MONOSEK

LIST OF EXPERIMENTS

Nihon Communication Solutions Pvt. Ltd.
#35, 2nd Floor, 16th Cross, 8th Main
Malleshwaram, Bangalore – 560055
www.ncs-in.com
Phone: +91 - 80 – 41204434 Fax: +91 - 80 - 23561866

Subject to change

Document ID: monosek/mkt/tech/20140127

EXPERIMENT NAMES

- EXPT_1_GENERAL_ANALYSIS
- EXPT_2_TCP_ANALYSIS
- EXPT_3_UDP_ANALYSIS
- EXPT_4_SMTP_ANALYSIS
- EXPT_5_POP3_ANALYSIS
- EXPT_6_HTTP_ANALYSIS
- EXPT_7_LIST_ALL_CLIENTS_IP
- EXPT_8_LIST_IP_USING_HTTP
- EXPT_9_TCP_SEQUENCE_FLOW
- EXPT_10_VOIP_FLOW
- EXPT_11_GENERAL_ANALYSIS-MULTI
- EXPT_12_TCP_ANALYSIS-MULTI
- EXPT_13_UDP_ANALYSIS-MULTI
- EXPT_14_SHOW_LAYERED_PKTS

ABOUT EXPERIMENTS

Packet Analysis

The **Experiment 1** shows the following details for every IPV4 packet analyzed using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Packet Size
- Packet Type
- Source IP Address
- Destination IP Address
- Application protocol
- Content Type field and corresponding Content Type string.

383	72	TCP	192.168.1.134	164.46.82.116	Extended SMTP
386	66	TCP	192.168.1.17	94.75.236.122	www-http
387	116	TCP	164.46.82.116	192.168.1.134	Extended SMTP
388	66	TCP	192.168.1.134	164.46.82.116	Extended SMTP
389	716	TCP	192.168.1.134	164.46.82.116	Extended SMTP
390	69	TCP	192.168.1.134	164.46.82.116	Extended SMTP
391	66	TCP	94.75.236.122	192.168.1.17	www-http
392	54	TCP	192.168.1.17	94.75.236.122	www-http
393	54	TCP	192.168.1.17	94.75.236.122	www-http
394	803	TCP	192.168.1.17	74.125.236.132	www-http
395	54	TCP	74.125.236.132	192.168.1.17	www-http
399	650	TCP	74.125.236.132	192.168.1.17	www-http
400	54	TCP	94.75.236.122	192.168.1.17	www-http
401	54	TCP	94.75.236.122	192.168.1.17	www-http

```
<MAILFM> <keerthana@ncs-in.com>
<RCPTTO> <sagar@ncs-in.com>
<RCPTTO> <shekhar@ncs-in.com>
<RCPTTO> <amulya@ncs-in.com>


<DATED:>  Tue, 13 Aug 2013 11:18:33 +0530      <FRMADS>  keerthana <keerthana@ncs-in.com>


<REQMTH> GET    <WEBADS> clients1.google.com    <WEBURL> clients1.google.com/complete/search?
<CNTTYP> text/javascript;       <CNTENC> gzip   <CNTLEN> 234
```

The **Experiment 2** shows the following details for every TCP packet analyzed using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Packet Size
- Packet Type
- Source IP Address
- Destination IP Address
- Application protocol
- Content Type field and corresponding Content Type string.

196	1484	TCP	74.125.236.69	192.168.1.17	www-http
197	361	TCP	74.125.236.69	192.168.1.17	www-http
198	66	TCP	173.194.36.57	192.168.1.17	www-http
199	94	TCP	164.46.82.116	192.168.1.134	Extended SMTP
200	54	TCP	192.168.1.17	74.125.236.69	www-http
201	54	TCP	192.168.1.17	173.194.36.57	www-http
202	63	TCP	164.46.82.116	192.168.1.72	POP3
203	109	TCP	192.168.1.134	164.46.82.116	Extended SMTP
204	644	TCP	192.168.1.17	74.125.236.156	www-http
205	668	TCP	192.168.1.17	74.125.236.156	www-http
206	573	TCP	192.168.1.17	74.125.239.15	www-http
207	54	TCP	74.125.236.156	192.168.1.17	www-http
208	54	TCP	74.125.236.156	192.168.1.17	www-http
209	60	TCP	192.168.1.72	164.46.82.116	POP3

```
<CNTTYP> image/png      <CNTLEN> 3486


<CNTTYP> image/jpeg     <CNTLEN> 4248






<MAILFM> <keerthana@ncs-in.com>
<REQMTH> GET    <WEBADS> ad.doubleclick.net     <WEBURL> ad.doubleclick.net/N6762/adi/mkt.ythor
<REQMTH> GET    <WEBADS> ad.doubleclick.net     <WEBURL> ad.doubleclick.net/N4061/adi/com.ythor
<REQMTH> GET    <WEBADS> csi.gstatic.com        <WEBURL> csi.gstatic.com/csi?v=2&s=youtube&acti
```

