

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

---

Wireshark ağ trafik analiz aracını ve faydalı olabilecek araçları kullanarak **uygulama1.pcap** dosyasını inceleyiniz ve aşağıdaki soruları yanıtlayınız:

- Ann kullanıcısının e-posta adresi nedir?
- Ann kullanıcısının e-posta parola nedir?
- Ann'in e-posta gönderdiği adres nedir?
- Ann'in arkadaşının gönderdiği e-postada yanında getirmesini söylediği iki şey nedir?
- Ann'in gönderdiği eposta'nın ekinde gönderilen dosyanın adı nedir?
- E-posta ekinde gönderilen dosyanın MD5 ve SHA1 değeri nedir?
- Ekte gönderilen belgeye göre buluşma yeri hangi ülke ve şehirdedir?
- Ekte gönderilen belge içindeki resmin MD5 ve SHA1 değeri nedir?

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

evidence02.pcap dosyası

The image shows a Wireshark network traffic analysis interface. The top toolbar includes icons for file operations, search, and display filters. Below the toolbar is a search bar with the text "Apply a display filter ... <%%/>" and a button labeled "Expression...".

The main packet list table has the following columns: No., Time, Source, Destination, Protocol, Length, and Info. It contains 13 rows of data, including ARP, NTP, Syslog, and TCP packets.

The detailed view pane at the bottom shows the structure of the selected packet (No. 113). It includes the following information:

- Frame 113: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
- Ethernet II, Src: 00:21:70:4d:4f:ae, Dst: 00:0c:29:9b:ee:14
- Internet Protocol Version 4, Src: 192.168.1.159, Dst: 64.12.102.142
- Transmission Control Protocol, Src Port: 1038, Dst Port: 587, Seq: 0, Len: 0
  - Source Port: 1038
  - Destination Port: 587
  - [Stream index: 1]
  - [TCP Segment Len: 0]
  - Sequence number: 0 (relative sequence number)
  - Acknowledgment number: 0
  - Header Length: 28 bytes
  - Flags: 0x002 (SYN)
  - Window size value: 64240
  - [Calculated window size: 64240]

The status bar at the bottom indicates: Frame (frame), 62 bytes | Packets: 572 - Displayed: 572 (100.0%) - Load time: 0:0.14 | Profile: Default

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

Wireshark · Conversations · Odev2

Ethernet · 6   IPv4 · 6   IPv6   **TCP · 2**   UDP · 7

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.1.159	1036	64.12.102.142	587	36	3958	14	2259	0	0
192.168.1.159	1038	64.12.102.142	587	454	310 k	221	297 k	0	0

☐ Name resolution   ☐ Limit to display filter   ☐ Absolute start time   Conversation Types ▾

Help   Copy ▾   Follow Stream...   Graph...   Close

Wireshark · Conversations · Odev2

Ethernet · 6   IPv4 · 6   IPv6   **TCP · 2**   UDP · 7

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.1.159	1036	64.12.102.142	587	36	3958	14	2259	0	0
192.168.1.159	1038	64.12.102.142	587	454	310 k	221	297 k	0	0

☐ Name resolution   ☐ Limit to display filter   ☐ Absolute start time   Conversation Types ▾

Help   Copy ▾   Follow Stream...   Graph...   Close

Apply as Filter ▸  
Prepare a Filter ▸  
Find ▸  
Colorize ▸

Selected ▸  
Not Selected ▸  
...and Selected ▸  
...or Selected ▸  
...and not Selected ▸  
...or not Selected ▸

A ↔ B  
A → B  
B → A  
A ↔ Any  
A → Any  
Any → A  
Any ↔ B  
Any → B  
B → Any

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

Odev2.pcap

ip.addr==192.168.1.159 && tcp.port==1038 && ip.addr==64.12.102.142 && tcp.port==587

