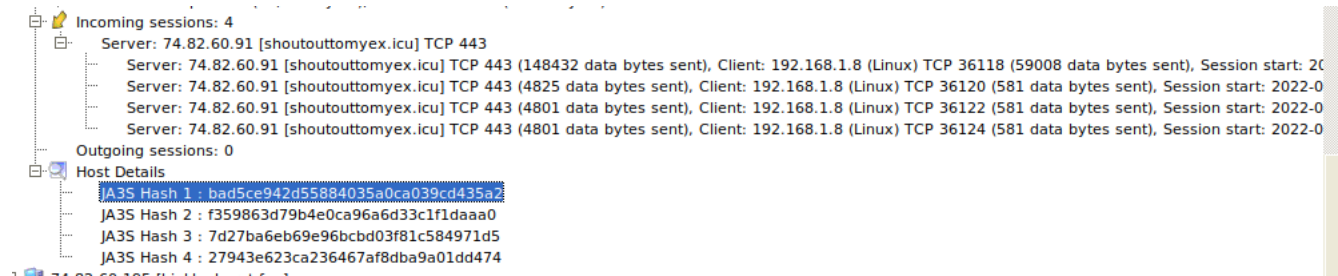
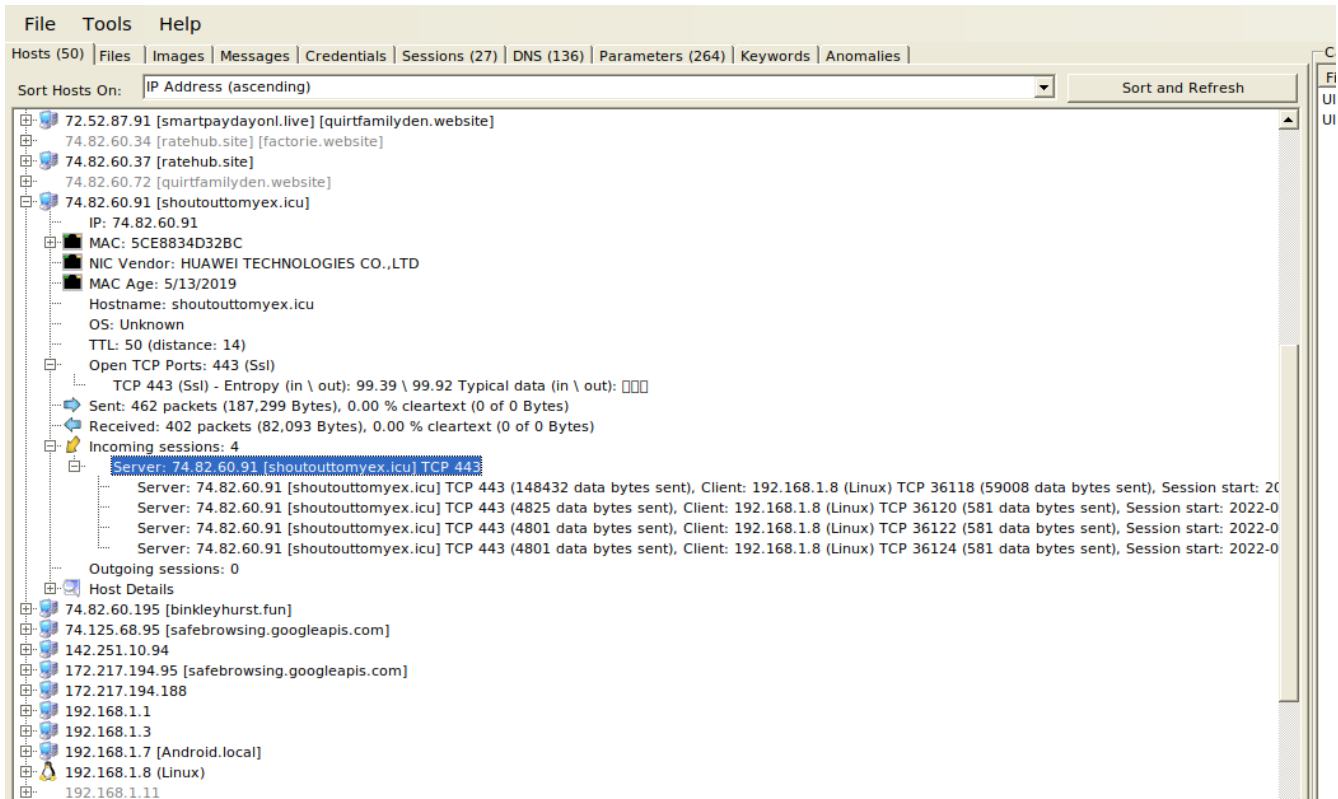


# NetworkMiner Tool DNS analysis



DNS dig:

## \$dig shoutouttomyex.icu

```
<<>> DiG 9.16.1-Ubuntu <<>> shoutouttomyex.icu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27744
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags::; udp: 65494
;; QUESTION SECTION:
;shoutouttomyex.icu.      IN      A

;; ANSWER SECTION:
shoutouttomyex.icu.     600    IN      A       64.62.219.27
shoutouttomyex.icu.     600    IN      A       64.62.219.21
shoutouttomyex.icu.     600    IN      A       64.62.219.36
```

Reverse DNS lookup for VPN mentioned IP (Server: 74.82.60.91 [shoutouttomyex.icu] TCP 443)

**Result:** Dig command return IP address and VPN mentioned IP address are mismatched for the mentioned domain name-shoutouttomyex.icu. The reverse DNS lookup for the IP from VPN-74.82.60.91 no such domain name returned.

```
$
<<>> DiG 9.16.1-Ubuntu <<>> -x 74.82.60.91
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64165
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;91.60.82.74.in-addr.arpa.    IN      PTR
```