Vaše jméno	Martin Nohava
VUT ID	211569
Vypracovaný lab (označení)	CT_8hod.pcapng

Řešení:

ARP (Address Resolution Protocol): [frames 1-2 a 11-12]

Ve zkoumaném provozu je nejprve pomocí ARP protokolu nalezena fyzická MAC adresa (00:00:00:00:00:04) pro logickou IP adresu 192.168.1.4 (frame 1 a 2). Následně je zahájeno dotazování (ECHO Request viz níže) od klienta 192.168.1.1 na 192.168.3.4 přes uzel 192.168.1.4 (směrovač). Pro zaslání odpovědi na klienta 192.168.1.1 je tedy potřeba aby mezilehlý uzel 192.168.1.4 také znal jeho MAC adresu. Na tu se dotazuje ve frame 11 a 12 a získává odpověď (00:00:00:00:00:01).

1	0.000000	00:00:00_00:00:01	Broadcast	ARP	64	Who has 192.168.1.4? Tell 192.168.1.1
2	0.000024	00:00:00_00:00:04	00:00:00_00:00:01	ARP	64	192.168.1.4 is at 00:00:00:00:00:04
3	0.000024	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0000)
4	0.000147	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0000)
5	0.000276	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0000)
6	0.492000	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0001) [Reassembled in #10]
7	0.492122	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0001) [Reassembled in #10]
8	0.492261	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0001) [Reassembled in #10]
9	0.492397	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=4440, ID=0001) [Reassembled in #10]
10	0.492526	192.168.1.1	192.168.3.4	ECHO	126	Request
11	0.514501	00:00:00_00:00:04	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.4
12	0.514501	00:00:00_00:00:01	00:00:00_00:00:04	ARP	64	192.168.1.1 is at 00:00:00:00:00:01

Obrázek 1

ECHO IPv4: [frames 3-25]

Mezi klientskou stanicí 192.168.1.1 a serverem na adrese 192.168.3.4 (port 7), přes uzel 192.168.1.4 (směrovač) probíhá zasílání zpráv ECHO o velikosti datové části 6000 bajtů. Že uzel 192.168.1.4 opravdu slouží jako mezilehlý uzel, lze ověřit v Ethernetovém rámci pomocí MAC adres Viz horní část Obrázek 3. Komunikaci zajišťuje UDP. Jelikož je ale MTU nastaveno na 1500 bajtů dochází k fragmentaci těchto zpráv v síti viz Obrázek 2. Jelikož odpovědi serveru mají stejnou datovou část jako dotazy, i tyto odpovědi jsou fragmentované. První ECHO Request (s ID=0000) a odpověď na něj vypadají nekompletní. V posledních fragmentech (frame 5 a pro odpověď frame 15) jsou nastavené příznakové bity *More fragments*, (viz Obrázek 3) ale další fragmenty již nepřicházejí.

3	0.000024	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0000)
4	0.000147	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0000)
5	0.000276	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0000)
6	0.492000	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0001) [Reassembled in #10]
7	0.492122	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0001) [Reassembled in #10]
8	0.492261	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0001) [Reassembled in #10]
9	0.492397	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=4440, ID=0001) [Reassembled in #10]
10	0.492526	192.168.1.1	192.168.3.4	ECHO	126	Request
13	0.514643	192.168.3.4	192.168.1.1	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0000)
14	0.514777	192.168.3.4	192.168.1.1	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0000)
15	0.514909	192.168.3.4	192.168.1.1	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0000)
16	0.992000	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0002) [Reassembled in #20]
17	0.992122	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0002) [Reassembled in #20]
18	0.992250	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0002) [Reassembled in #20]
19	0.992381	192.168.1.1	192.168.3.4	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=4440, ID=0002) [Reassembled in #20]
20	0.992511	192.168.1.1	192.168.3.4	ECHO	126	Request
21	1.008592	192.168.3.4	192.168.1.1	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0001) [Reassembled in #25]
22	1.010995	192.168.3.4	192.168.1.1	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0001) [Reassembled in #25]
23	1.013399	192.168.3.4	192.168.1.1	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=2960, ID=0001) [Reassembled in #25]
24	1.015802	192.168.3.4	192.168.1.1	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=4440, ID=0001) [Reassembled in #25]
25	1.015866	192.168.3.4	192.168.1.1	ECHO	126	Response