No.	Time	Source	Destination	Protocol	Length	Info
113	242.7952...	192.168.1.1...	64.12.102.1...	TCP	62	1038->587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
114	242.9063...	64.12.102.1...	192.168.1.1...	TCP	58	587->1038 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
115	242.9067...	192.168.1.1...	64.12.102.1...	TCP	54	1038->587 [ACK] Seq=1 Ack=1 Win=64240 Len=0
116	243.0780...	64.12.102.1...	192.168.1.1...	SMTP	134	S: 220 220.10.10.10 SMTP service ready
117	243.0790...	192.168.1.1...	64.12.102.1...	SMTP	70	C: EH 64.12.102.142
118	243.0794...	64.12.102.1...	192.168.1.1...	TCP	54	587->1038 [ACK] Seq=0 Ack=1 Win=64240 Len=0
119	243.1913...	64.12.102.1...	192.168.1.1...	SMTP	305	S: 250 250.10.10.10 SMTP service ready
120	243.1930...	192.168.1.1...	64.12.102.1...	SMTP	66	C: A
121	243.1935...	64.12.102.1...	192.168.1.1...	TCP	54	587->1038 [ACK] Seq=0 Ack=1 Win=64240 Len=0
122	243.3014...	64.12.102.1...	192.168.1.1...	SMTP	72	S: 350 350.10.10.10 SMTP service ready
123	243.3023...	192.168.1.1...	64.12.102.1...	SMTP	80	C: U
124	243.3028...	64.12.102.1...	192.168.1.1...	TCP	54	587->1038 [ACK] Seq=0 Ack=1 Win=64240 Len=0
125	243.4133...	64.12.102.1...	192.168.1.1...	SMTP	72	S: 350 350.10.10.10 SMTP service ready
126	243.4142...	192.168.1.1...	64.12.102.1...	SMTP	68	C: F
127	243.4147...	64.12.102.1...	192.168.1.1...	TCP	54	587->1038 [ACK] Seq=0 Ack=1 Win=64240 Len=0
128	243.5369...	64.12.102.1...	192.168.1.1...	SMTP	85	S: 250 250.10.10.10 SMTP service ready
129	243.5405...	192.168.1.1...	64.12.102.1...	SMTP	87	C: M
130	243.5410...	64.12.102.1...	192.168.1.1...	TCP	54	587->1038 [ACK] Seq=0 Ack=1 Win=64240 Len=0

