# Network Forensics Module

Difficulty Level: Intermediate  
Prerequisite: Introduction to digital forensics processes and procedures, and

network fundamentals

Overview  
This module focuses on integrating network forensics essentials and practices to the designed game. Network forensics relates to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Upon successful completion of the module, students can effectively apply network forensics tools to capture and analyze network traffic and log files. Students will be capable of solving medium difficulty level cases through our game system to uncover network evidence from stored communications.

Rationale  
Given the popularity of internet-enabled devices, forensics evidence can be found in data transferred over a network, within network devices, and stored on network servers. Evidence may be in the form of messages sent over a network, files downloaded or uploaded, network logs, and more. If data is not found on the user’s machine or if investigators do not have access to the machine in question, network forensics data may yield missing evidence. Also, investigators may be looking for a more complete picture during an investigation. The goal of this module is to provide future investigators with an introduction to network forensics by focusing on important artifacts that can be found during a typical investigation.

## Tools Required

Users will need to download and install the following free tools.

* Wireshark
* NetworkMiner

Other Files Needed

Users will also need the following files. Links to these files are located a step of the game.

* rhino1.log
* rhino2.log

## Learning Outcomes By the completion of this module, students should be able to:

* Identify pertinent system information, and use court-approved network forensics tools to retrieve admissible evidence.
* Understand basic sources of network evidence
* Use network forensics tools to view and analyze packet captures in order to locate and validate evidence
* Document findings in a professional report