Obrázek 2

```
    5 0.000276      192.168.1.1                192.168.3.4                IPv4     1518 Fragmented IP protocol (proto=UDP 17, off=2960, ID=0000)
```

```
> Frame 5: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits) on interface unknown, id 1
> Ethernet II, Src: 00:00:00_00:00:01 (00:00:00:00:00:01), Dst: 00:00:00_00:00:04 (00:00:00:00:00:04)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.3.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x0000 (0)
  v Flags: 0x21, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 1011 1001 0000 = Fragment Offset: 2960
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.3.4
v Data (1480 bytes)
```

Obrázek 3

ECHO IPv6: [frames 26-55]

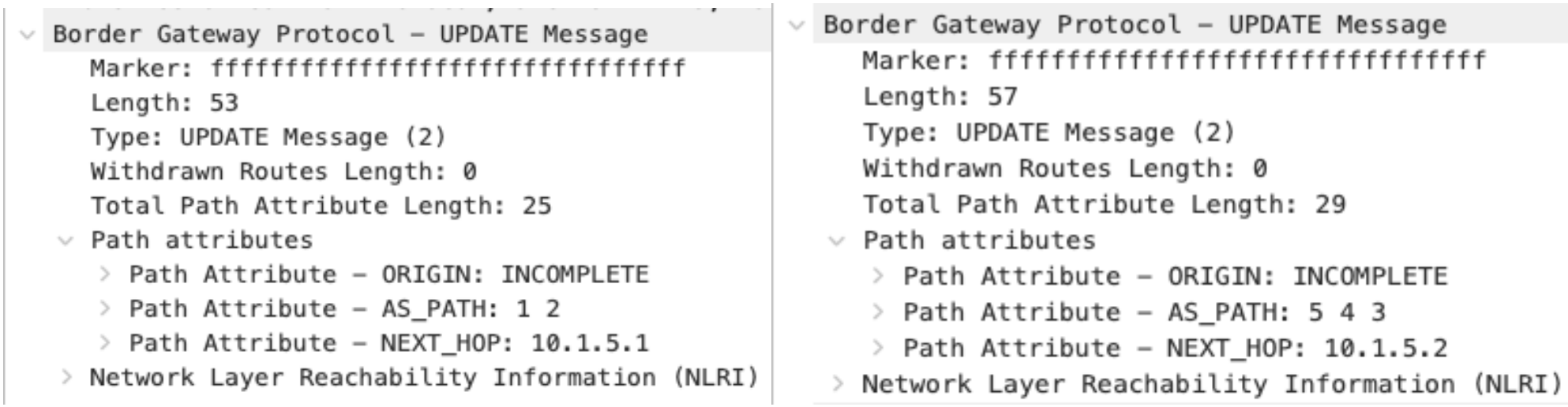
Následně je ve zkoumaném provozu použito zasílání zpráv ECHO mezi stejnými uzly (dle MAC), ale pomocí protokolu IPv6. Datová část zprávy ECHO Request má i nadále velikost 6000 bajtů a je taktéž fragmentována. Pro adresaci jsou využity unicastove IPv6 adresy ve 2 různých subnetech (2001:beef:cafe:1 a 2001:beef:cafe:3). Klient má adresu 2001:beef:cafe:1:200:ff:fe00:1 a server 2001:beef:cafe:3:200:ff:fe00:a s portem 7. Komunikaci opět zajišťuje nespolehlivé UDP. Celá komunikace viz Obrázek 4.