The **Experiment 3** shows the following details for every UDP packet analyzed using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Packet Size
- Packet Type
- Source IP Address
- Destination IP Address
- Application protocol
- Content Type field and corresponding Content Type string.

75	110	UDP	192.168.1.2	192.168.1.134	DNS
76	164	UDP	192.168.1.2	192.168.1.134	DNS
291	92	UDP	192.168.1.126	192.168.1.255	netbios-ns
358	92	UDP	192.168.1.126	192.168.1.255	netbios-ns
373	92	UDP	192.168.1.126	192.168.1.255	netbios-ns
444	458	UDP	192.168.1.26	192.168.1.17	SIP
445	657	UDP	192.168.1.17	192.168.1.26	SIP
446	657	UDP	192.168.1.17	192.168.1.26	SIP
447	657	UDP	192.168.1.17	192.168.1.26	SIP
448	657	UDP	192.168.1.17	192.168.1.26	SIP
449	652	UDP	192.168.1.26	192.168.1.17	SIP
450	557	UDP	192.168.1.17	192.168.1.26	SIP
451	557	UDP	192.168.1.17	192.168.1.26	SIP
452	557	UDP	192.168.1.17	192.168.1.26	SIP
453	557	UDP	192.168.1.17	192.168.1.26	SIP
591	75	UDP	192.168.1.134	192.168.1.2	DNS

```
<PKTTYP> 200 OK          <FRDETL> phone2 <sip:126@192.168.1.17:5060>
<PKTTYP> 200 OK          <FRDETL> phone2 <sip:126@192.168.1.17:5060>
<PKTTYP> 200 OK          <FRDETL> phone2 <sip:126@192.168.1.17:5060>
<PKTTYP> 200 OK          <FRDETL> phone2 <sip:126@192.168.1.17:5060>
```

The **Experiment 4** shows the following details for every analysed SMTP packet using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Header length
- VLAN tag
- Type Of Service
- Time of arrival of packet
- Packet length
- Source IP Address
- Destination IP Address
- Source IP Address(hex)
- Destination IP Address(hex)
- Source Mac address
- Destination Mac address
- IP protocol
- IP protocol string
- TCP source port
- TCP destination port

- TCP flag status
- Application protocol number
- Application protocol name
- Content Type field and corresponding Content Type string.

```
..............END OF A PACKET......................

..............START OF A PACKET......................

Kamal packet number      : 9162
Kamal Header Length      : 72
VLAN tag                 : 0
IP Type Of Service       : 0
Time of arrival of Packet: Tue Aug 13 11:18:53 2013

The IP packet length     : 1514
The Source IP            : 192.168.1.131
Source IP (hex)          : c0a80183
The Destination IP       : 164.46.82.116
Destination IP (hex)     : a42e5274
Source Mac address       : 00:15:17:B7:07:6C
Destination Mac address  : 00:17:7C:13:AC:CC
IP protocol              : 6
IP Protocol String       : TCP
TCP source port          : 51016
TCP The destination port : 587
Its NOT SYN packet
Its NOT PUSH packet
Its a ACK packet
Its NOT URG packet
Its NOT RST packet
Its NOT FIN packet
TCP Application Protocol Number : 587
TCP The Application Protocol Name : Extended SMTP
Content Type   : <DATED:>
Content String :  Tue, 13 Aug 2013 11:18:49 +0530
Content Type   : <FRMADS>
Content String :  shekhar <shekhar@ncs-in.com>
Content Type   : <TO_ADS>
Content String :  sagar <sagar@ncs-in.com>, keerthana <keerthana@ncs-in.com>
Content Type   : <SUBJCT>
Content String :  Fwd: Tester mail
Content Type   : <SUBJCT>
Content String :        Tester mail
Content Type   : <DATED:>
Content String :        Mon, 12 Aug 2013 11:16:28 +0530
Content Type   : <FRMADS>
Content String :        sagar <sagar@ncs-in.com>
Content Type   : <TO_ADS>
Content String :        shekhar@ncs-in.com
..............END OF A PACKET......................
```

