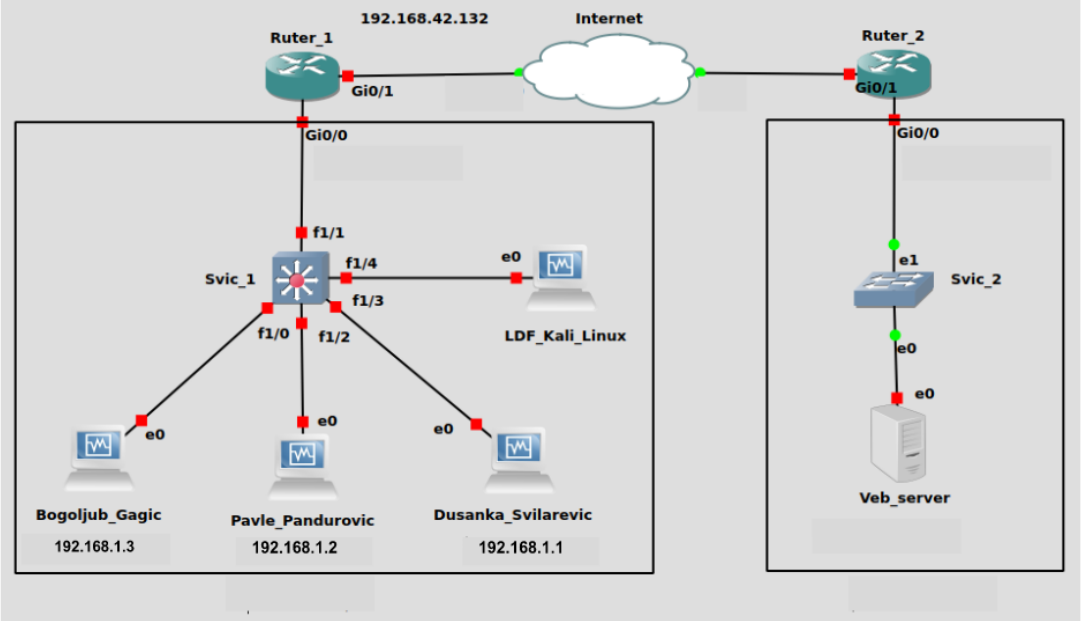
Форензика рачунарских мрежа

Доказни материјал укључује следећи доказни материјал:

- Датотека access.log веб сервера који хостује сервис за евидентирање полазака камиона.
- Датотека са логовима сервиса NAT (NAT.log) конфигурисаног на рутеру фирме „Муња транс” (Ruter_1).
- Снимак мрежног саобраћаја Душанке Свиларевић и Павла Пандуровића (munja_trans.pcap) добијен конфигурисањем SPAN порта на свичу Svic_1.

Форензичке слике поменутих меморијских складишта налазе се на локацији Documents/ ForenzickeSlike у оквиру форензичке радне станице LDF Kali Linux (виртуелне машине).

Шема рачунарске мреже од интереса налази се на слици 1. Напомена: због начина на који је симулирана рачунарска мрежа, јавне IP адресе не припадају опсегу јавних IP адреса.



Слика 1: Шема рачунарске мреже

У циљу разрешења случаја спровести следећи поступак:

1. Увидом у датотеку access.log издвојити јавне IP адресе фирме „Муња транс” (и одговарајуће портове) са којих је приступано веб сервису за евидентирање полазака камиона (1 бод).
2. Увидом у логове сервиса NAT конфигурисаног на рутеру фирме „Муња транс”, одредити приватне IP адресе са којих је приступано веб сервису за евидентирање полазака камиона, а потом одредити којим запосленима те адресе припадају (1 бод).
3. Увидом у снимак мрежног саобраћаја Душанке Свиларевић, одговорити на питање да ли је и ако јесте, када, успостављена безбедна комуникација са сервером чије је име домена airserbia.com (1 бод).