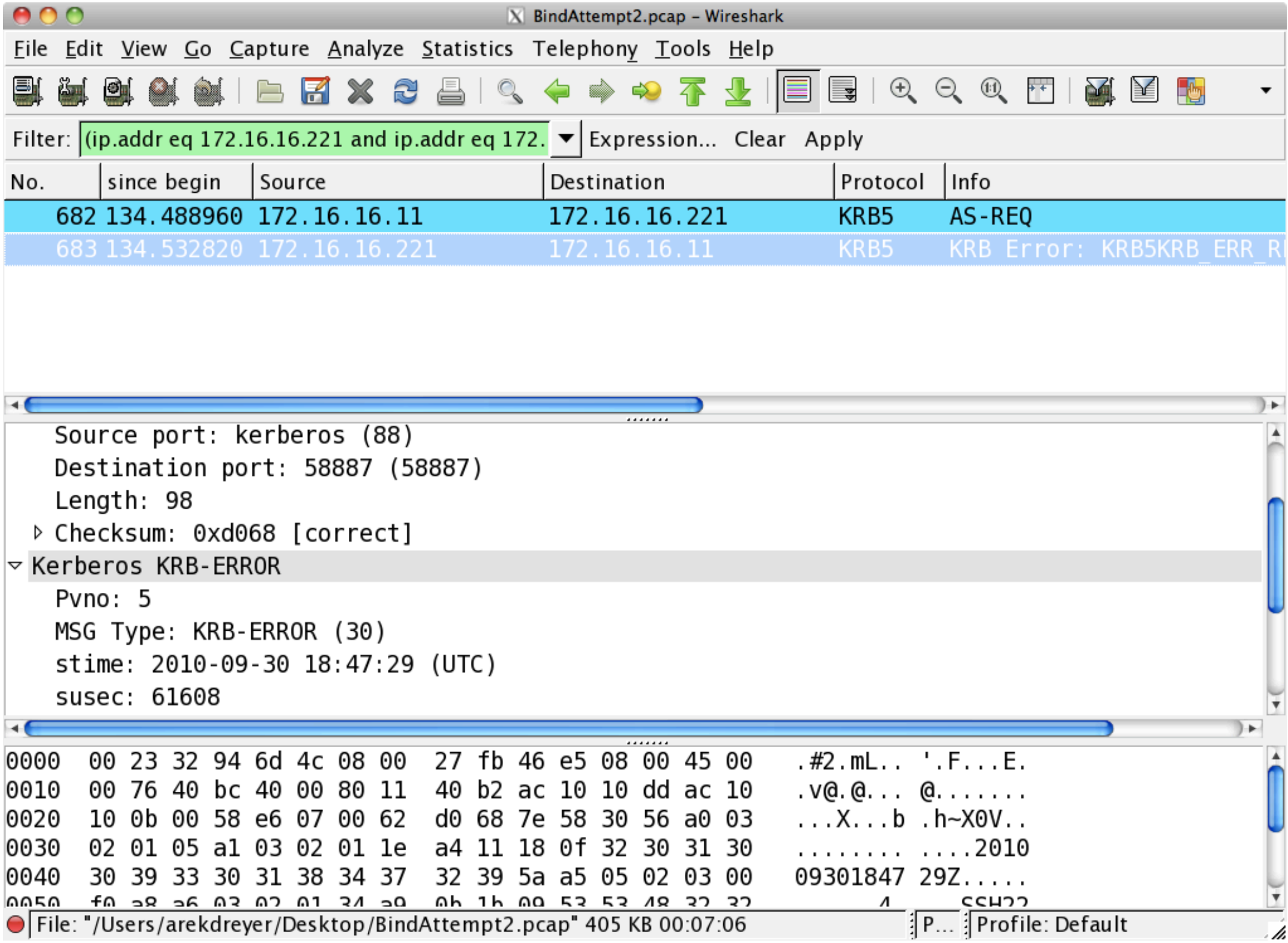
- Find ASCII string in packets
- Follow UDP or TCP stream
  - Automatically creates filter
- 4 TCP graphs

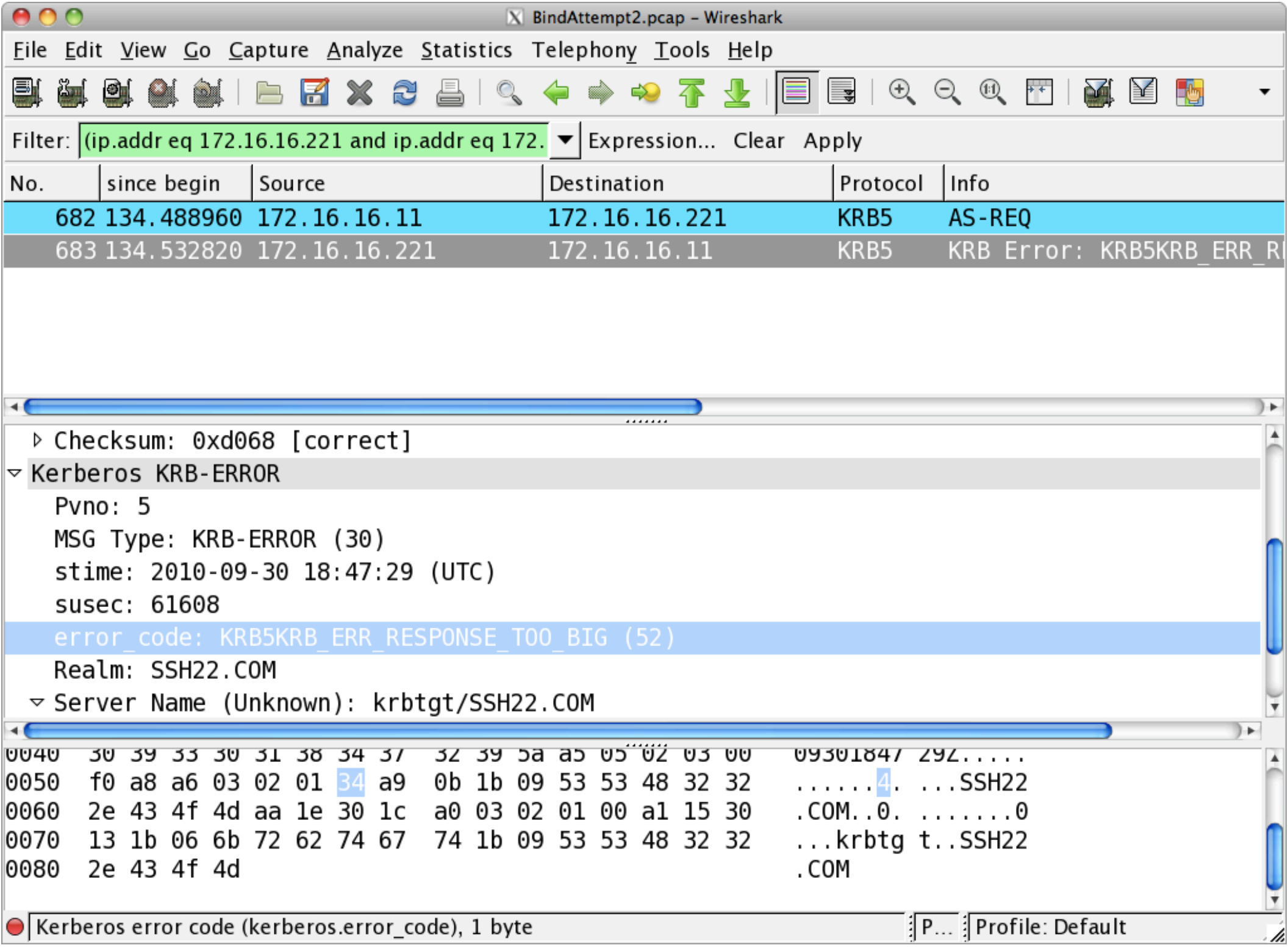

Wireshark: Find Packet
Find
By: Display filter Hex value String
Filter:
Too
Search In
Packet list
Packet details
Packet bytes
String Options
Case sensitive
Character set:
ASCII Unicode & Non-Unicode
Direction
Up
Down
Help
Cancel
Find