The **Experiment 5** shows the following details for every analysed POP3 packet using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Header length
- VLAN tag
- Type Of Service
- Time of arrival of packet
- Packet length
- Source IP Address
- Destination IP Address
- Source IP Address(hex)
- Destination IP Address(hex)
- Source Mac address
- Destination Mac address

- IP protocol
- IP protocol string
- TCP source port
- TCP destination port
- TCP flag status
- Application protocol number
- Application protocol name
- Content Type field and corresponding Content Type string.

```
...............START OF A PACKET......................

Kamal packet number       : 10964
Kamal Header Length       : 72
VLAN tag                  : 0
IP Type Of Service        : 0
Time of arrival of Packet: Tue Aug 13 11:19:07 2013

The IP packet length      : 1514
The Source IP             : 164.46.82.116
Source IP (hex)           : a42e5274
The Destination IP        : 192.168.1.134
Destination IP (hex)      : c0a80186
Source Mac address        : 00:17:7C:13:AC:CC
Destination Mac address   : 00:0E:0C:3C:72:79
IP protocol               : 6
IP Protocol String        : TCP
TCP source port           : 110
TCP The destination port  : 35287
Its NOT SYN packet
Its NOT PUSH packet
Its a ACK packet
Its NOT URG packet
Its NOT RST packet
Its NOT FIN packet
TCP Application Protocol Number : 110
TCP The Application Protocol Name : POP3
Content Type    : <SENDIP>
Content String : 122.166.22.231
Content Type    : <DATED:>
Content String : Tue, 13 Aug 2013 11:18:49 +0530
Content Type    : <FRMADS>
Content String :  shekhar <shekhar@ncs-in.com>
Content Type    : <TO_ADS>
Content String :  sagar <sagar@ncs-in.com>, keerthana <keerthana@ncs-in.com>
Content Type    : <SUBJCT>
Content String : Fwd: Tester mail
Content Type    : <SUBJCT>
Content String :         Tester mail
Content Type    : <DATED:>
Content String :         Mon, 12 Aug 2013 11:16:28 +0530
Content Type    : <FRMADS>
Content String :         sagar <sagar@ncs-in.com>
Content Type    : <TO_ADS>
Content String :         shekhar@ncs-in.com
...............END OF A PACKET......................
```

The **Experiment 6** shows the following details for every analysed HTTP packet using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Header length
- VLAN tag
- Type Of Service
- Time of arrival of packet
- Packet length

- Source IP Address
- Destination IP Address
- Source IP Address(hex)
- Destination IP Address(hex)
- Source Mac address
- Destination Mac address
- IP protocol
- IP protocol string
- TCP source port
- TCP destination port
- TCP flag status
- Application protocol number
- Application protocol name
- Content Type field and corresponding Content Type string.

```
Its NOT FIN packet
TCP Application Protocol Number : 80
TCP Application Protocol Name : www-http
Content Type   : <REQMTH>
Content String : GET
Content Type   : <WEBADS>
Content String : dnl-17.geo.kaspersky.com
Content Type   : <WEBURL>
Content String : dnl-17.geo.kaspersky.com/index/../bases/av/kdb/i386/dailyc.kdc
...............END OF A PACKET......................

...............START OF A PACKET......................

Kamal packet number      : 593
Kamal Header Length      : 72
VLAN tag                 : 0
IP Type Of Service       : 0
Time of arrival of Packet: Tue Aug 13 11:17:58 2013

The IP packet length     : 1514
The Source IP            : 38.124.168.119
Source IP (hex)          : 267ca877
The Destination IP       : 192.168.1.22
Destination IP (hex)     : c0a80116
Source Mac address       : 00:17:7C:13:AC:CC
Destination Mac address  : 00:1E:EC:12:5E:4E
IP protocol              : 6
IP Protocol String       : TCP
TCP source port          : 80
TCP The destination port : 1345
Its NOT SYN packet
Its NOT PUSH packet
Its a ACK packet
Its NOT URG packet
Its NOT RST packet
Its NOT FIN packet
TCP Application Protocol Number : 80
TCP Application Protocol Name : www-http
Content Type   : <CNTTYP>
Content String : application/octet-stream
Content Type   : <CNTLEN>
Content String : 123127
...............END OF A PACKET......................
```

