Implementation of A Dissector for ForCES Protocol in Ethereal

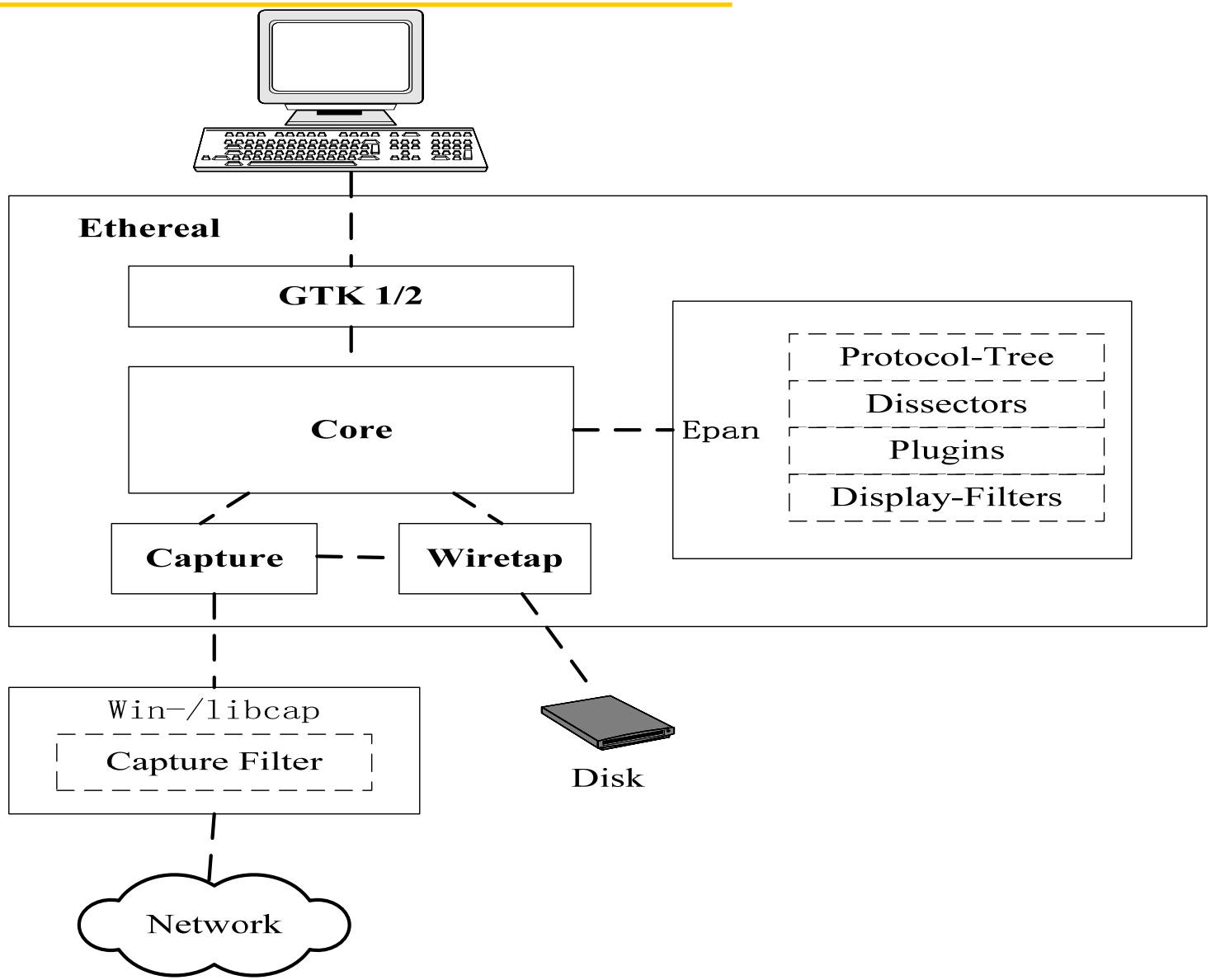
Fenggen Jia，jfg@mail.zjgsu.edu.cn
Chuanhuang Li, chuanhuang_li@pop.zjgsu.edu.cn
Ming Gao, gmyyqno1@pop.zjgsu.edu.cn
Ligang Dong, donglg@mail.zjgsu.edu.cn
Bin Zhuge, zhugebin@mail.zjgsu.edu.cn