26	5.992028	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=0 more=y ident=0xa68f4557 nxt=17)
27	5.992151	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=1448 more=y ident=0xa68f4557 nxt=17)
28	5.992289	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=2896 more=y ident=0xa68f4557 nxt=17)
29	5.992418	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=4344 more=y ident=0xa68f4557 nxt=17)
30	5.992546	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	ECHO	282	Request
31	6.020910	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=0 more=y ident=0x18485103 nxt=17)
32	6.021045	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=1448 more=y ident=0x18485103 nxt=17)
33	6.021175	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=2896 more=y ident=0x18485103 nxt=17)
34	6.022071	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=4344 more=y ident=0x18485103 nxt=17)
35	6.022398	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	ECHO	282	Response
36	6.492000	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=0 more=y ident=0x8c7cd8e0 nxt=17)
37	6.492122	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=1448 more=y ident=0x8c7cd8e0 nxt=17)
38	6.492251	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=2896 more=y ident=0x8c7cd8e0 nxt=17)
39	6.492382	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=4344 more=y ident=0x8c7cd8e0 nxt=17)
40	6.492510	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	ECHO	282	Request
41	6.508821	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=0 more=y ident=0x904a8ced nxt=17)
42	6.511218	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=1448 more=y ident=0x904a8ced nxt=17)
43	6.513615	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=2896 more=y ident=0x904a8ced nxt=17)
44	6.516012	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=4344 more=y ident=0x904a8ced nxt=17)
45	6.516339	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	ECHO	282	Response
46	6.992000	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=0 more=y ident=0x8ed0be55 nxt=17)
47	6.992122	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=1448 more=y ident=0x8ed0be55 nxt=17)
48	6.992250	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=2896 more=y ident=0x8ed0be55 nxt=17)
49	6.992378	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	IPv6	1514	IPv6 fragment (off=4344 more=y ident=0x8ed0be55 nxt=17)
50	6.992508	2001:beef:cafe:1:200:ff:fe00:1	2001:beef:cafe:3:200:ff:fe00:a	ECHO	282	Request
51	7.008821	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=0 more=y ident=0x8561df05 nxt=17)
52	7.011218	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=1448 more=y ident=0x8561df05 nxt=17)
53	7.013615	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=2896 more=y ident=0x8561df05 nxt=17)
54	7.016012	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	IPv6	1514	IPv6 fragment (off=4344 more=y ident=0x8561df05 nxt=17)
55	7.016339	2001:beef:cafe:3:200:ff:fe00:a	2001:beef:cafe:1:200:ff:fe00:1	ECHO	282	Response

Obrázek 4

BGP (Border Gateway Protocol): [frames 56-83]

Směrovač 10.1.5.1 otevírá nejprve TCP spojení se směrovačem 10.1.5.2 a zasílá mu BGP OPEN zprávu. V tento okamžik nejspíše uzel ještě není nakonfigurovaný jako hraniční BGP směrovač a tím pádem neodpoví a pouze zavře TCP spojení. Následně (frame 64) však sám otevírá TCP spojení se směrovačem 10.1.5.1 a zasílá mu BGP OPEN zprávu. Ta obsahuje údaje o tom, že směrovač 10.1.5.2 zajišťuje přístup k autonomnímu systému číslo 5. 10.1.5.1 odpovídá a oznamuje, že zpřístupňuje AS číslo 1. Následné zprávy UPDATE informují především o dalších dostupných AS v síti. Nakonec je ustanoveno, že AS číslo 1 a 2 jsou dostupné přes 10.1.5.1 a AS číslo 3, 4 a 5 přes 10.1.5.2. Viz Obrázek 5.