The **Experiment 7** displays list of IP addresses of the clients in a dotted string format for every analysed packet.

```
IP Address of Clients
192.168.1.123
192.168.1.131
192.168.1.17
192.168.1.2
192.168.1.135
192.168.1.72
192.168.1.11
192.168.1.12
192.168.1.134
192.168.1.126
```

The **Experiment 8** displays list of IP addresses of the clients in a dotted string format for every analysed HTTP packet.

```
IP Address of Clients
192.168.1.131
192.168.1.17
192.168.1.12
192.168.1.22
192.168.1.134
192.168.1.187
192.168.1.72
192.168.1.130
```

Flow Analysis

The **Experiment 9** shows the TCP SEQUENCE flow details for an analysed packet belonging to a 5 Tuple based flow information in the following format.

Flow header details

- Source IP address
- Source port
- Destination IP address
- Destination port

Flow Analysis

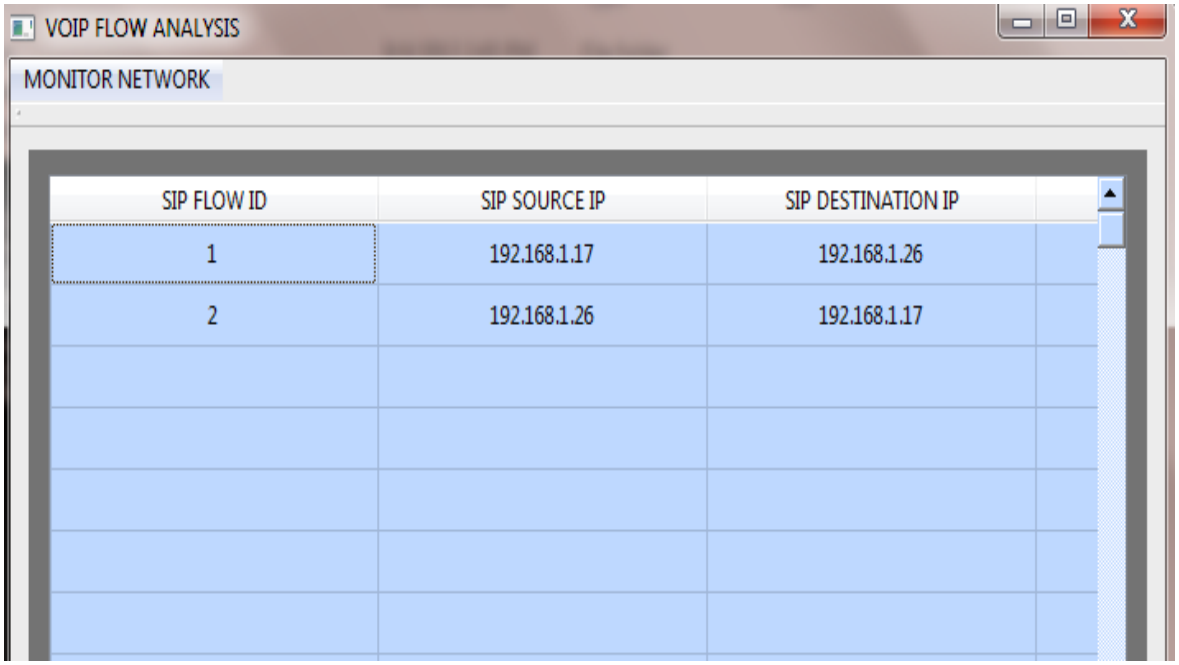
- Packet Size
- Timestamp
- Sequence Number
- Acknowledge Number
- Flow Direction
- TCP flag

```
Running INPUT MODE...
Enter Client IP ADDRESS:
192.168.1.130

-----------------------------------FLOW HEADER DETAILS----------------------------------------------
Src IP : 192.168.1.130   Src Port : 52059       Dst IP : 164.46.82.116  Dst Port : 110  IP Protocol : 6
----------------------------------------------------------------------------------------------------

-----------------------------------FLOW ANALYSIS----------------------------------------------------
PktSize TimeStamp(Sec:Microsec)  Seq number      Ack number     FlowDir         TCPFlag

----------------------------------------------------------------------------------------------------
 66      1390816104 : 468595     2330647236      0000000000      ---->           SYN
 66      1390816104 : 756249     0835464448      2347424452      <----           SYN ACK
 54      1390816104 : 758082     2347424452      0852241664      ---->           ACK
 114     1390816105 : 084216     0852241664      2347424452      <----           PUSH ACK
 66      1390816105 : 085819     2347424452      1858874624      ---->           PUSH ACK
 54      1390816105 : 425870     1858874624      2548751044      <----           ACK
 88      1390816105 : 426362     1858874624      2548751044      <----           PUSH ACK
 69      1390816105 : 428301     2548751044      2429299968      ---->           PUSH ACK
 120     1390816105 : 717094     2429299968      2800409284      <----           PUSH ACK
 60      1390816105 : 718650     2800409284      3536596224      ---->           PUSH ACK
 71      1390816106 : 017712     3536596224      2901072580      <----           PUSH ACK
 60      1390816106 : 022308     2901072580      3821808896      ---->           PUSH ACK
 97      1390816106 : 347231     3821808896      3001735876      <----           PUSH ACK
 54      1390816106 : 543148     3001735876      0248327424      ---->           ACK
 400     1390816106 : 840173     0248327424      3001735876      <----           PUSH ACK
 60      1390816106 : 842344     3001735876      1758342400      ---->           PUSH ACK
 82      1390816107 : 167030     1758342400      3102399172      <----           PUSH ACK
 54      1390816107 : 369355     3102399172      2228104448      ---->           ACK
 898     1390816107 : 657060     2228104448      3102399172      <----           PUSH ACK
 60      1390816107 : 660179     3102399172      3503369472      ---->           PUSH ACK
 116     1390816107 : 956445     3503369472      3203062468      <----           PUSH ACK
 54      1390816107 : 956942     0248655104      3203062468      <----           ACK FIN

Flow Analysis Completed
```

