Implementujte program *dns-monitor*, který bude monitorovat DNS komunikaci na zvoleném rozhraní, případně zpracuje DNS zprávy z existujícího záznamu komunikace ve fomátu PCAP.

Nástroj bude zpracovávat zprávy protokolu DNS a vypisovat informace z nich zjištěné. Dále bude nástroj schopen zjišťovat, jaká doménová jména se objevovala v DNS zprávách. Třetí funkcionalitou je hledání překladů doménových jmen na IPv4/6 adresy.

Program má tři možné výstupy:

- standardní výstup s informacemi o DNS zprávách,
- (volitelně) soubor se spatřenými doménovými jmény a
- (volitelně) soubor s překlady doménových jmen na IP adresy.

Syntaxe spuštení:
./dns-monitor (-i <interface> | -p <pcapfile>) [-v] [-d <domainsfile>] [-t <translationsfile>]
Parametry:
-i <interface> - název rozhraní, na kterém bude program naslouchat, nebo
-r <pcapfile> - název souboru PCAP, který program zpracuje;
-v - režim "verbose": kompletní výpis detailů o zprávách DNS;
-d <domainsfile> - název souboru s doménovými jmény;
-t <translationsfile> - název souboru s překladem doménových jmen na IP.

Popis funkcionality
Program bude číst síťové pakety ze vstupu (síťové rozhraní, soubor PCAP) a zpracovávat zprávy protokolu DNS.

Rozsah implementace: Pro účely projektu stačí podpora DNS přes protokol UDP.
Také stačí, když bude program podporovat následující typy záznamů:
A, AAAA, NS, MX, SOA, CNAME, SRV. Podpora dalších typů záznamů (PTR aj.) není vyžadována (tj. nástroj je může ignorovat).

Program bude zajišťovat následující funkcionalitu:
A) Výpis informací o DNS zprávách;
B) Hledání doménových jmen;
C) Hledání překladů doménových jmen na IPv4/6 adresy.
Následují informace o jednotlivých funkcích programu.

A) Výpis informací o DNS zprávách
O spatřených DNS zprávách bude program **na standardní výstup** vypisovat informace dle parametrů. Bez parametru "-v" bude zobrazen **zjednodušený výpis**, s parametrem "-v" bude **kompletní vypis**.

Zjednodušený výpis
Ve zjednodušeném výpisu bude 1 řádek pro 1 zprávu protokolu DNS. Formát je následující:

<YYYY-MM-DD><mezera><HH:MM:SS><mezera><zdrojová IP><mezera>-><mezera><cílová IP><mezera>(<Q/R - query/response><mezera><počet záznamů v sekci Question>/<počet záznamů v sekci Answer>/<počet záznamů v sekci Authority/<počet záznamů v sekci Additional>)

Příklad zjednodušeného výpisu:
2024-09-17 14:40:32 192.168.1.5 -> 1.1.1.1 (R 1/2/2/2)

Kompletní výpis (režim -v)
Kompletní výpis bude zobrazovat následující informace:

- Timestamp - datum a čas
- SrcIP - zdrojová IPv4/6 adresa z IP hlavičky
- DstIP - cílová IPv4/6 adresa z IP hlavičky
- SrcPort - zdrojový port: <TCP/UDP>/<číslo portu>
- DstPort - cílový port: <TCP/UDP>/<číslo portu>
- Identifier - identifikátor dotazu (z hlavičky DNS)
- Příznaky - hodnoty příznaků QR, OPCODE, AA, TC, RD, RA, AD, CD, RCODE (formát: <uppercase název příznaku>=<hodnota>)
- Obsah sekcí Question, popř. Answer, Authority, Additional

Syntax kompletního výstupu
<Název položky>:<mezera><hodnota>
...
<Název požky>:<mezera><hodnota>
(Název položky může být: Timestamp, SrcIP, DstIP, Identifier, Flags)
<prázdný řádek>
[Question Section]
<záznamy ze sekce Question>
(pro oddělování polí lze použít mezery či tabulátory)
<prázdný řádek>
[Answer Section] (existuje li, pokud je prázdná, lze vynechat)
(následují případné záznamy a podobně další sekce)
========== *(slouží jako oddělovač pro přehlednost)*

Příklad kompletního výpisu:
Timestamp: 2024-09-17 14:40:32
SrcIP: 192.168.1.5
DstIP: 1.1.1.1
SrcPort: UDP/53
DstPort: UDP/54321
Identifier: 0xC3D4
Flags: QR=1, OPCODE=0, AA=0, TC=0, RD=1, RA=1, AD=0, CD=0, RCODE=0

[Question Section]
example.com. IN A

[Answer Section]

example.com. 300 IN A 93.184.216.34
example.com. 300 IN AAAA 2606:2800:220:1:248:1893:25c8:1946

[Authority Section]
example.com. 172800 IN NS ns1.example.com.
example.com. 172800 IN NS ns2.example.com.

[Additional Section]
ns1.example.com. 86400 IN A 192.0.2.1
ns2.example.com. 86400 IN A 192.0.2.2
==========

B) Hledání doménových jmen (režim -d)
Je-li zadán parametr "-d", bude program vyhledávat doménová jména a ukládat je do souboru s doménovými jmény. Tato jména bude hledat ve všech DNS zprávach, tedy v dotazech i odpovědích, vždy ve všech dostupných sekcích (Question, Answer, Authority, Additional). Kdekoliv se objeví doménové jméno (např. v poli "Name" u záznamu typu A, nebo v poli "RDATA" u záznamu typu NS), program jej uloží do souboru s doménovými jmény, pokud zde dané jméno již není. Pokud doménové jméno v souboru již existuje, nestane se nic.