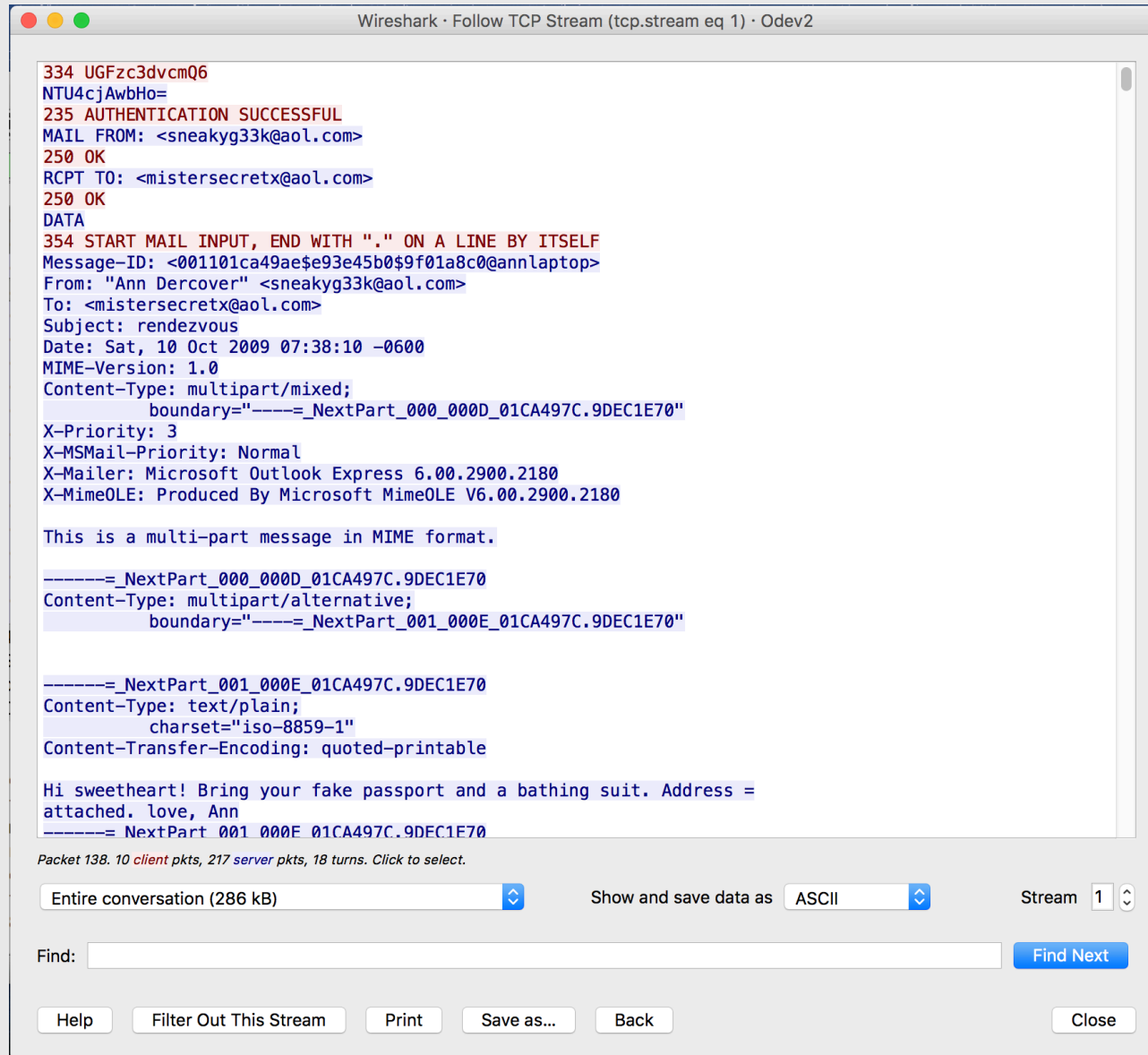
Frame 116: 134 bytes on wire (1072 bits), 134 bytes captured (1072 b)

- Ethernet II, Src: 00:0c:29:9b:ee:14, Dst: 00:21:70:4d:4f:ae
- Internet Protocol Version 4, Src: 64.12.102.142, Dst: 192.168.1.159
- Transmission Control Protocol, Src Port: 587, Dst Port: 1038, Seq: 1
  - Source Port: 587
  - Destination Port: 1038
  - [Stream index: 1]
  - [TCP Segment Len: 80]
  - Sequence number: 1 (relative sequence number)
  - [Next sequence number: 81 (relative sequence number)]
  - Acknowledgment number: 1 (relative ack number)
  - Header Length: 20 bytes
  - Flags: 0x018 (PSH, ACK)
  - Window size value: 64240

Frame (frame), 134 bytes

Packets: 572 · Displayed: 454 (79.4%) · Load time: 0:0.50 Profile: Default

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi



```
334 UGFzc3dvcmQ6
NTU4cjAwbHo=
235 AUTHENTICATION SUCCESSFUL
MAIL FROM: <sneakyg33k@aol.com>
250 OK
RCPT TO: <mistersecretx@aol.com>
250 OK
DATA
354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
Message-ID: <001101ca49ae$e93e45b0$9f01a8c0@annlaptop>
From: "Ann Dercover" <sneakyg33k@aol.com>
To: <mistersecretx@aol.com>
Subject: rendezvous
Date: Sat, 10 Oct 2009 07:38:10 -0600
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="=====_NextPart_000_000D_01CA497C.9DEC1E70"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

=====_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: multipart/alternative;
    boundary="=====_NextPart_001_000E_01CA497C.9DEC1E70"

=====_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Hi sweetheart! Bring your fake passport and a bathing suit. Address =
attached. love, Ann
=====_NextPart_001_000E_01CA497C.9DEC1E70
```

Packet 138. 10 client pkts, 217 server pkts, 18 turns. Click to select.