The **Experiment 10** is to recreate VOIP call session captured using two VOIP enabled phones, using KDF. For this, we ran a VoIP session, which was captured and KDF files were created using MONOSEK. Using this KDF files, we are able to segregate VoIP sessions and show these in a GUI. User can also play any of the conversation, by clicking on appropriate VoIP Session rows and columns displayed on the GUI.

```
Started Sniffing
Server: The Winsock dll found!
Server: The status: Running.
Server: The dll supports the Winsock version 2.2!
Server: The highest version this dll can support: 2.2
Server: Waiting for a client to connect...
***Hint: Server is ready...run your client program...***
Server: Client Connected!
UDP : 15802 Total : 98977
```

This experiment also requires VLC media player 2.0 or higher to be installed in the system with PATH for VLC set as system environment variable, to play the recreated VOIP sessions at the click on cells in VOIP GUI.



The **Experiment 11** shows the following details for every analysed packet using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Header length
- VLAN tag
- Type Of Service
- Time of arrival of packet
- Packet length
- Source IP Address
- Destination IP Address
- Source IP Address(hex)
- Destination IP Address(hex)
- Source Mac address

- Destination Mac address
- IP protocol
- IP protocol string
- TCP/UDP source port
- TCP/UDP destination port
- TCP flag status
- TCP/UDP Application protocol number
- TCP/UDP Application protocol name.
- Content Type field and corresponding Content Type string.

```
...............START OF A PACKET......................

Kamal packet number       : 9
Kamal Header Length       : 72
VLAN tag                  : 0
IP Type Of Service        : 0
Time of arrival of Packet: Tue Aug 13 11:17:41 2013

The IP packet length      : 54
The Source IP             : 192.168.1.123
Source IP (hex)           : c0a8017b
The Destination IP        : 173.194.36.22
Destination IP (hex)      : adc22416
Source Mac address        : 00:15:58:CE:E4:77
Destination Mac address   : 00:17:7C:13:AC:CC
IP protocol               : 6
IP Protocol String        : TCP
TCP source port           : 1076
TCP The destination port  : 443
Its NOT SYN packet
Its NOT PUSH packet
Its a ACK packet
Its NOT URG packet
Its NOT RST packet
Its NOT FIN packet
TCP Application Protocol Number : 443
TCP Application Protocol Name : ssl - https
...............END OF A PACKET......................

...............START OF A PACKET......................

Kamal packet number       : 10
Kamal Header Length       : 72
VLAN tag                  : 0
IP Type Of Service        : 0
Time of arrival of Packet: Tue Aug 13 11:17:42 2013

The IP packet length      : 84
The Source IP             : 192.168.1.17
Source IP (hex)           : c0a80111
The Destination IP        : 125.22.47.125
Destination IP (hex)      : 7d162f7d
Source Mac address        : 00:26:2D:8C:46:BC
Destination Mac address   : 00:17:7C:13:AC:CC
IP protocol               : 17
IP Protocol String        : UDP
UDP source port           : 15326
UDP The destination port  : 13568
UDP Application Protocol Number : 53
UDP Application Protocol Name : DNS
...............END OF A PACKET......................
```

The **Experiment 12** shows the following details for every analysed TCP packet using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Header length
- VLAN tag
- Type Of Service
- Time of arrival of packet
- Packet length
- Source IP Address
- Destination IP Address