Výstupní soubor s doménovými jmény bude obsahovat doménová jména, která byla spatřena v DNS zprávách, jedno na každém řádku. Každý řádek bude unikátní.

Příklad obsahu:
fit.vut.cz
nonsenseexyz.io
seznam.cz
google.com

C) Hledání překladů doménových jmen na IPv4/6 adresy (režim -t)
Je-li zadán parametr "-t", bude program hledat také překlady doménových jmen na IPv4/6 adresy a tato ukládat do výstupního souboru s překlady. Informace o překladu je možné získat z A/AAAA záznamů v Answer Section (případně Additional Section) DNS odpovědí. Bude-li objeven nový překlad, program zkontroluje obsah souboru s překladem. Pokud zde zatím takový překlad neexistuje, přidá jej na nový řádek. Existuje-li, nestane se nic.

Soubor s překladem doménových jmen bude obsahovat řádky ve formátu:

Na více řádcích pochopitelně může být stejné doménové jméno. Každý řádek je však unikátní.

Příklad obsahu:
fit.vut.cz 147.229.9.65
seznam.cz 77.75.79.222
seznam.cz 77.75.77.222
google.com 2607:f8b0:4004:c08::8b

Implementační detaily
Program implementujte v jazyce C/C++ pro prostředí Unixových systémů. Referenční prostředí pro překlad budou servery merlin.fit.vutbr.cz a eva.fit.vutbr.cz (program musí být přeložitelný a funkční na obou).
(Pozn. zde pravděpodobně nebudete moci naslouchat na rozhraní. Doporučuji tedy vyzkoušet zde režim se vstupem PCAP a samotný poslech zkoušet někde, kde máte příslušná práva, např. s využitím vlastního fyzického či virtuálního stroje).

Je povoleno (a doporučeno) použít knihovnu libpcap (a hlavičku pcap.h). Můžete využít také knihovnu libresolv (a hlavičku resolv.h). Dále je možné použít hlavičkové soubory pro práci se sokety a další obvyklé funkce používané v síťovém prostředí (jako je netinet/*, sys/*, arpa/* apod.), knihovnu pro práci s vlákny (pthread), signály, časem, stejně jako standardní knihovnu jazyka C (varianty ISO/ANSI i POSIX, všetně souvisejících hlavičkových souborů: ctype.h, string.h., aj), standardní knihovnu jazyka C++ a STL (včetně souvisejících hlaviček). Jiné knihovny nejsou povoleny, nestanoví-li vyučující jinak.

Příklad spuštění 1:
./dns-monitor -i eth0 *(Objeví se dotaz na A záznam pro google.com.)* 2024-09-17 14:42:10 192.168.1.5 -> 8.8.8.8 (Q 1/0/0/0) *(Objeví se odpověď.)* 2024-09-17 14:42:11 8.8.8.8 -> 192.168.1.5 (R 1/1/2/2)

Příklad spuštění 2:
./dns-monitor -i eth0 -v *(Objeví se dotaz na A záznam pro google.com.)*
Timestamp: 2024-09-17 14:42:10
SrcIP: 192.168.1.5
DstIP: 8.8.8.8
SrcPort: UDP/54321
DstPort: UDP/53
Identifier: 0xA1B2
Flags: QR=0, OPCODE=0, AA=0, TC=0, RD=1, RA=0, AD=0, CD=0, RCODE=0

[Question Section]
google.com. IN A.
==========

(Objeví se odpověď.)
Timestamp: 2024-09-17 14:42:11
SrcIP: 8.8.8.8
DstIP: 192.168.1.5
SrcPort: UDP/53
DstPort: UDP/54321
Identifier: 0xA1B2
Flags: QR=1, OPCODE=0, AA=1, TC=0, RD=1, RA=1, AD=0, CD=0, RCODE=0

[Question Section]
google.com. IN A

[Answer Section]
google.com. 300 IN A 142.250.183.142

[Authority Section]
google.com. 86400 IN NS ns1.google.com.
google.com. 86400 IN NS ns2.google.com.

[Additional Section]
ns1.google.com. 86400 IN A 216.239.32.10
ns2.google.com. 86400 IN A 216.239.34.10
==========

Příklad spuštění 3:
(Program spustíme na pozadí a budeme zadávat další příkazy.) **./dns-monitor -i eth0 -d domains.txt -t translations.txt &**
nslookup seznam.cz
Server: 195.113.172.3
Address: 195.113.172.3#53

Non-authoritative answer:
Name: seznam.cz
Address: 77.75.79.222
Name: seznam.cz
Address: 77.75.77.222
Name: seznam.cz
Address: 2a02:598:a::79:222
Name: seznam.cz
Address: 2a02:598:2::1222

sleep 1

cat domains.txt
seznam.cz

cat translations.txt
seznam.cz 77.75.79.222
seznam.cz 77.75.77.222
seznam.cz 2a02:598:a::79:222
seznam.cz 2a02:598:2::1222

Doporučené zdroje

- RFC 1035
- RFC 3596
- Ukázkové příklady kódu na Moodle předmětu ISA