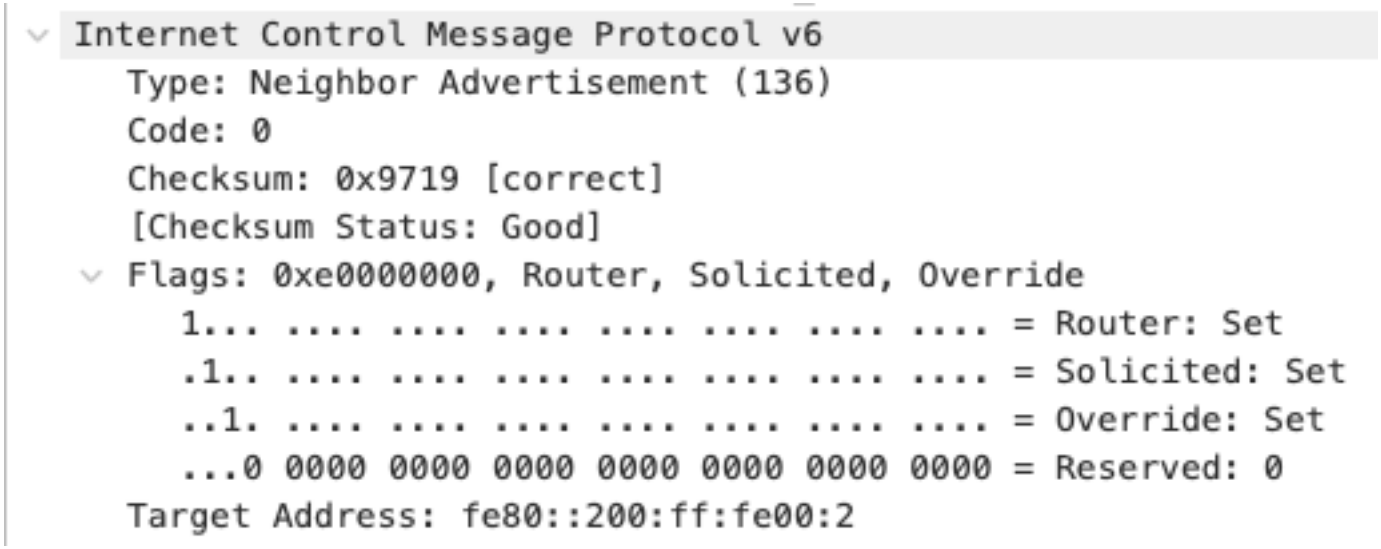
Obrázek 5

ECHO ICMPv6: [frames 84-138]

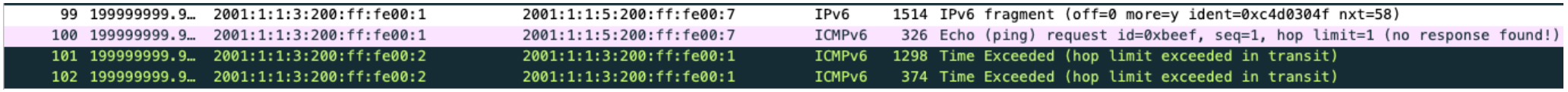
V této části zaznamenaného provozu nejprve dochází pomocí Neighbour Discovery a zpráv Neighbour Solicitation a Neighbour Advertisement k ověření uzly, zda jsou jejich IPv6 adresy unikátní (volné) v dané síti (frames 84-89). Viz tabulka. Následně uzel fe80::200:ff:fe00:1 začíná hledat v síti router pomocí zprávy Router Solicitation (frame 90). Odpověď se mu dostane v podobě zprávy Neighbour Adrertisement (frame 92), kde se díky příznakovému bitu *rtr* dozvídá, že uzel fe80::200:ff:fe00:2 slouží v síti jako router. Viz Obrázek 6.

Následně je od frame 93 zahájena komunikace Echo (ping) přes ICMPv6 protokol mezi klientem 2001:1:1:3:200:ff:fe00:1 a serverem 2001:1:1:5:200:ff:fe00:7 přes směrovač 2001:1:1:3:200:ff:fe00:2. Velikost datové části činní 1700 bajtů a je tedy opět fragmentována, konkrétně na 2 rámce. Hodnota Hop limit v IPv6 hlavičce je však nastavena u těchto paketů na příliš malou hodnotu *1*. Proto hned v dalším skoku, tedy na směrovači 2001:1:1:3:200:ff:fe00:2 jsou zahazovány a zpět na klienta 2001:1:1:3:200:ff:fe00:1 jsou posílány ICMPv6 zprávy Time Exceeded za každý zahozený rámec.Viz Obrázek 7

MAC	link local addr.	global addr.
00:00:00:00:00:01	fe80::200:ff:fe00:1	2001:1:1:3:200:ff:fe00:1
00:00:00:00:00:02	fe80::200:ff:fe00:2	2001:1:1:3:200:ff:fe00:2
00:00:00:00:00:03	fe80::200:ff:fe00:3	2001:1:1:3:200:ff:fe00:3