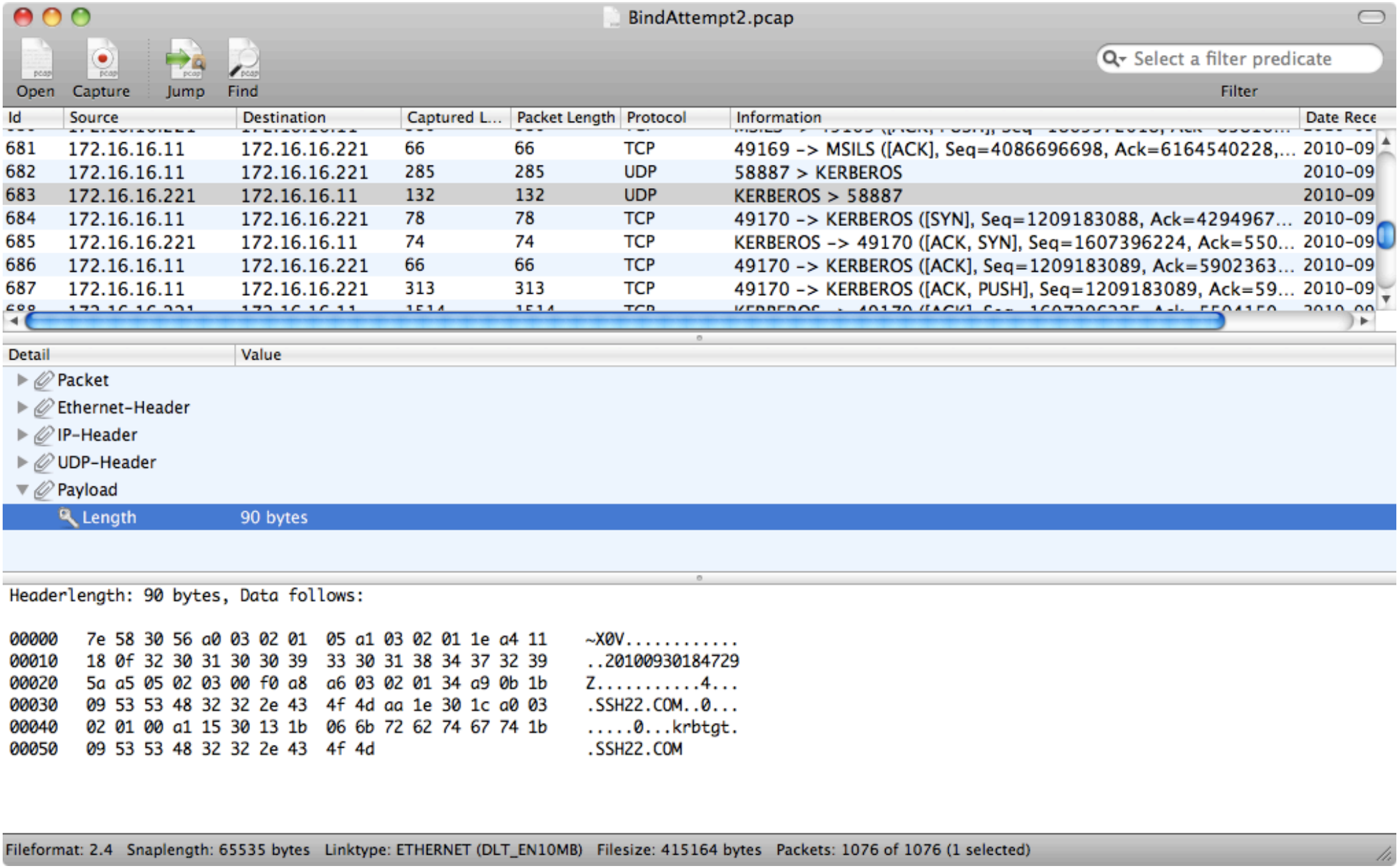

BindAttempt2.pcap – Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. since begin Source Destination Protocol Info
681 134.365980 172.16.16.11 172.16.16.221 TCP 49169 > ldap [ACK] Seq=
682 134.488960 172.16.16.11 172.16.16.221 KRB5 AS-REQ
683 134.532820 172.16.16.221 172.16.16.11 KRB5 KRB Error: KRB5KRB_ERR_
684 134.599188 172.16.16.11 172.16.16.221 TCP 49170 > kerberos [SYN]
685 134.599766 172.16.16.221 172.16.16.11 TCP kerberos > 49170 [SYN,
686 134.599824 172.16.16.11 172.16.16.221 TCP 49170 > kerberos [ACK]
Source port: kerberos (88)
Destination port: 58887 (58887)
Length: 98
Checksum: 0xd068 [correct]
Kerberos KRB-ERROR
Pvno: 5
MSG Type: KRB-ERROR (30)
stime: 2010-09-30 18:47:29 (UTC)
susec: 61608
0000 00 23 32 94 6d 4c 08 00 27 fb 46 e5 08 00 45 00 .#2.mL.. '.F...E.
0010 00 76 40 bc 40 00 80 11 40 b2 ac 10 10 dd ac 10 .v@.@... @.......
0020 10 0b 00 58 e6 07 00 62 d0 68 7e 58 30 56 a0 03 ...X...b .h~X0V..
0030 02 01 05 a1 03 02 01 1e a4 11 18 0f 32 30 31 30 2010
0040 30 39 33 30 31 38 34 37 32 39 5a a5 05 02 03 00 09301847 29Z.....
File: "/Users/arekdreyer/Desktop/BindAttempt2.pcap" 405 KB 00:07:06
P...
Profile: Default