- Source IP Address(hex)
- Destination IP Address(hex)
- Source Mac address
- Destination Mac address
- IP protocol
- IP protocol string
- TCP source port
- TCP destination port
- TCP flag status
- TCP Application protocol number
- TCP Application protocol name.
- Content Type field and corresponding Content Type string.

```
...............START OF A PACKET......................

Kamal packet number      : 216
Kamal Header Length      : 72
VLAN tag                 : 0
IP Type Of Service       : 0
Time of arrival of Packet: Tue Aug 13 11:17:49 2013

The IP packet length     : 1484
The Source IP            : 74.125.236.156
Source IP (hex)          : 4a7dec9c
The Destination IP       : 192.168.1.17
Destination IP (hex)     : c0a80111
Source Mac address       : 00:17:7C:13:AC:CC
Destination Mac address  : 00:26:2D:8C:46:BC
IP protocol              : 6
IP Protocol String       : TCP
TCP source port          : 80
TCP The destination port : 51088
Its NOT SYN packet
Its NOT PUSH packet
Its a ACK packet
Its NOT URG packet
Its NOT RST packet
Its NOT FIN packet
TCP Application Protocol Number : 80
TCP Application Protocol Name : www-http
Content Type   : <CNTTYP>
Content String : text/html;
Content Type   : <CNTENC>
Content String : gzip
Content Type   : <CNTLEN>
Content String : 1999
...............END OF A PACKET......................
```

The **Experiment 13** shows the following details for every analysed UDP packet using MONOSEK. Display on the command prompt for every analysed packet follows the following format:

- Packet Number
- Header length
- VLAN tag
- Type Of Service
- Time of arrival of packet
- Packet length
- Source IP Address
- Destination IP Address
- Source IP Address(hex)
- Destination IP Address(hex)
- Source Mac address
- Destination Mac address
- IP protocol
- IP protocol string
- UDP source port
- UDP destination port
- UDP Application protocol number
- UDP Application protocol name.
- Content Type field and corresponding Content Type string.

```
...............START OF A PACKET......................

Kamal packet number      : 76
Kamal Header Length      : 72
VLAN tag                 : 0
IP Type Of Service       : 0
Time of arrival of Packet: Tue Aug 13 11:17:47 2013

The IP packet length     : 164
The Source IP            : 192.168.1.2
Source IP (hex)          : c0a80102
The Destination IP       : 192.168.1.134
Destination IP (hex)     : c0a80186
Source Mac address       : 00:17:7C:13:AC:CC
Destination Mac address  : 00:0E:0C:3C:72:79
IP protocol              : 17
IP Protocol String       : UDP
UDP source port          : 13568
UDP The destination port : 31901
UDP Application Protocol Number : 53
UDP Application Protocol Name : DNS
...............END OF A PACKET......................

...............START OF A PACKET......................

Kamal packet number      : 291
Kamal Header Length      : 72
VLAN tag                 : 0
IP Type Of Service       : 0
Time of arrival of Packet: Tue Aug 13 11:17:49 2013

The IP packet length     : 92
The Source IP            : 192.168.1.126
Source IP (hex)          : c0a8017e
The Destination IP       : 192.168.1.255
Destination IP (hex)     : c0a801ff
Source Mac address       : 08:9E:01:26:2A:F9
Destination Mac address  : FF:FF:FF:FF:FF:FF
IP protocol              : 17
IP Protocol String       : UDP
UDP source port          : 35072
UDP The destination port : 35072
UDP Application Protocol Number : 137
UDP Application Protocol Name : netbios-ns
...............END OF A PACKET......................
```