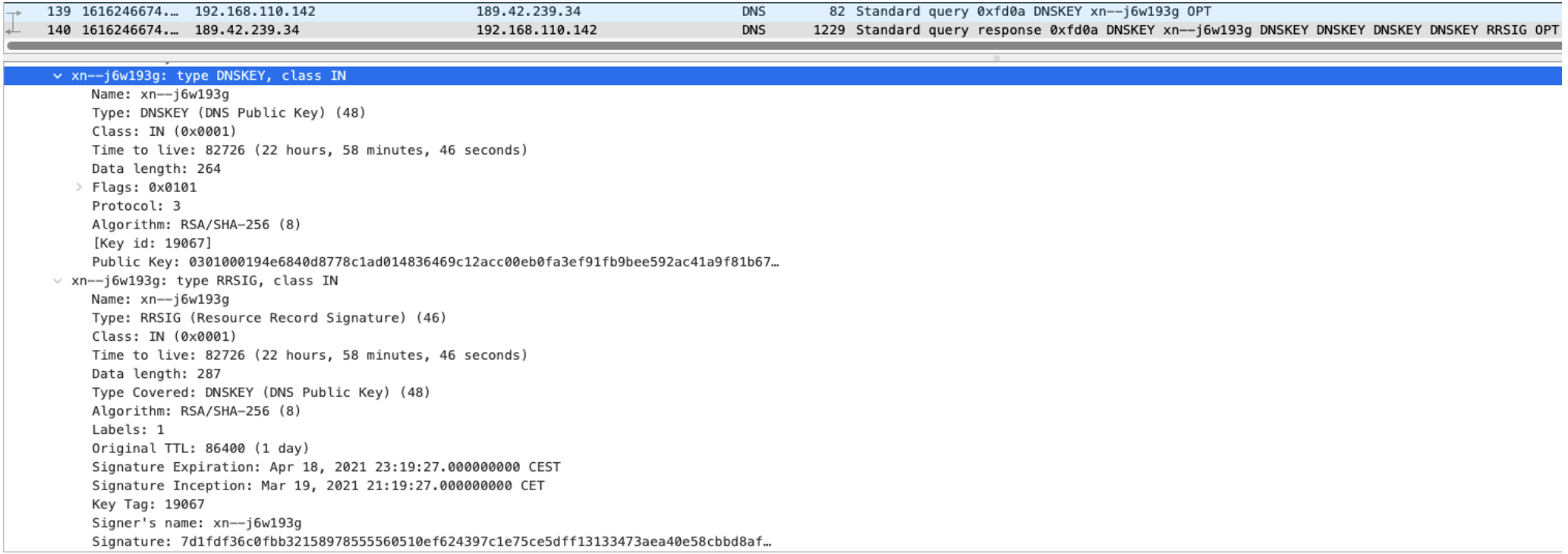
Obrázek 6



Obrázek 7

DNSSEC DNSKEY: [frames 139-140]

V této části komunikace lze vidět DNS dotaz typu DNSKEY (veřejný asymetrický klíč domény) týkající se domény s IDN xn--j6w193g. V konverzi do UNICODE 香港. Jedná se o doménu prvního řádu .hk, tedy domény pro Hong Kong. V žádosti je také nastavený bit *AD (Authenticate Data)*, tedy klient žádá nadřazený resolver o ověření záznamů pomocí DNSSEC. V sekci OPT (v rámci sekce rozšiřujících záznamů) klient také nastavuje bit *DO* a požaduje tak zaslání RRSIG podpisu v rámci odpověďi.
Následně mu je zaslána odpověď obsahující DNSKEY záznamy obsažené u domény .hk, a podpis RRSIG. Viz Je tak zde zajištěna integrita a autentizace dat. Komunikace probíhá v otevřeném formátu pomocí protokolu UDP. Zaslaný klíč a RRSIG viz Obrázek 8.



Obrázek 8

HTTP over TLS: [frames 141-675]