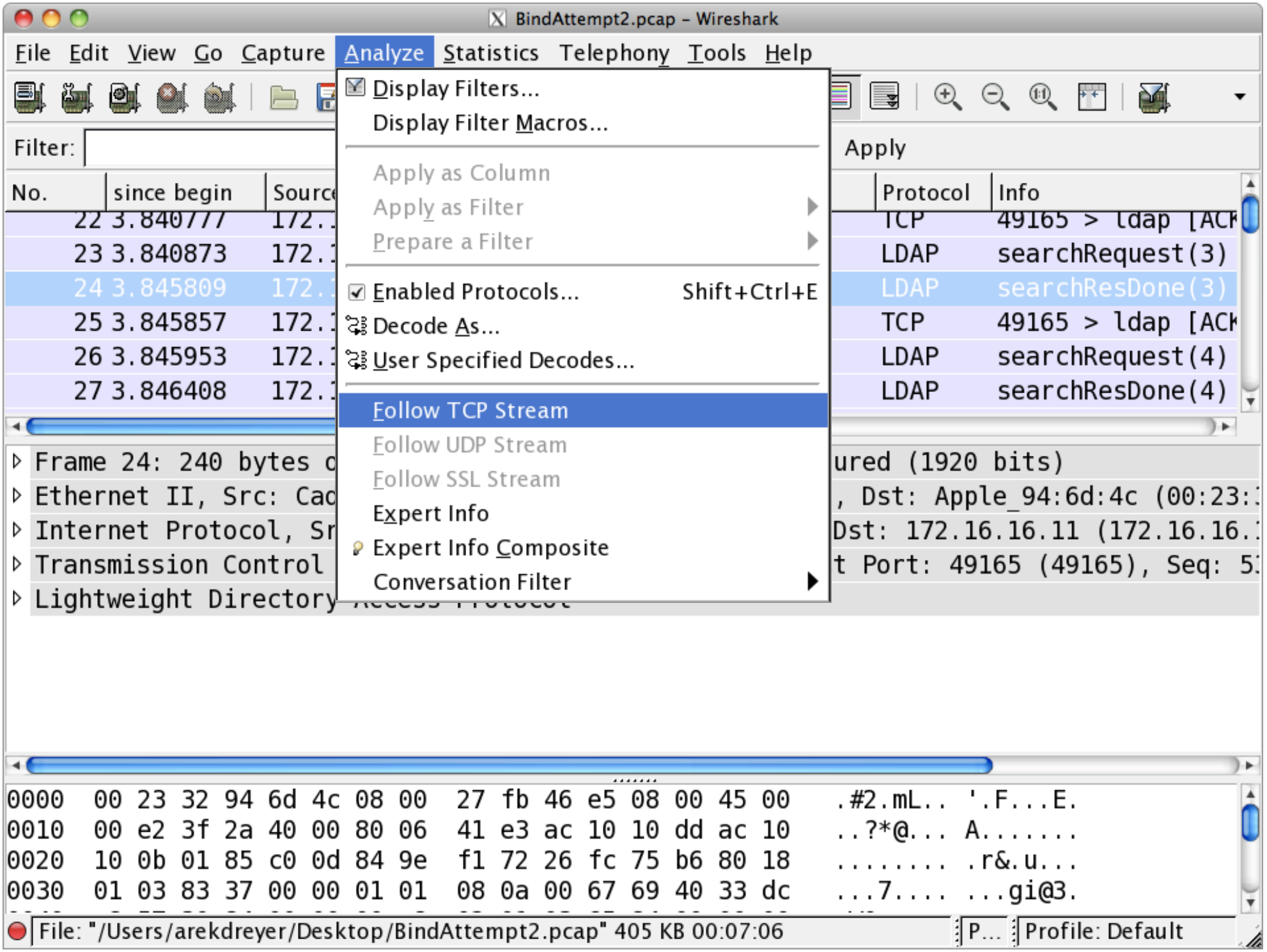

BindAttempt2.pcap – Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Enabled Protocols... Shift+Ctrl+E
Decode As...
User Specified Decodes...
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Expert Info
Expert Info Composite
Conversation Filter
Filter:
Apply
No. since begin Source Protocol Info
682 134.488960 KRB5 AS-REQ
683 134.532820 KRB5 KRB Error: KRB5KRB_ERR
684 134.599188 TCP 49170 > kerberos [SYN]
685 134.599766 TCP kerberos > 49170 [SYN,
686 134.599824 TCP 49170 > kerberos [ACK]
Source port: kerber
Destination port: 5
Length: 98
Checksum: 0xd068 [c
Kerberos KRB-ERROR
Pvno: 5
MSG Type: KRB-ERROR (30)
stime: 2010-09-30 18:47:29 (UTC)
susec: 61608
0000 00 23 32 94 6d 4c 08 00 27 fb 46 e5 08 00 45 00 .#2.mL.. '.F...E.
0010 00 76 40 bc 40 00 80 11 40 b2 ac 10 10 dd ac 10 .v@.@... @.....
0020 10 0b 00 58 e6 07 00 62 d0 68 7e 58 30 56 a0 03 ...X...b .h~X0V..
0030 02 01 05 a1 03 02 01 1e a4 11 18 0f 32 30 31 30 2010
0040 30 39 33 30 31 38 34 37 32 39 5a a5 05 02 03 00 09301847 29Z.....
File: "/Users/arekdreyer/Desktop/BindAttempt2.pcap" 405 KB 00:07:06
Profile: Default

