



Implementation of A Dissector for ForCES Protocol in Ethereal

Fenggen Jia, jfg@mail.zjgsu.edu.cn
Chuanhuang Li, chuanhuang_li@pop.zjgsu.edu.cn
Ming Gao, gmyyqno1@pop.zjgsu.edu.cn
Ligang Dong, donglg@mail.zjgsu.edu.cn
Bin Zhuge, zhugebin@mail.zjgsu.edu.cn

IETF 76th Meeting
Nov 9, 2009, Hiroshima Japan

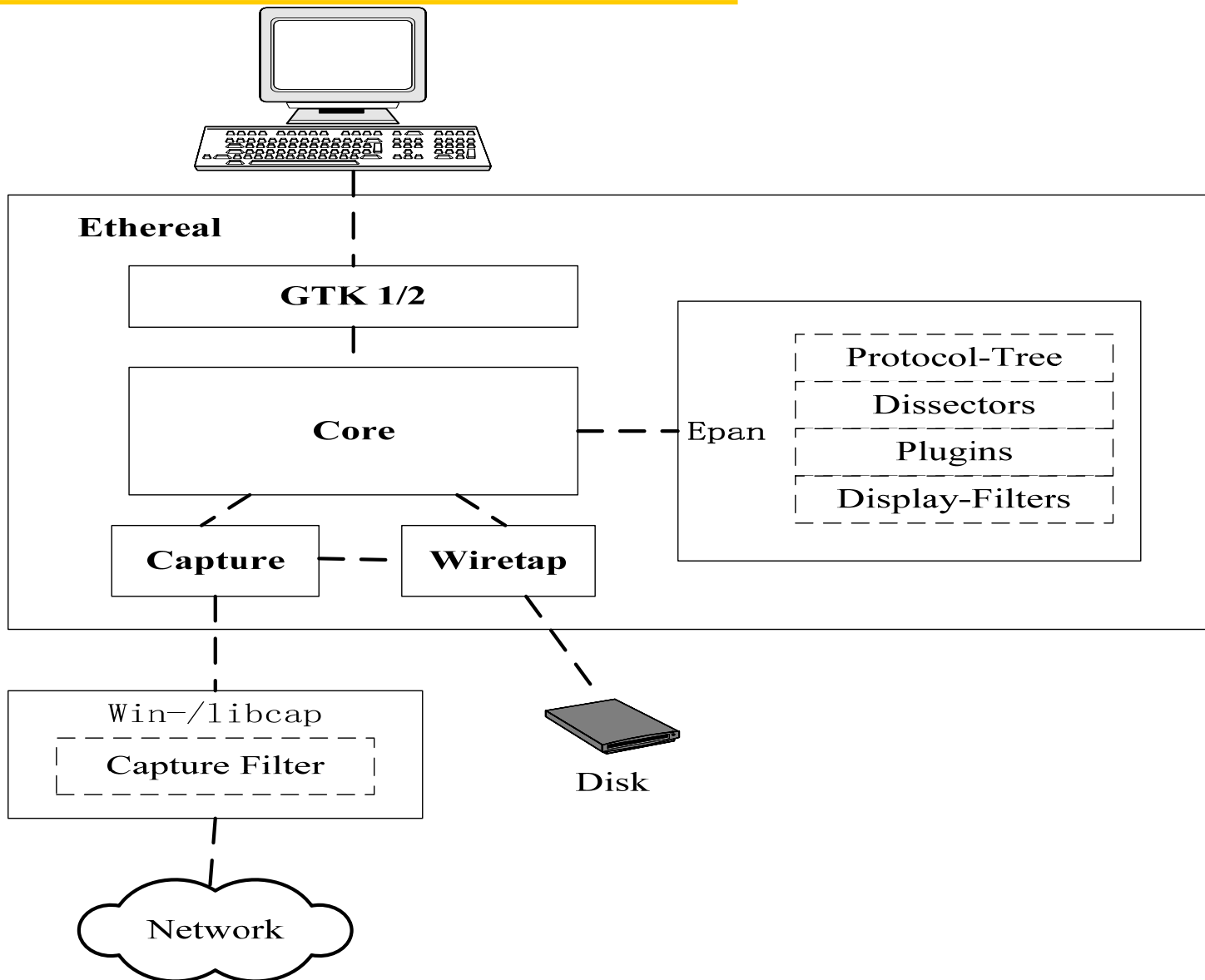




What We Have Implemented

- Analyzing the ForCES protocol encapsulated in TCP/IP, SCTP TML;
- Decode all the fields of ForCES Main Header;
- Decode and show all the fields of LFBselect-TLV included in Main TLV;
 - Oper-TLV included in LFBselect-TLV as well.
- Decode and show all the fields of REDIRECT-TLV included in Main TLV;
- Decode and show all the fields of ASResult-TLV and ASTreason-TLV included in Main TLV;
- All the above are displayed as a tree in Ethereal;

Function Blocks in Ethereal





Insert A “ForCES” Dissector into Ethereal

- Parent-node of ForCES sub-tree is TCP/UDP /SCTP;
- Implement the routine which is used for decoding the message head in the ForCES protocol and shows its protocol tree;
- Register all the fields and parameters in the ForCES protocol to ethereal;
- Implement routine which is used for registering decoding function of the ForCES protocol.