The **Experiment 14** displays the packet status at each layer for every analysed packet:

- Layer 2:
  VLan Tag, Source MAC address ,Destination MAC address
- Layer 3:
  IP TOS, Time of arrival of packet, IP Packet Length, Source IP (hex) ,Destination IP (hex), IP protocol, IP protocol string
- Layer 4:
  TCP/UDP source port , TCP/UDP destination port, TCP flag status
- Layer 5:
  TCP/UDP Application protocol number, TCP/UDP Application protocol name, Content Type field and corresponding Content Type string.

```
..............START OF A PACKET......................

LAYER 2
VLAN tag :: 0
Source Mac address :: 00:17:7C:13:AC:CC
Destination Mac address :: 00:24:21:A1:A9:CB

LAYER 3

IP Type Of Service(DiffServ) :: 0
Time of arrival of Packet :: Mon Jan 27 15:53:21 2014

The IP packet length :: 1514
The Source IP :: 74.125.169.108
Source IP (hex) :: 4a7da96c
The Destination IP :: 192.168.1.130
Destination IP (hex) :: c0a80182
IP protocol :: 6
IP Protocol String :: TCP

LAYER 4 TCP

TCP source port :: 80
TCP The destination port :: 52296
TCP Sequence Number :: 384202007
TCP Acknowledgement Number :: 3160237999
Its NOT SYN packet
Its NOT PUSH packet
Its a ACK packet
Its NOT URG packet
Its NOT RST packet
Its NOT FIN packet

LAYER 5 TCP DATA

TCP Application Protocol Number : 80
TCP Application Protocol Name : www-http
..............END OF A PACKET......................
```

Session Analysis

This experiment shows the following details for every analysed session created using MONOSEK and creates sessions for each flow supported by SDK.

Protocol supported by SDK for purpose of session creation are -

- HTTP:
    - Web Pages: html
    - Images: jpeg, png, gif
    - Videos: mp4
- SMTP
- POP3

The application shows the following details on the terminal for each analysed session (one line per session):

- Session Number
- Session Start Time
- Session End Time
- Session Duration
- Session Size
- Source IP Address
- Destination IP Address
- Application protocol
- Content Type field and corresponding Content Type string.

The application also creates a session file for session types HTTP, (html, jpeg, png), SMTP, POP3.

By Default, this application creates session files in the same path where the gsf files are saved. It also uses the gsf file name as base file name for the session files with extensions .html, .jpg, .png or .eml depending on type of session. If the session file already exists, (because this app was already executed earlier), then by default, the application_overwrites on the previous file.

You can also store created sessions as per user's choice as illustrated in the image below.

```
root@monosek:~# cd /home/Monosek2Ver1_0/
EXPERIMENTS/  Monosek_Data/
root@monosek:~# cd /home/Monosek2Ver1_0/EXPERIMENTS/
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS# ls
FORENSIC_EXE  MONOSEK_LIBRARY  README  SAMPLE_SRC
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS# cd FORENSIC_EXE/
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS/FORENSIC_EXE# ls
General_Console
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS/FORENSIC_EXE# ./General_Console
Syntax : ./General_Console http|smtp|pop3|other PMode
Example: ./General_Console http|smtp|pop3|other 0
Pmode can be set to 1 for Pause Refreshing
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS/FORENSIC_EXE# ./General_Console http 0

Session file output will be placed in default location
Default path is set using monosek2config.sh file. Verify on a terminal by typing : set | grep MSE
Do you want to set path of your choice, (yes):  yes

Please provide path :   /root/Desktop/session
```

```
1091    05-09-2013 15:00:49     05-09-2013 15:00:50     1       3528    192.168.1.17    2
.yimg.com <WEBURL> l.yimg.com/qx/cricket/fufp/images/6-11-2-2012-e492bb0be566324796f25d3b
1092    05-09-2013 14:54:51     05-09-2013 14:59:51     300     2944    192.168.1.17    1
conomictimes.indiatimes.com <WEBURL> economictimes.indiatimes.com/toisensexniftyblock.cms
Warning::content type text/html;charset=UTF-8 not yet supported
1093    05-09-2013 15:00:46     05-09-2013 15:00:51     5       56703   192.168.1.17    2
n.news.yahoo.com <WEBURL> in.news.yahoo.com/photos/samsung-galaxy-gear-photos-slideshow/
Warning::content type text/html;charset=utf-8 not yet supported
1094    05-09-2013 15:00:50     05-09-2013 15:00:51     1       9506    192.168.1.17    2
.yimg.com <WEBURL> l.yimg.com/zz/combo?os/mit/media/m/sharing/sharing-min-1129164.css <CN
```