Entire conversation (286 kB) Show and save data as ASCII Stream 1

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Odev2

```
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

-----=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: multipart/alternative;
        boundary="-----=_NextPart_001_000E_01CA497C.9DEC1E70"

-----=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Hi sweetheart! Bring your fake passport and a bathing suit. Address =
attached. love, Ann
-----=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2900.2853" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3DArial size=3D2>Hi sweetheart! Bring your fake passport =
and a=20
bathing suit. Address attached. love, Ann</FONT></DIV></BODY></HTML>

-----=_NextPart_001_000E_01CA497C.9DEC1E70--
```

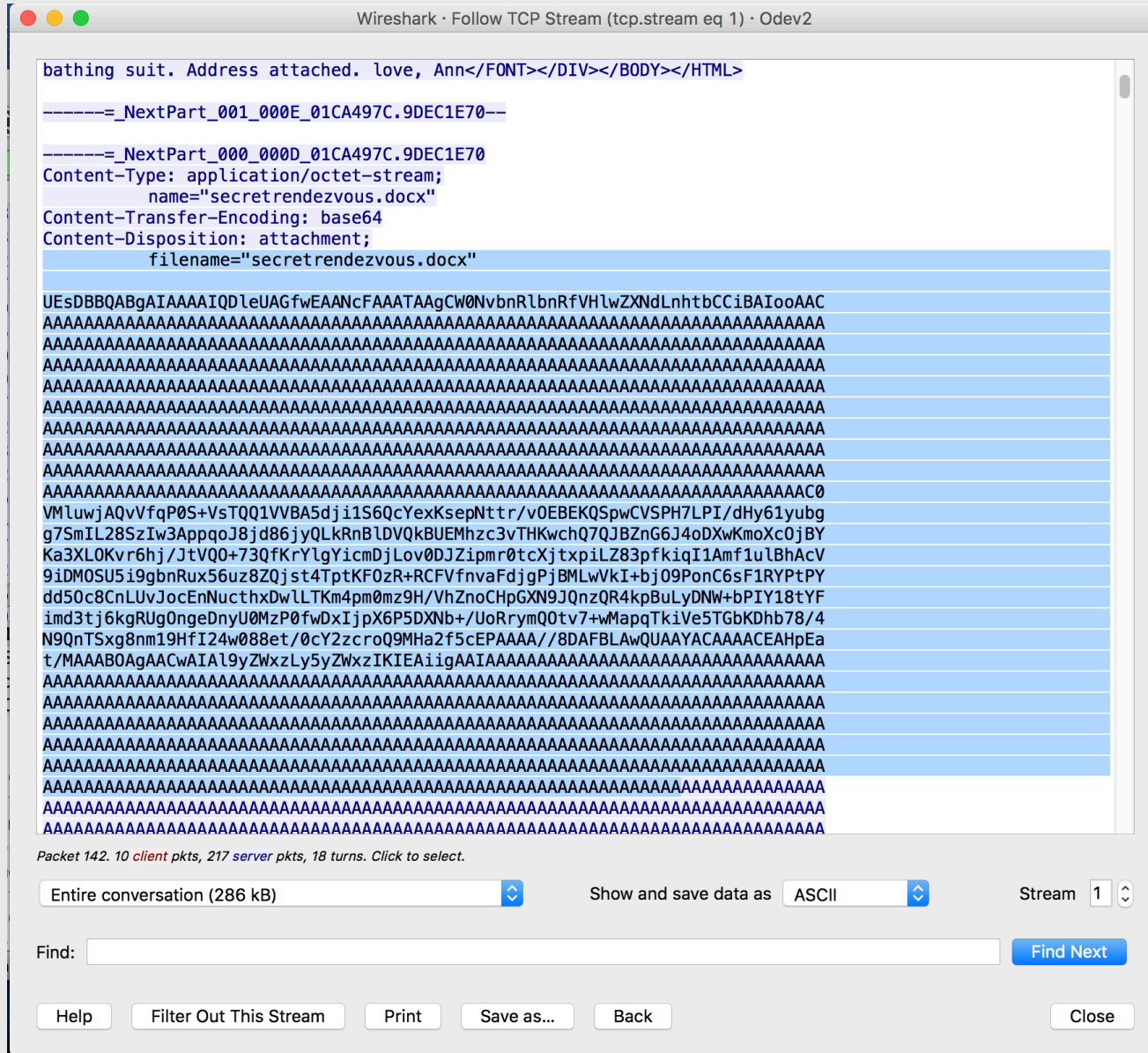
10 client pkts, 217 server pkts, 18 turns.