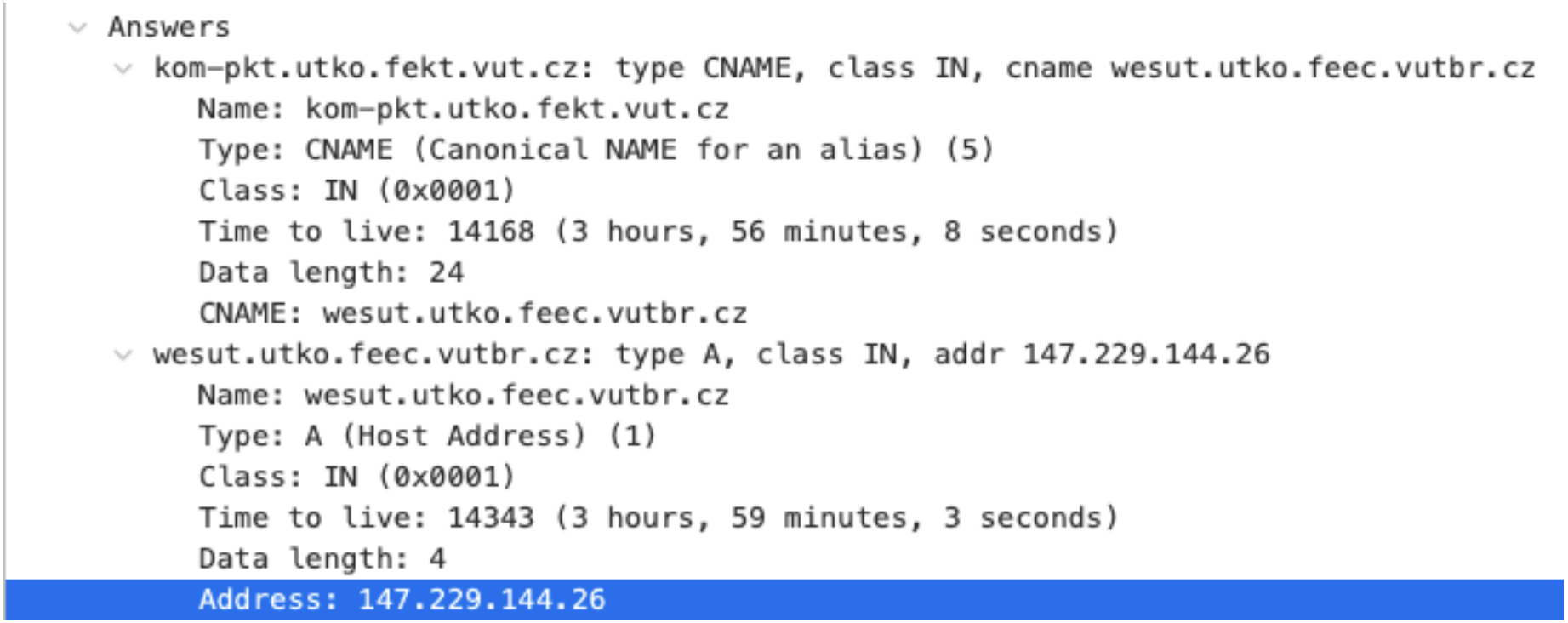
Od frame 141 až po frame 675 probíhá šifrovaná komunikace (zajištěna důvěrnost) pomocí TLS přes TCP. Komuniace směřuje na port 443 → nejspíše HTTPS provoz. Komunikace se účastní klient 192.168.204.132 a pětice serverů patřících společnosti Google 142.251.36.142, 142.251.36.74, 142.251.36.67, 142.251.36.131 a 142.251.37.99. Celkem bylo takto pomocí TLS přeneseno 138 kB dat viz Obrázek 9.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	141	100.0	142240	1454 k	0	0	0
Ethernet	100.0	141	1.4	1974	20 k	0	0	0
Internet Protocol Version 4	100.0	141	2.0	2820	28 k	0	0	0
Transmission Control Protocol	100.0	141	96.6	137344	1403 k	30	600	6133
Transport Layer Security	80.9	114	97.5	138660	1417 k	111	135591	1386 k

Obrázek 9

DNS over UDP: [frames 676-677]

V těchto dvou paketech je vidět žádost stanice 192.168.110.129 na Google DNS server 8.8.8.8 přes UDP s dotazem na záznam typu A (IPv4) k doméně kom-pkt.utko.fekt.vut.cz. V následujícím paketu je obsažena odpověď, která stanici informuje, že kom-pkt.utko.fekt.vut.cz je záznam typu CNAME s hodnotu wesut.utko.feec.vutbr.cz. Druhá část odpovědi informuje o záznamu typu A pro wesut.utko.feec.vutbr.cz respektive pkt.utko.fekt.vut.cz, tedy IPv4 adrese 147.229.144.26. Viz Obrázek 10.



