NetFox.Detective: An Advanced Tool for Network Forensics

Petr Matoušek, Jan Pluskal, Ondřej Ryšavý, Martin Kmeť, Vladimír Veselý, Filip Karpíšek, Martin Vymlátil,

{matousp,ipluskal,rysavy,ikmet,ivesely}@fit.vutbr.cz,{xkarpi03,xvymla01}@stud.fit.vutbr.cz

Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic

Extended abstract

Network forensics is a process of capturing, collecting and analysing network data for the purposes of information gathering, legal evidence, or intrusion detection. The new generation internet opens novel opportunities for cybercrime activities and security incidents using network applications. Security administrators and LEA (Law Enforcement Agency) officers are challenged to employ advanced tools and techniques in order to detect unlawful or unauthorized activities. In case of serious suspicion of crime activity, network forensics tools and techniques are used to find out legal evidences in a captured network communication that prove or disprove someone's participation on that activity.

Today, there are various commercial and free tools for network forensics analysis, e.g., Wireshark, Network Miner, NetWitness, Xplico, NetIntercept, or PacketScan. Many of these tools lack the ability of successful reconstruction of communication when using incomplete, duplicated or corrupted input data. Another challenge represents identification of application protocols that is based not only on port numbers but also on intelligent processing of captured data. Investigators also require an advanced automatic processing of application data that helps them to see real contents of conversation that include chats, VoIP talks, file transmission, email exchange etc.

In our research we focused on design and implementation of a modular tool for network forensics with advanced possibilities of application reconstruction. Its architecture includes (i) an advanced reconstruction of L7 conversations when some packets are missing, (ii) detection of application protocols based on well-known protocol numbers but also on statistical methods and supervised learning, (iii) identification of RTP traffic and multimedia codecs in case of missing signalling protocols, (iv) identification and analysis of bitcoin transactions, (v) reconstruction of webmail communication, etc.

This paper presents our tool NetFox.Detective. Our description focuses on advanced techniques used to build a network forensics analyser. We will discuss the main issues of automatic processing of incomplete or corrupted input data and techniques how to solve it. We also present detection of L7 conversations using heuristic approaches, advanced processing and presentation of selected applications and other techniques. Last part of the paper compares our results with other available network forensics tools.