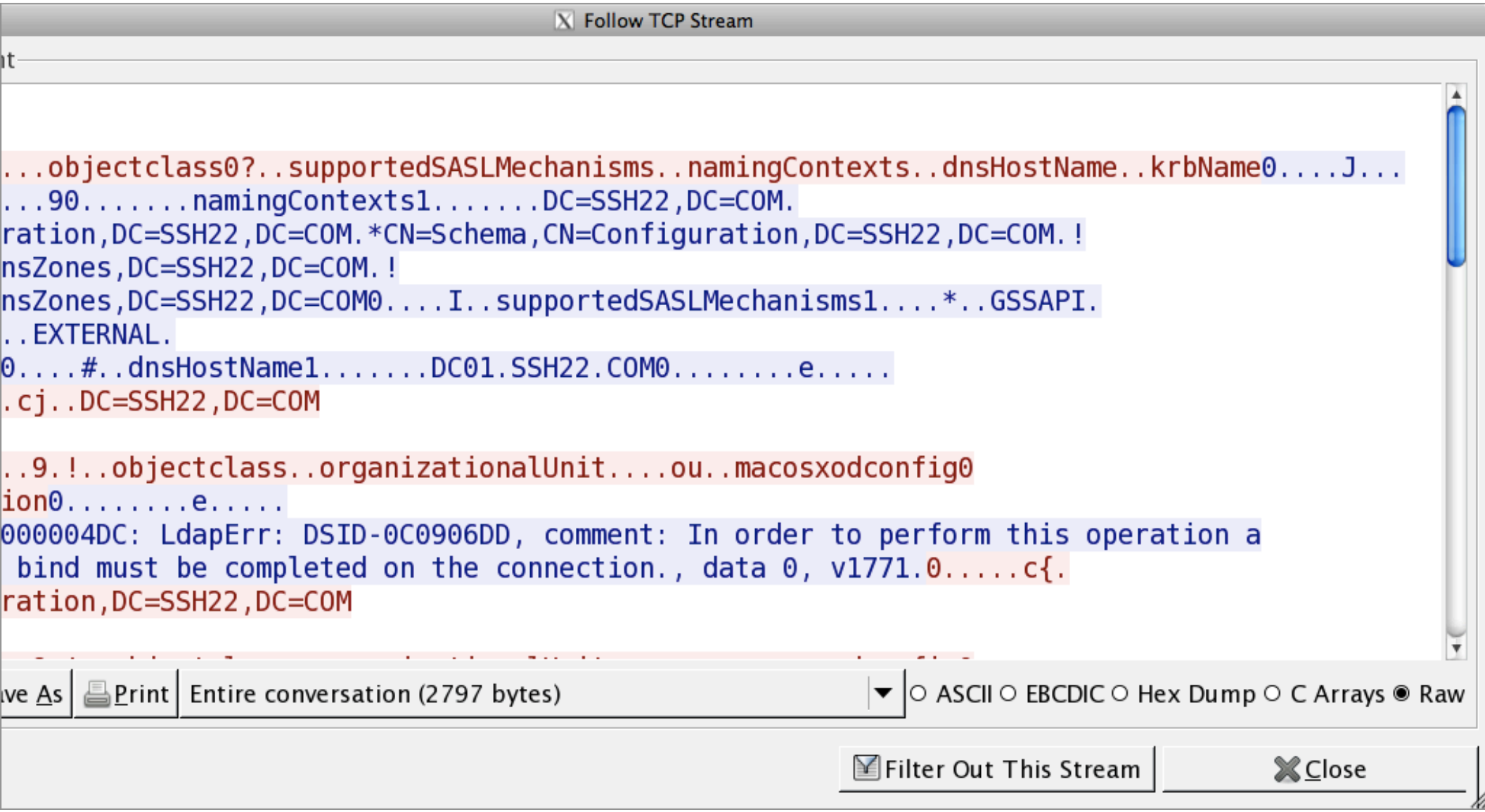

Follow UDP Stream
Stream Content
j..0.....
.L0J0H.....A.?0=.....6.4..\.....%.uv...C...p1.z..4Z.Np.....3.Lg7..(.....0.....P..
0...bigbinder....SSH22.COM..0.....0...krbtgt..SSH22.COM....20100930184707Z....20101001184
^..0.....~X0V.....20100930184729Z.....4....SSH22.COM..0.....0..
22.COM
Find
Save As
Print
Entire conversation (333 bytes)
ASCII
EBCDIC
Hex Dump
Help
Filter Out This Stream

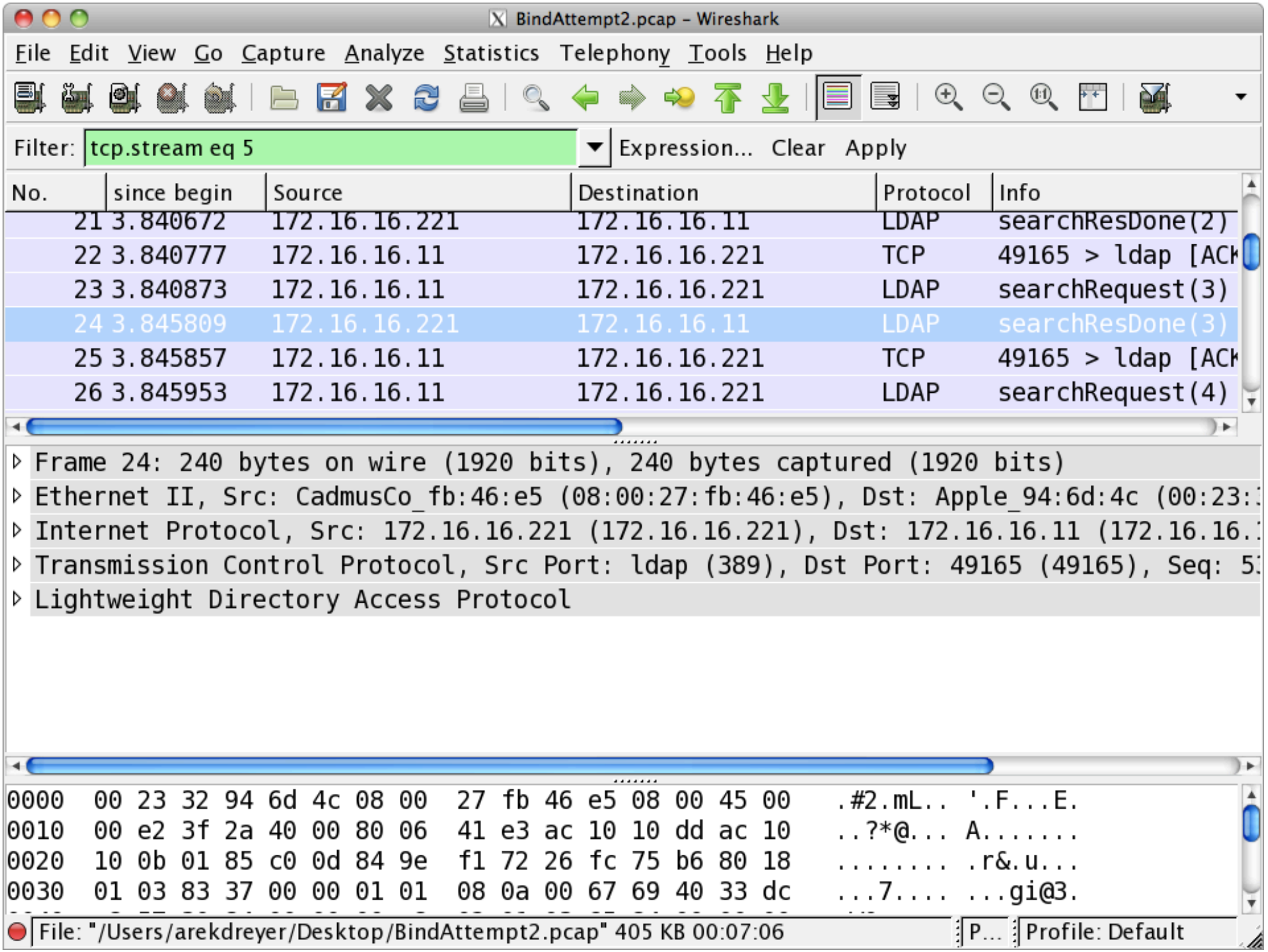

BindAttempt2.pcap – Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: (ip.addr eq 172.16.16.221 and ip.addr eq 172.
Expression... Clear Apply
No. since begin Source Destination Protocol Info
682 134.488960 172.16.16.11 172.16.16.221 KRB5 AS-REQ
683 134.532820 172.16.16.221 172.16.16.11 KRB5 KRB Error: KRB5KRB_ERR_R
Source port: kerberos (88)
Destination port: 58887 (58887)
Length: 98
Checksum: 0xd068 [correct]
Kerberos KRB-ERROR
Pvno: 5
MSG Type: KRB-ERROR (30)
stime: 2010-09-30 18:47:29 (UTC)
susec: 61608
0000 00 23 32 94 6d 4c 08 00 27 fb 46 e5 08 00 45 00 .#2.mL.. '.F...E.
0010 00 76 40 bc 40 00 80 11 40 b2 ac 10 10 dd ac 10 .v@.@... @.......
0020 10 0b 00 58 e6 07 00 62 d0 68 7e 58 30 56 a0 03 ...X...b .h~X0V..
0030 02 01 05 a1 03 02 01 1e a4 11 18 0f 32 30 31 30 2010
0040 30 39 33 30 31 38 34 37 32 39 5a a5 05 02 03 00 09301847 29Z.....
File: "/Users/arekdreyer/Desktop/BindAttempt2.pcap" 405 KB 00:07:06
P...
Profile: Default