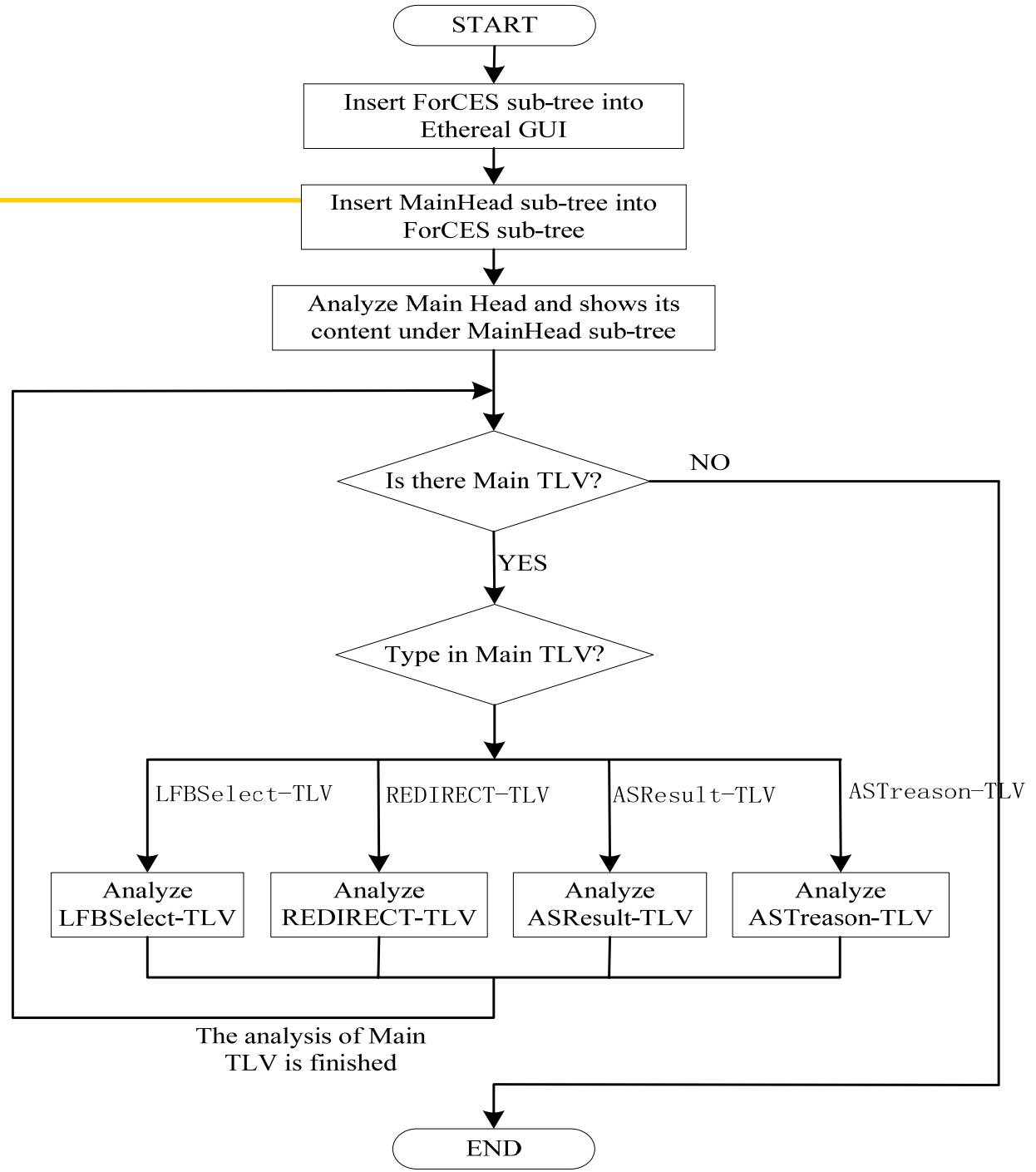


How to Analyze ForCES Protocol

- ForCES sub-tree is inserted under TCP or UDP\SCTP parent-node;
- Create MainHead sub-tree under ForCES sub-tree;
- Analyze the content of MainHead, and show the meaning of special values;
- Create multiple Main TLV sub-trees under ForCES sub-tree according to the number and type of Main TLV. The type of Main TLV is LFBselect-TLV, REDIRECT-TLV, ASResult-TLV, or ASTreason-TLV;
- If the type of Main TLV is LFBselect-TLV, then
 - Analyze LFBCLASSID and LFBInstance in this TLV;
 - Create multiple OPER-TLV sub-tree under LFBselect-TLV sub-tree;
 - Analyze the type of OPER-TLV, and show its type name and length.
- If the type of Main TLV is REDIRECT-TLV, ASResult-TLV, or ASTreason-TLV, then the content in the TLV is shown.



The Flow Chart of Analyzing ForCES Protocol



Interface of Ethereal with ForCES Plugin

The screenshot displays the Ethereal (Wireshark) interface with the ForCES plugin. The main window shows a list of captured packets on the interface eth1, filtered by 'forces && ospf'. The selected packet (No. 68) is expanded to show its details:

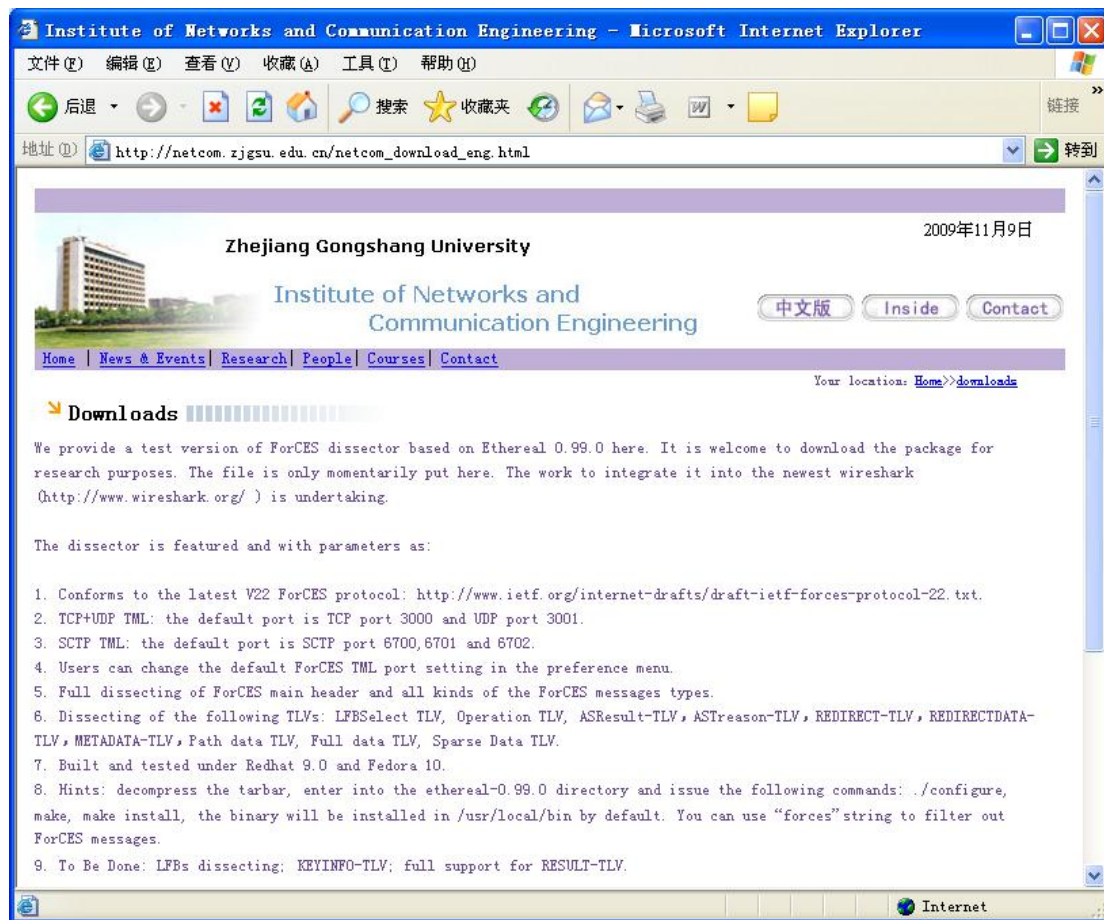
- Frame 5 (182 bytes on wire, 182 bytes captured)
- Ethernet II, Src: Giga-Byt_4e:bf:5f (00:0fea:4e:bf:5f), Dst: Giga-Byt_32:58:3d (00:16:e6:32:58:3d)
 - Destination: Giga-Byt_32:58:3d (00:16:e6:32:58:3d)
 - Source: Giga-Byt_4e:bf:5f (00:0fea:4e:bf:5f)
 - Type: IP (0x0800)
- Internet Protocol, Src: 192.168.10.3 (192.168.10.3), Dst: 192.168.10.1 (192.168.10.1)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - 0000 00.. = Differentiated Services Codepoint: Default (0x00)
 - 0. = ECN-Capable Transport (ECT): 0
 - .. 0 = ECN-CE: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 16 e6 32 58 3d 00 0f ea 4e bf 5f 08 00 45 00 ...2X=..N...E.
0010 00 a8 00 00 40 00 40 11 a4 f0 c0 a8 0a 03 c0 a8 ...@.@. ....
0020 0a 01 80 05 0b b9 00 94 81 9f 10 06 00 8c 00 00 .....
0030 00 03 40 00 00 00 00 00 00 00 00 00 00 00 00 ..@.....
0040 00 00 00 01 00 74 01 15 00 28 00 00 00 01 00 00 .....
0050 00 0c 00 00 08 00 00 00 00 02 00 00 00 0c 00 00 .....
eth1: <live capture in progress> P: 74 D: 20 M: 0
```


Ethereal with ForCES Plugin Download

- Download web:
 - http://netcom.zjgsu.edu.cn/netcom_download_eng.html
- File:
 - [ethereal-0.99.0_forces.tar.gz](#)





Thanks!