Entire conversation (286 kB) Show and save data as ASCII Stream 1

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

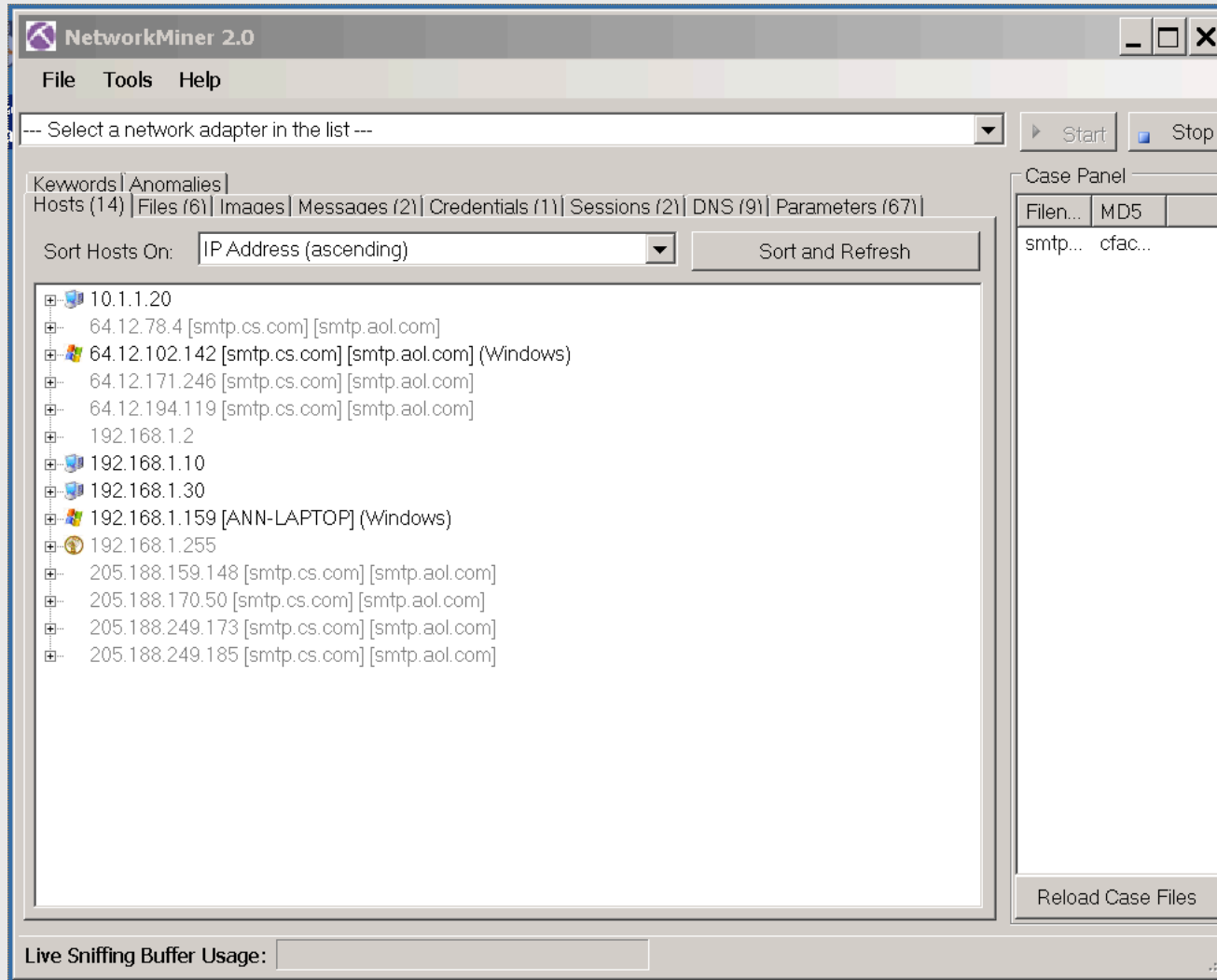
## Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi





# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

## ■ Alternatif Çözüm: Network Miner





# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

## ■ Alternatif Çözüm: Network Miner

The screenshot displays the NetworkMiner 2.0 application window. The interface includes a menu bar (File, Tools, Help), a network adapter selection dropdown, and Start/Stop buttons. The main area is divided into several panes:

- Hosts (14) | Files (6) | Images | Messages (2) | Credentials (1) | Sessions (2) | DNS (9) | Parameters (67) | Keywords | Anomalies**: A tabbed interface with 'Messages (2)' selected.
- actPhrase**: A dropdown menu with 'Clear' and 'Apply' buttons.
- Table 1: Message Details**

Frame nr.	Source host	Destination
80	192.168.1.159 [ANN-LAPTOP] (Windo...	64.12.1
557	192.168.1.159 [ANN-LAPTOP] (Windo...	64.12.1

- Table 2: Message Headers**

Attribute	Value
Message-ID	<001101ca49ae\$e93e45b0\$9f01a8c0...
From	"Ann Dercover" <sneakyg33k@aol.com>
To	<mistersecretx@aol.com>
Subject	rendezvous
Date	Sat, 10 Oct 2009 07:38:10 -0600
MIME-Vers...	1.0
Content-Ty...	multipart/mixed
boundary	-----_NextPart_000_000D_01CA497C....
X-Priority	3
X-MSMail...	Normal
X-Mailer	Microsoft Outlook Express 6.00.2900.2...
X-MimeOLE	Produced By Microsoft MimeOLE V6.0...
charset	iso-8859-1
Content-Tr...	quoted-printable

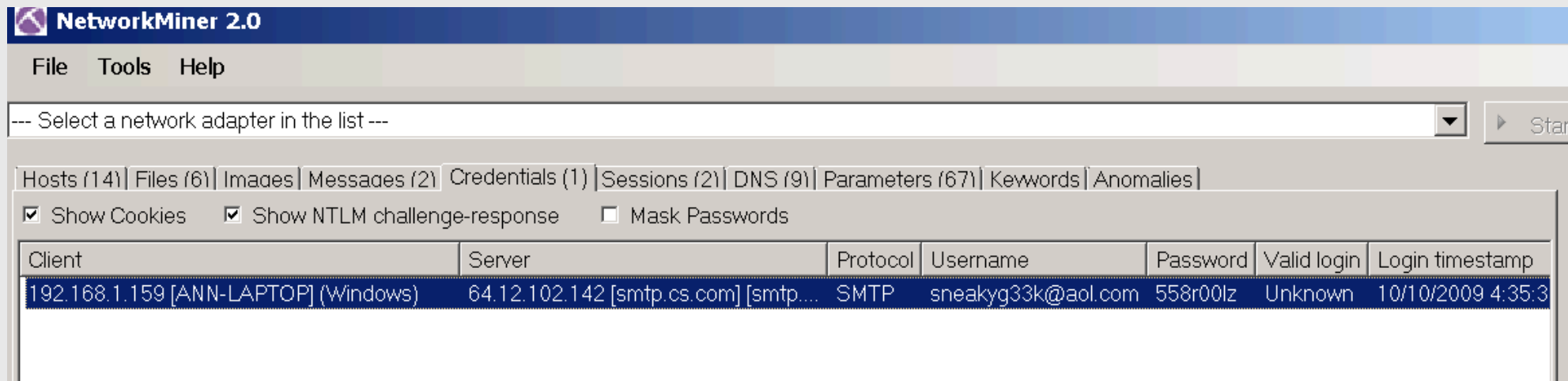
- Windows-1252 Western European (Windows)**: A text area showing the message body: "Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann".
- Table 3: Attachments**