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



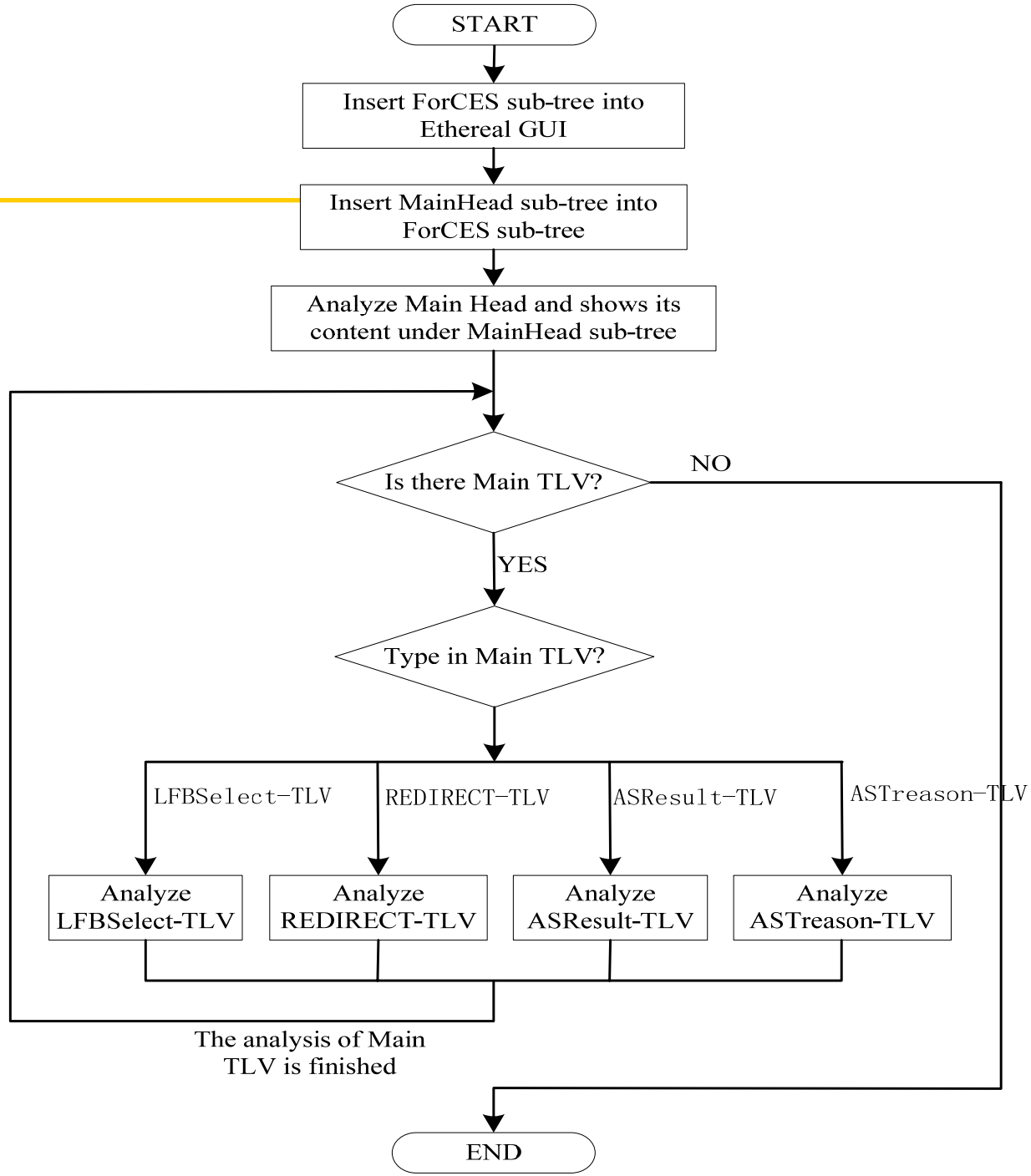
Insert A “ForCES” Dissector into Ethereal

- 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.