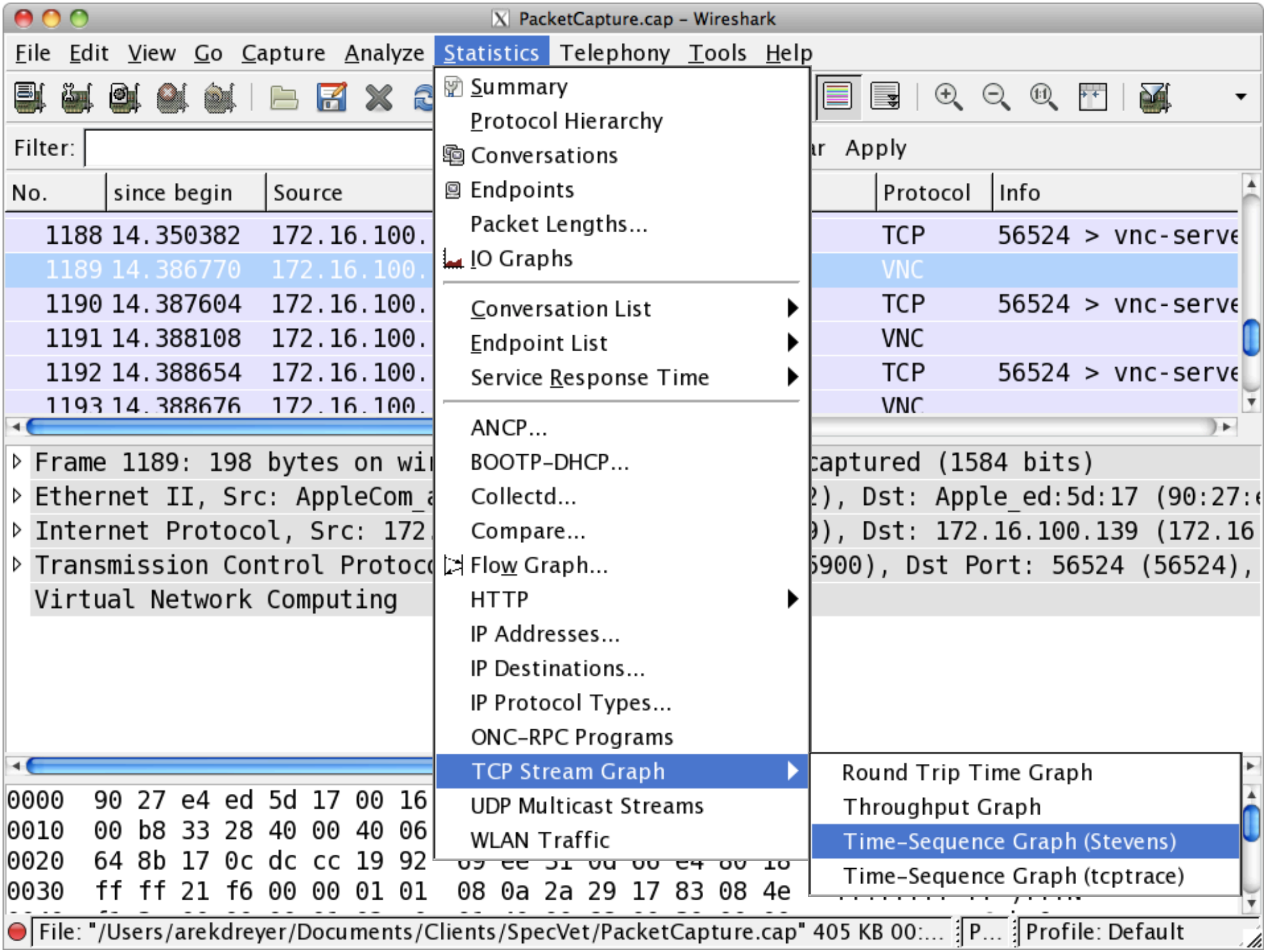

BindAttempt2.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: (ip.addr eq 172.16.16.221 and ip.addr eq 172.
Expression... Clear Apply
No. since begin Source Destination Protocol Info
682 134.488960 172.16.16.11 172.16.16.221 KRB5 AS-REQ
683 134.532820 172.16.16.221 172.16.16.11 KRB5 KRB Error: KRB5KRB_ERR_R
Checksum: 0xd068 [correct]
Kerberos KRB-ERROR
Pvno: 5
MSG Type: KRB-ERROR (30)
stime: 2010-09-30 18:47:29 (UTC)
susec: 61608
error_code: KRB5KRB_ERR_RESPONSE_TOO_BIG (52)
Realm: SSH22.COM
Server Name (Unknown): krbtgt/SSH22.COM
0040 30 39 33 30 31 38 34 37 32 39 5a a5 05 02 03 00 09301847 292.....
0050 f0 a8 a6 03 02 01 34 a9 0b 1b 09 53 53 48 32 32 ......4. ...SSH22
0060 2e 43 4f 4d aa 1e 30 1c a0 03 02 01 00 a1 15 30 .COM..0. 0
0070 13 1b 06 6b 72 62 74 67 74 1b 09 53 53 48 32 32 ...krbtg t..SSH22
0080 2e 43 4f 4d .COM
Kerberos error code (kerberos.error_code), 1 byte
P...
Profile: Default