Obrázek 10

HTTP: [frames 678-688]

Následně je pomocí IP adresy získané z předchozí DNS komunikace otevřeno nezabezpečené HTTP spojení s webovým serverem na portu 80 a jsou stažena data webové stránky http://kom-pkt.utko.fekt.vut.cz/page.html. Celá komunikace viz Obrázek 11.

678	1648040460.…	192.168.204.132	147.229.144.26	TCP	66	50759 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
679	1648040460.…	147.229.144.26	192.168.204.132	TCP	60	80 → 50759 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
680	1648040460.…	192.168.204.132	147.229.144.26	TCP	54	50759 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
681	1648040460.…	192.168.204.132	147.229.144.26	HTTP	542	GET /page.html HTTP/1.1
682	1648040460.…	147.229.144.26	192.168.204.132	TCP	60	80 → 50759 [ACK] Seq=1 Ack=489 Win=64240 Len=0
683	1648040460.…	147.229.144.26	192.168.204.132	HTTP	610	HTTP/1.1 200 OK (text/html)
684	1648040460.…	192.168.204.132	147.229.144.26	TCP	54	50759 → 80 [ACK] Seq=489 Ack=557 Win=63684 Len=0
685	1648040465.…	147.229.144.26	192.168.204.132	TCP	60	80 → 50759 [FIN, PSH, ACK] Seq=557 Ack=489 Win=64240 Len=0
686	1648040465.…	192.168.204.132	147.229.144.26	TCP	54	50759 → 80 [ACK] Seq=489 Ack=558 Win=63684 Len=0
687	1648040465.…	192.168.204.132	147.229.144.26	TCP	54	50759 → 80 [FIN, ACK] Seq=489 Ack=558 Win=63684 Len=0
688	1648040465.…	147.229.144.26	192.168.204.132	TCP	60	80 → 50759 [ACK] Seq=558 Ack=490 Win=64239 Len=0

Obrázek 11

DNS over TCP: [frames 689-698]

V poslední části zkoumaného souboru je možné vidět DNS dotazování pomocí TCP spojení. V paketech 689 až 691 je nejprve otevřeno samotné TCP spojení, poté je zaslán opět DNS dotaz na doménu kom-pkt.utko.fekt.vut.cz, ale tentokrát je pomocí bitu AD a DO, vyžadováno po nadřazeném resolveru ověření zasílaných dat pomocí DNSSEC a zároveň zaslání i podpisu RRSIG.
V odpovědi obsažené v paketu 694 jsou zaslány všechna tato vyžádaná data, tedy opět hodnota CNAME S RRSIG a poté A s RRSIG.
Poté je už pouze ukončeno TCP spojení. Vše viz Obrázek 12.

689	1648107911.…	192.168.204.132	1.1.1.1	TCP	66	51129 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
690	1648107911.…	1.1.1.1	192.168.204.132	TCP	60	53 → 51129 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
691	1648107911.…	192.168.204.132	1.1.1.1	TCP	54	51129 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
692	1648107911.…	192.168.204.132	1.1.1.1	DNS	109	Standard query 0x6a66 A kom-pkt.utko.fekt.vut.cz OPT
693	1648107911.…	1.1.1.1	192.168.204.132	TCP	60	53 → 51129 [ACK] Seq=1 Ack=56 Win=64240 Len=0
694	1648107911.…	1.1.1.1	192.168.204.132	DNS	761	Standard query response 0x6a66 A kom-pkt.utko.fekt.vut.cz CNAME wesut.utko.feec.vutbr.cz RRSIG A 147.229.144.26 RRSIG OPT
695	1648107911.…	192.168.204.132	1.1.1.1	TCP	54	51129 → 53 [FIN, ACK] Seq=56 Ack=708 Win=63533 Len=0
696	1648107911.…	1.1.1.1	192.168.204.132	TCP	60	53 → 51129 [ACK] Seq=708 Ack=57 Win=64239 Len=0
697	1648107911.…	1.1.1.1	192.168.204.132	TCP	60	53 → 51129 [FIN, PSH, ACK] Seq=708 Ack=57 Win=64239 Len=0
698	1648107911.…	192.168.204.132	1.1.1.1	TCP	54	51129 → 53 [ACK] Seq=57 Ack=709 Win=63533 Len=0

Obrázek 12