You can view these re-constructed session files by double clicking on these files if there are default apps for them. You can also open them using corresponding apps on command line. For example firefox for web pages and thunderbird for mails. This folder contains a Makefile and ".c" source file (gen_session_sample.c).

```
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS/FORENSIC_EXE#
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS/FORENSIC_EXE#
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS/FORENSIC_EXE#
root@monosek:/home/Monosek2Ver1_0/EXPERIMENTS/FORENSIC_EXE# cd /root/Desktop/session/
root@monosek:~/Desktop/session# ls
sessionfile_10.html   sessionfile_325.jpg   sessionfile_397.html  sessionfile_454.gif   sessionfile_501.png
sessionfile_11.html   sessionfile_326.png   sessionfile_39.html   sessionfile_458.html  sessionfile_502.png
sessionfile_16.html   sessionfile_32.gif    sessionfile_400.gif   sessionfile_45.gif    sessionfile_503.png
sessionfile_19.html   sessionfile_333.html  sessionfile_401.html  sessionfile_462.html  sessionfile_504.html
sessionfile_20.html   sessionfile_334.gif   sessionfile_402.html  sessionfile_464.html  sessionfile_509.html
sessionfile_246.html  sessionfile_335.png   sessionfile_404.html  sessionfile_46.html   sessionfile_520.png
sessionfile_262.gif   sessionfile_336.html  sessionfile_406.gif   sessionfile_470.jpg   sessionfile_521.png
sessionfile_296.gif   sessionfile_337.gif   sessionfile_414.html  sessionfile_480.jpg   sessionfile_522.png
sessionfile_29.html   sessionfile_352.gif   sessionfile_416.html  sessionfile_486.jpg   sessionfile_523.png
sessionfile_304.html  sessionfile_368.gif   sessionfile_41.html   sessionfile_487.jpg   sessionfile_524.png
sessionfile_312.png   sessionfile_36.html   sessionfile_422.html  sessionfile_488.jpg   sessionfile_530.jpg
sessionfile_314.png   sessionfile_373.gif   sessionfile_436.html  sessionfile_489.jpg   sessionfile_531.gif
sessionfile_316.png   sessionfile_37.gif    sessionfile_437.gif   sessionfile_490.jpg   sessionfile_532.html
sessionfile_317.png   sessionfile_380.html  sessionfile_43.gif    sessionfile_491.jpg   sessionfile_540.gif
sessionfile_318.gif   sessionfile_38.gif    sessionfile_441.png   sessionfile_492.jpg   sessionfile_543.html
sessionfile_31.html   sessionfile_394.gif   sessionfile_447.html  sessionfile_493.jpg   sessionfile_544.html
sessionfile_324.png   sessionfile_395.gif   sessionfile_451.gif   sessionfile_494.jpg   sessionfile_548.html
root@monosek:~/Desktop/session#
root@monosek:~/Desktop/session#
root@monosek:~/Desktop/session#
```

Note:
These are sample experiments which are provided to the user with source code, so that the user can understand how to use API calls and SDK to write a new experiment.

Additionally, Students can take projects in various fields,

- Data mining technique to estimate Network packet characteristics
- Data mining technique to estimate behavior of people's internet usage.
- Virus signatures – Study and analysis.
- Network attacks - Known attacks – Identifying and alerting, creating statistics.
- Network attacks – Behavioral pattern matching to estimate possible new threats.