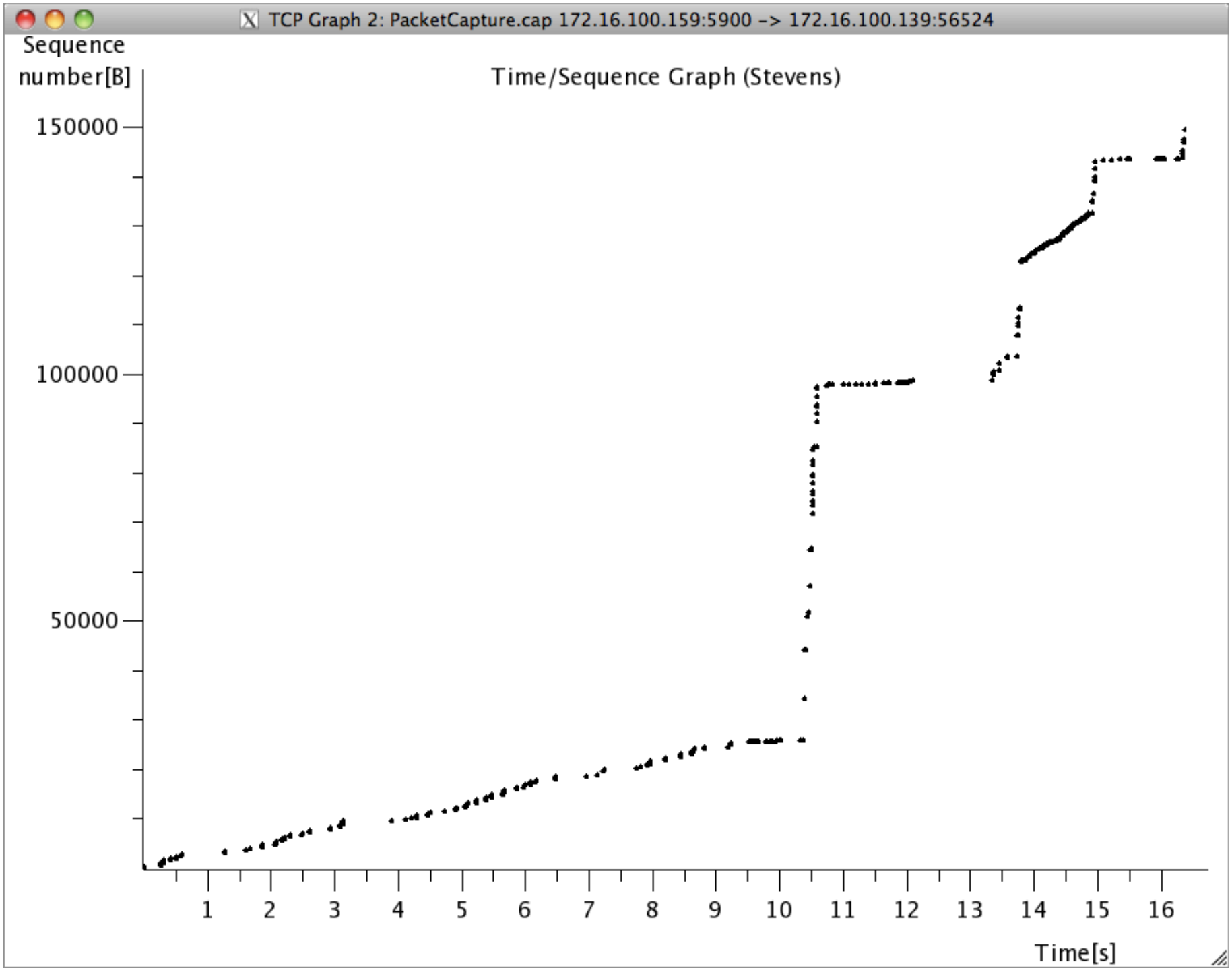

BindAttempt2.pcap
Open
Capture
Jump
Find
Select a filter predicate
Filter
Id Source Destination Captured L... Packet Length Protocol Information Date Rece
681 172.16.16.11 172.16.16.221 66 66 TCP 49169 -> MSILS ([ACK], Seq=4086696698, Ack=6164540228,... 2010-09
682 172.16.16.11 172.16.16.221 285 285 UDP 58887 > KERBEROS 2010-09
683 172.16.16.221 172.16.16.11 132 132 UDP KERBEROS > 58887 2010-09
684 172.16.16.11 172.16.16.221 78 78 TCP 49170 -> KERBEROS ([SYN], Seq=1209183088, Ack=4294967... 2010-09
685 172.16.16.221 172.16.16.11 74 74 TCP KERBEROS -> 49170 ([ACK, SYN], Seq=1607396224, Ack=550... 2010-09
686 172.16.16.11 172.16.16.221 66 66 TCP 49170 -> KERBEROS ([ACK], Seq=1209183089, Ack=5902363... 2010-09
687 172.16.16.11 172.16.16.221 313 313 TCP 49170 -> KERBEROS ([ACK, PUSH], Seq=1209183089, Ack=59... 2010-09
Detail Value
Packet
Ethernet-Header
IP-Header
UDP-Header
Payload
Length 90 bytes
Headerlength: 90 bytes, Data follows:
00000 7e 58 30 56 a0 03 02 01 05 a1 03 02 01 1e a4 11 ~X0V.....
00010 18 0f 32 30 31 30 30 39 33 30 31 38 34 37 32 39 ..20100930184729
00020 5a a5 05 02 03 00 f0 a8 a6 03 02 01 34 a9 0b 1b Z.....4...
00030 09 53 53 48 32 32 2e 43 4f 4d aa 1e 30 1c a0 03 .SSH22.COM..0...
00040 02 01 00 a1 15 30 13 1b 06 6b 72 62 74 67 74 1b .....0...krbtgt.
00050 09 53 53 48 32 32 2e 43 4f 4d .SSH22.COM
Fileformat: 2.4 Snaplength: 65535 bytes Linktype: ETHERNET (DLT_EN10MB) Filesize: 415164 bytes Packets: 1076 of 1076 (1 selected)


BindAttempt2.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Enabled Protocols... Shift+Ctrl+E
Decode As...
User Specified Decodes...
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Expert Info
Expert Info Composite
Conversation Filter
Filter:
Apply
No. since begin Source Protocol Info
22 3.840777 TCP 49165 > ldap [ACK
23 3.840873 LDAP searchRequest(3)
24 3.845809 LDAP searchResDone(3)
25 3.845857 TCP 49165 > ldap [ACK
26 3.845953 LDAP searchRequest(4)
27 3.846408 LDAP searchResDone(4)
Frame 24: 240 bytes
Ethernet II, Src: Cad
Internet Protocol, Sr
Transmission Control
Lightweight Directory
0000 00 23 32 94 6d 4c 08 00 27 fb 46 e5 08 00 45 00 .#2.mL.. '.F...E.
0010 00 e2 3f 2a 40 00 80 06 41 e3 ac 10 10 dd ac 10 ..?*@... A.....
0020 10 0b 01 85 c0 0d 84 9e f1 72 26 fc 75 b6 80 18 ..... .r&.u...
0030 01 03 83 37 00 00 01 01 08 0a 00 67 69 40 33 dc ...7.... ...gi@3.
File: "/Users/arekdreyer/Desktop/BindAttempt2.pcap" 405 KB 00:07:06
P...
Profile: Default


Follow TCP Stream
...objectclass0?..supportedSASLMechanisms..namingContexts..dnsHostName..krbName0....J...
...90.......namingContexts1.......DC=SSH22,DC=COM.
ration,DC=SSH22,DC=COM.*CN=Schema,CN=Configuration,DC=SSH22,DC=COM.!
nsZones,DC=SSH22,DC=COM.!
nsZones,DC=SSH22,DC=COM0....I..supportedSASLMechanisms1....*..GSSAPI.
..EXTERNAL.
0....#..dnsHostName1.......DC01.SSH22.COM0........e.....
.cj..DC=SSH22,DC=COM
..9.!..objectclass..organizationalUnit....ou..macosxodconfig0
ion0........e.....
000004DC: LdapErr: DSID-0C0906DD, comment: In order to perform this operation a
bind must be completed on the connection., data 0, v1771.0.....c{.
ration,DC=SSH22,DC=COM
ve As
Print
Entire conversation (2797 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Filter Out This Stream
Close


BindAttempt2.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: tcp.stream eq 5
Expression... Clear Apply
No. since begin Source Destination Protocol Info
21 3.840672 172.16.16.221 172.16.16.11 LDAP searchResDone(2)
22 3.840777 172.16.16.11 172.16.16.221 TCP 49165 > ldap [ACK
23 3.840873 172.16.16.11 172.16.16.221 LDAP searchRequest(3)
24 3.845809 172.16.16.221 172.16.16.11 LDAP searchResDone(3)
25 3.845857 172.16.16.11 172.16.16.221 TCP 49165 > ldap [ACK
26 3.845953 172.16.16.11 172.16.16.221 LDAP searchRequest(4)
Frame 24: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits)
Ethernet II, Src: CadmusCo_fb:46:e5 (08:00:27:fb:46:e5), Dst: Apple_94:6d:4c (00:23:
Internet Protocol, Src: 172.16.16.221 (172.16.16.221), Dst: 172.16.16.11 (172.16.16.
Transmission Control Protocol, Src Port: ldap (389), Dst Port: 49165 (49165), Seq: 5
Lightweight Directory Access Protocol
0000 00 23 32 94 6d 4c 08 00 27 fb 46 e5 08 00 45 00 .#2.mL.. '.F...E.
0010 00 e2 3f 2a 40 00 80 06 41 e3 ac 10 10 dd ac 10 ..?*@... A.......
0020 10 0b 01 85 c0 0d 84 9e f1 72 26 fc 75 b6 80 18 .... .r&.u...
0030 01 03 83 37 00 00 01 01 08 0a 00 67 69 40 33 dc ...7.... ...gi@3.
File: "/Users/arekdreyer/Desktop/BindAttempt2.pcap" 405 KB 00:07:06
P...
Profile: Default