Attachement	Size
rendezvous[3].html	402 B
secretrendezvous[3].docx	207 438 B
rendezvous[3].eml	285 628 B

- Case**: A sidebar on the right with 'Filen...' and 'MD' buttons, and a 'Reload' button at the bottom.
- Live Sniffing Buffer Usage:**: A progress bar at the bottom of the window.

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

## ■ Alternatif Çözüm: Network Miner



The screenshot shows the NetworkMiner 2.0 application window. The title bar is blue with the text "NetworkMiner 2.0". Below the title bar is a menu bar with "File", "Tools", and "Help". A dropdown menu is open, showing "--- Select a network adapter in the list ---". Below the menu bar is a toolbar with buttons for "Hosts (14)", "Files (6)", "Images", "Messages (2)", "Credentials (1)", "Sessions (2)", "DNS (9)", "Parameters (67)", "Keywords", and "Anomalies". There are also checkboxes for "Show Cookies", "Show NTLM challenge-response", and "Mask Passwords". Below the toolbar is a table with the following columns: Client, Server, Protocol, Username, Password, Valid login, and Login timestamp. The table contains one row of data.

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.1.159 [ANN-LAPTOP] (Windows)	64.12.102.142 [smtp.cs.com] [smtp....	SMTP	sneakyg33k@aol.com	558r00lz	Unknown	10/10/2009 4:35:3

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

## ■ Alternatif Çözüm: Network Miner

The screenshot displays the NetworkMiner 2.0 application window. The interface includes a menu bar (File, Tools, Help) and a toolbar with a dropdown menu for selecting a network adapter. The main window is divided into several panes. The left pane shows a list of network traffic items, including Hosts (14), Files (6), Images, Messages (2), Credentials (1), Sessions (2), DNS (9), Parameters (67), Keywords, and Anomalies. The middle pane displays a table of network traffic data with columns for Frame nr., Source host, and Destination. The right pane shows the details of a selected message, including its attributes and content.

NetworkMiner 2.0

File Tools Help

--- Select a network adapter in the list --- Start

Hosts (14) Files (6) Images Messages (2) Credentials (1) Sessions (2) DNS (9) Parameters (67) Keywords Anomalies

actPhrase Clear Apply

Frame nr.	Source host	Destination
80	192.168.1.159 [ANN-LAPTOP] (Wind...	64.12.1
557	192.168.1.159 [ANN-LAPTOP] (Wind...	64.12.1

Attribute	Value
Message-ID	<001101ca49ae\$e93e45b0\$9f01a8c0...
From	"Ann Dercover" <sneakyg33k@aol.com>
To	<mistersecretx@aol.com>
Subject	rendezvous
Date	Sat, 10 Oct 2009 07:38:10 -0600
MIME-Vers...	1.0
Content-Ty...	multipart/mixed
boundary	-----=_NextPart_000_000D_01CA497C....
X-Priority	3
X-MSMail...	Normal
X-Mailer	Microsoft Outlook Express 6.00.2900.2...
X-MimeOLE	Produced By Microsoft MimeOLE V6.0...
charset	iso-8859-1
Content-Tr...	quoted-printable

Windows-1252 Western European (Windows)

Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

Attachement	Size
rendezvous[3].html	402 B
secretrendezvous[3].docx	207 438 B
rendezvous[3].eml	285 628 B

# Uygulama 1: Örnek Ağ Analizi - SMTP İncelemesi

## ■ Alternatif Çözüm: Network Miner