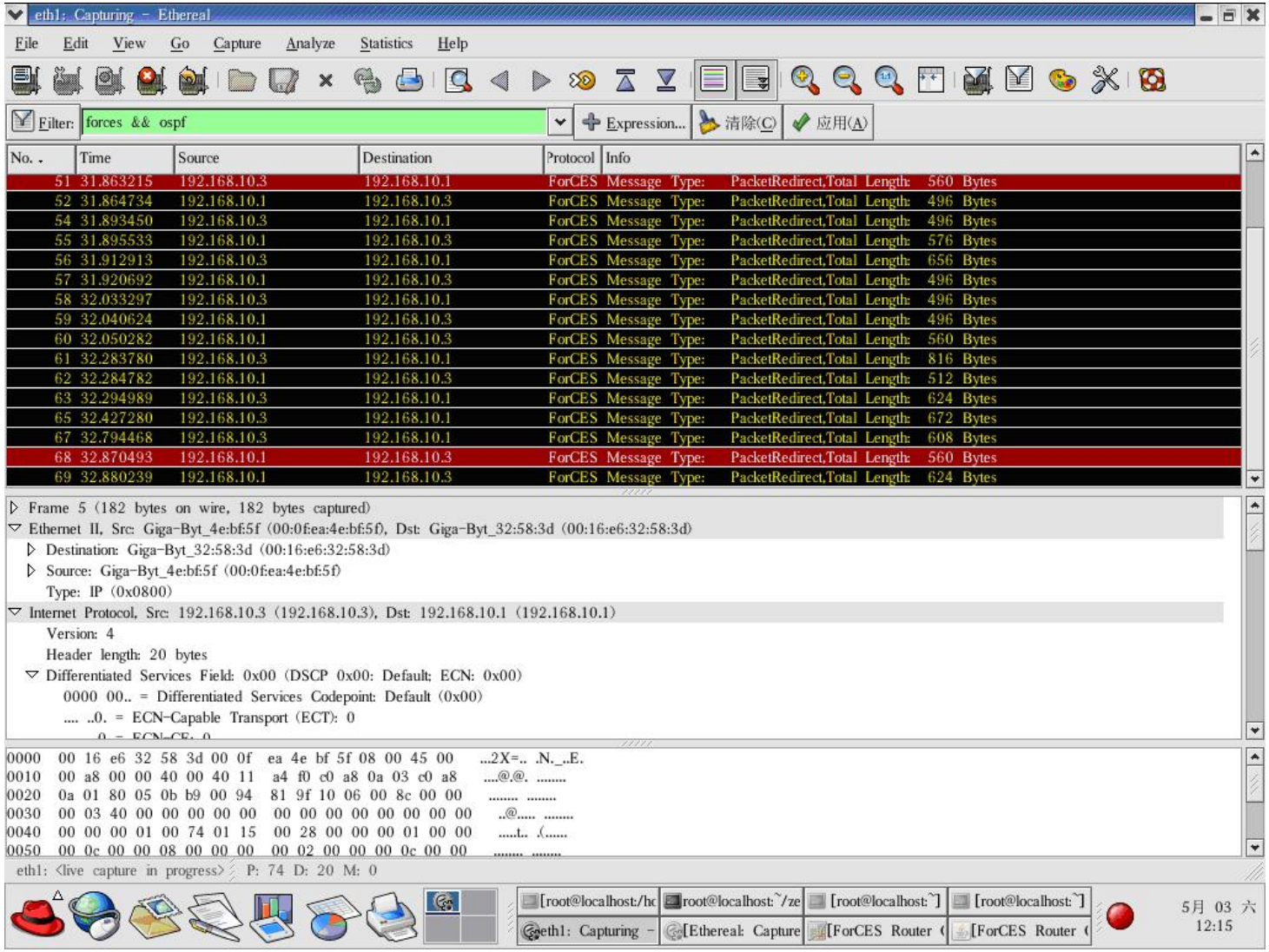
How to Analyze ForCES Protocol

- 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