PacketCapture.cap – Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Apply
No. since begin Source Protocol Info
1188 14.350382 172.16.100. TCP 56524 > vnc-serve
1189 14.386770 172.16.100. VNC
1190 14.387604 172.16.100. TCP 56524 > vnc-serve
1191 14.388108 172.16.100. VNC
1192 14.388654 172.16.100. TCP 56524 > vnc-serve
1193 14.388676 172.16.100. VNC
Frame 1189: 198 bytes on wi captured (1584 bits)
Ethernet II, Src: AppleCom_a 2), Dst: Apple_ed:5d:17 (90:27:e
Internet Protocol, Src: 172. 9), Dst: 172.16.100.139 (172.16
Transmission Control Protoc 5900), Dst Port: 56524 (56524),
Virtual Network Computing
0000 90 27 e4 ed 5d 17 00 16
0010 00 b8 33 28 40 00 40 06
0020 64 8b 17 0c dc cc 19 92
0030 ff ff 21 f6 00 00 01 01 08 0a 2a 29 17 83 08 4e
Summary
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths...
IO Graphs
Conversation List
Endpoint List
Service Response Time
ANCP...
BOOTP-DHCP...
Collectd...
Compare...
Flow Graph...
HTTP
IP Addresses...
IP Destinations...
IP Protocol Types...
ONC-RPC Programs
TCP Stream Graph
UDP Multicast Streams
WLAN Traffic
Round Trip Time Graph
Throughput Graph
Time-Sequence Graph (Stevens)
Time-Sequence Graph (tcptrace)
File: "/Users/arekdreyer/Documents/Clients/SpecVet/PacketCapture.cap" 405 KB 00:...
P...
Profile: Default


TCP Graph 2: PacketCapture.cap 172.16.100.159:5900 -> 172.16.100.139:56524
Sequence number[B]
Time/Sequence Graph (Stevens)
150000
100000
50000
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Time[s]

Wireshark Quirks

- X11
- Open window is funny

Commercial

- Many out there
- Additional automatic analysis

Packet Review

- Capture
- Analyze

Filesystem Activity

- `lsof`
- `fs_usage`
- fseventer

`lsof`

- list of open files
- snapshot at the time you start lsof
- Demo: Quicktime Screen Capture

`lsof` options

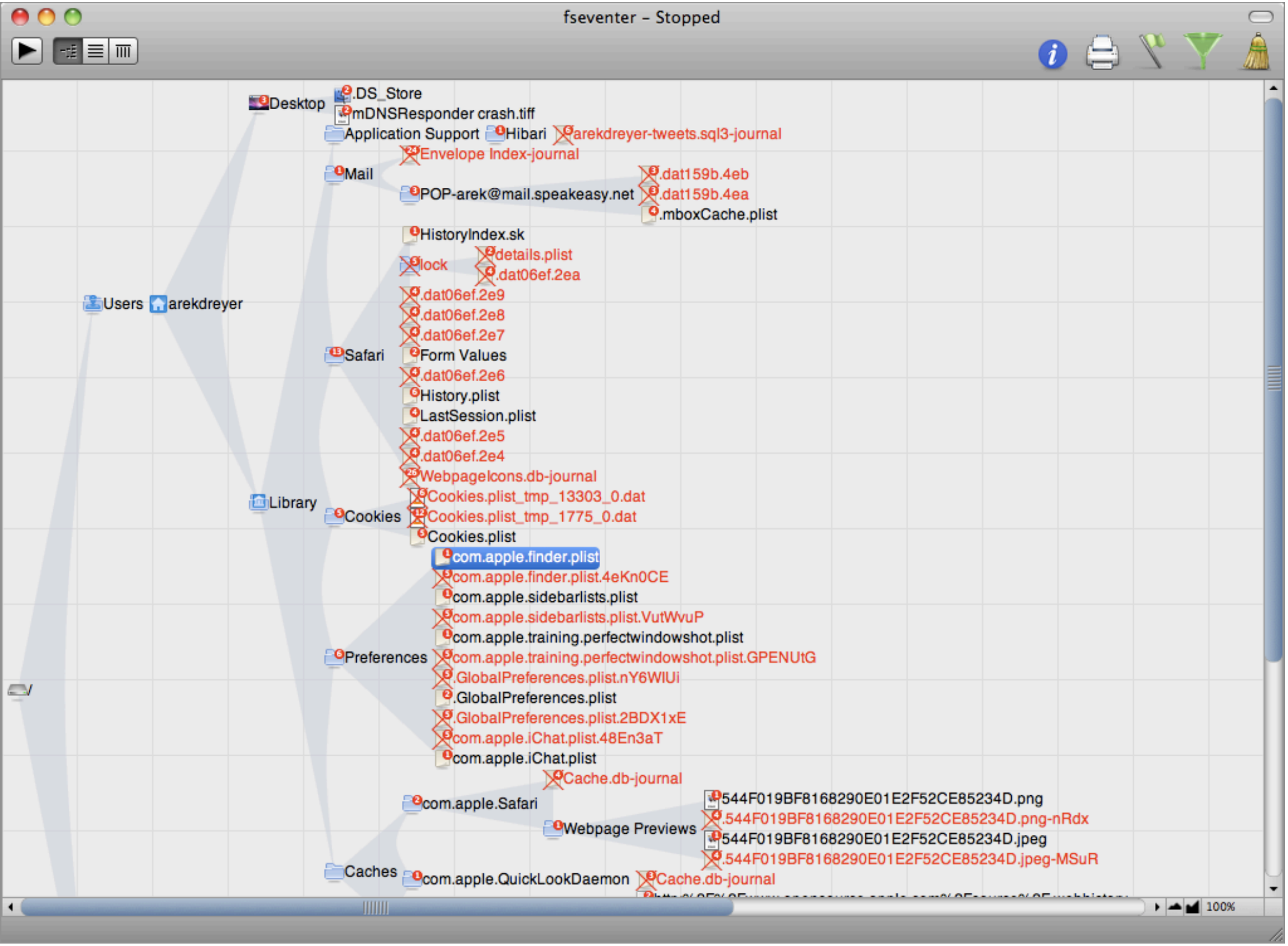
- -u username or user ID
- -p processid
- name of a path or file
  - lsof /etc/hosts

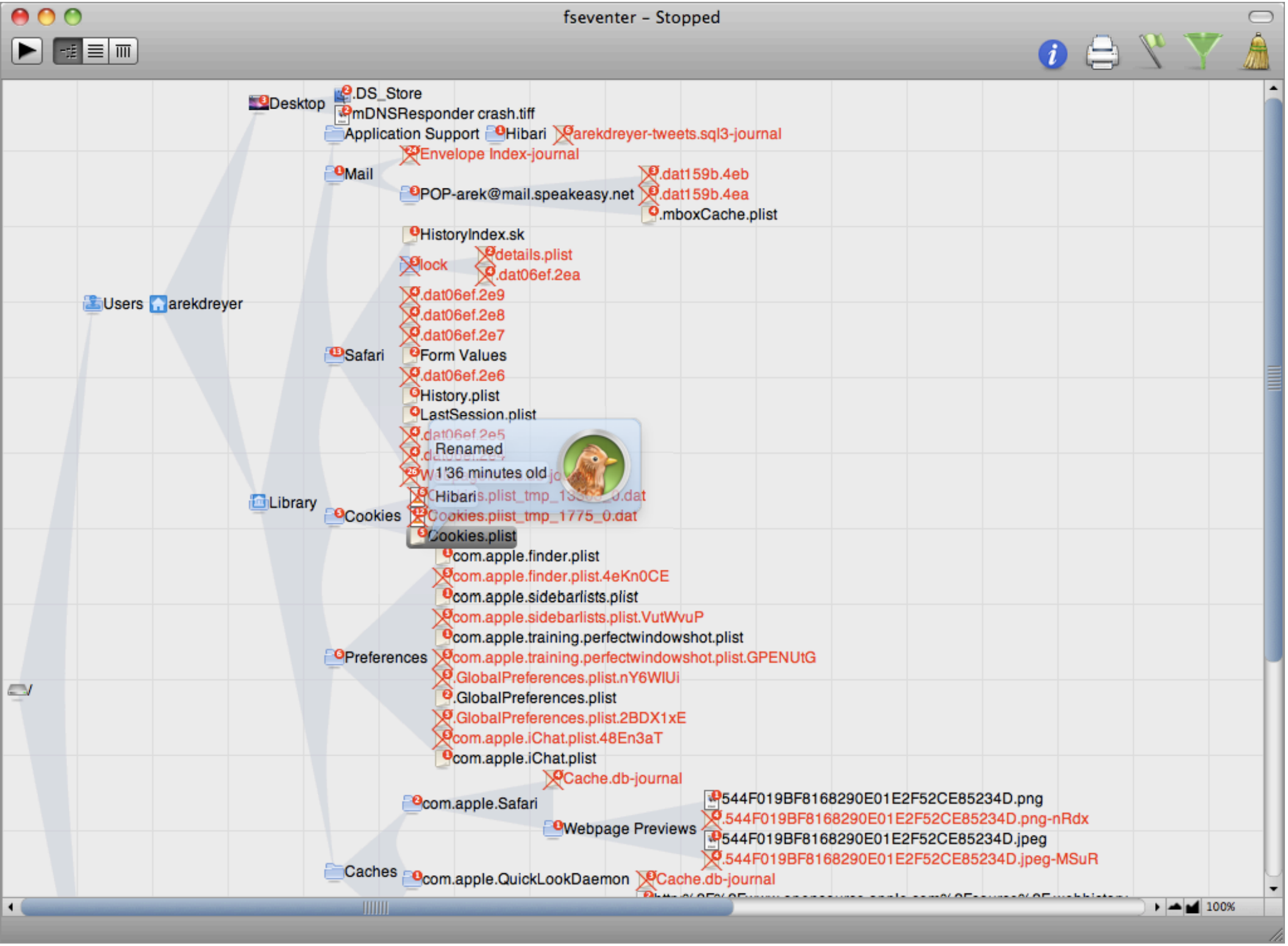
fs_usage

- filesystem activity
  - system calls
  - page faults
- -f network | filesys | cachehit
- Huge stream of information

fseventer

- Commercial software
- uses fseventsd


fseventer - Stopped
Desktop
.DS_Store
mDNSResponder crash.tiff
Application Support
Hibari
arekdreyer-tweets.sql3-journal
Envelope Index-journal
Mail
.dat159b.4eb
POP-arek@mail.speakeasy.net
.dat159b.4ea
.mboxCache.plist
HistoryIndex.sk
details.plist
lock
.dat06ef.2ea
Users
arekdreyer
.dat06ef.2e9
.dat06ef.2e8
.dat06ef.2e7
Safari
Form Values
.dat06ef.2e6
History.plist
LastSession.plist
.dat06ef.2e5
.dat06ef.2e4
WebpageIcons.db-journal
Library
Cookies.plist_tmp_13303_0.dat
Cookies
Cookies.plist_tmp_1775_0.dat
Cookies.plist
com.apple.finder.plist
com.apple.finder.plist.4eKn0CE
com.apple.sidebarlists.plist
com.apple.sidebarlists.plist.VutWvuP
com.apple.training.perfectwindowshot.plist
Preferences
com.apple.training.perfectwindowshot.plist.GPENUtG
.GlobalPreferences.plist.nY6WlUi
/
.GlobalPreferences.plist
.GlobalPreferences.plist.2BDX1xE
com.apple.iChat.plist.48En3aT
com.apple.iChat.plist
Cache.db-journal
com.apple.Safari
544F019BF8168290E01E2F52CE85234D.png
.544F019BF8168290E01E2F52CE85234D.png-nRdx
Webpage Previews
544F019BF8168290E01E2F52CE85234D.jpeg
.544F019BF8168290E01E2F52CE85234D.jpeg-MSuR
Caches
com.apple.QuickLookDaemon
Cache.db-journal
100%


fseventer - Stopped
Desktop
.DS_Store
mDNSResponder crash.tiff
Application Support
Hibari
arekdreyer-tweets.sql3-journal
Envelope Index-journal
Mail
.dat159b.4eb
POP-arek@mail.speakeasy.net
.dat159b.4ea
.mboxCache.plist
HistoryIndex.sk
details.plist
lock
.dat06ef.2ea
Users
arekdreyer
.dat06ef.2e9
.dat06ef.2e8
.dat06ef.2e7
Safari
Form Values
.dat06ef.2e6
History.plist
LastSession.plist
Renamed
1'36 minutes old
Library
Hibari
Cookies
Cookies.plist_tmp_1775_0.dat
Cookies.plist
com.apple.finder.plist
com.apple.finder.plist.4eKn0CE
com.apple.sidebarlists.plist
com.apple.sidebarlists.plist.VutWvuP
com.apple.training.perfectwindowshot.plist
Preferences
com.apple.training.perfectwindowshot.plist.GPENUtG
.GlobalPreferences.plist.nY6WlUi
.GlobalPreferences.plist
.GlobalPreferences.plist.2BDX1xE
com.apple.iChat.plist.48En3aT
com.apple.iChat.plist
Cache.db-journal
com.apple.Safari
544F019BF8168290E01E2F52CE85234D.png
.544F019BF8168290E01E2F52CE85234D.png-nRdx
Webpage Previews
544F019BF8168290E01E2F52CE85234D.jpeg
.544F019BF8168290E01E2F52CE85234D.jpeg-MSuR
Caches
com.apple.QuickLookDaemon
Cache.db-journal
100%

Filesystem Activity Recap

- `lsof`
- `fs_usage`
- fseventer

DTrace

- Dynamic Tracing Facility
- Observational toolset
- Low impact
- Instruments.app and DTrace Toolkit

Solaris Performance and Tools

DTRACE AND MDB TECHNIQUES FOR SOLARIS 10 AND OPENSOLARIS

Richard McDougall, Jim Mauro, and Brendan Gregg
Foreword by Bryan Cantrill

Instruments

- GUI
- I like using dtrace over SSH

DTrace Toolkit

- man -k dtrace
- Two basic kinds of scripts
  - instantaneous feedback
  - aggregative summaries
- Write your own

Instantaneous

- `man -k dtrace | grep snoop`
  - `execsnoop`
  - `filebyproc.d`
  - `iosnoop`
  - `kill.d`
  - `opensnoop`
- `dtruss`

Aggregative

- Just a few examples
  - iotop
  - pathopens
  - pidpersec.d

spindump

- `sudo spindump`
- review /tmp/spindump.[n.]txt

Troubleshooting Tools

- DNS
- Packet Analysis
- File Use Analysis
- DTrace
- `spindump`

Advanced Troubleshooting Tools

arek@arekdreyer.com

MacSysAdmin 2010