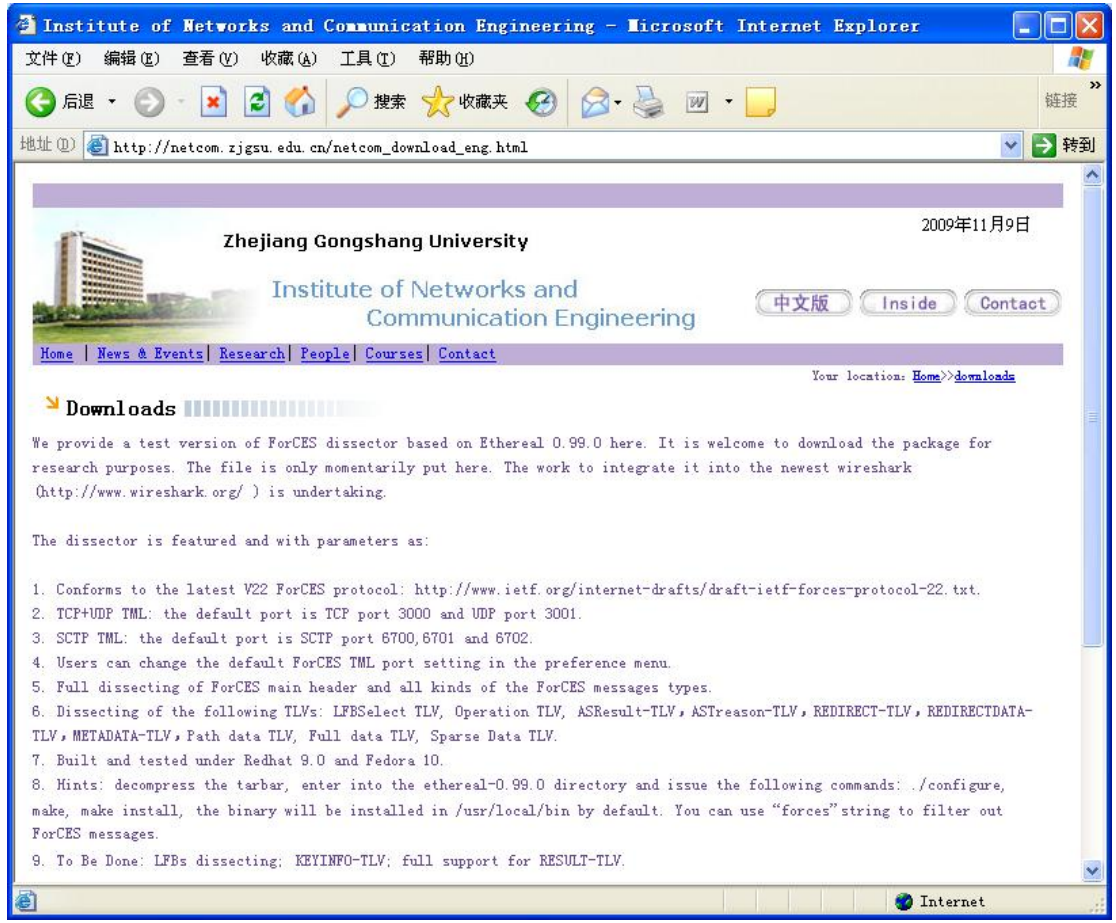


Interface of Ethereal with ForCES Plugin



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!