Wireshark Ping

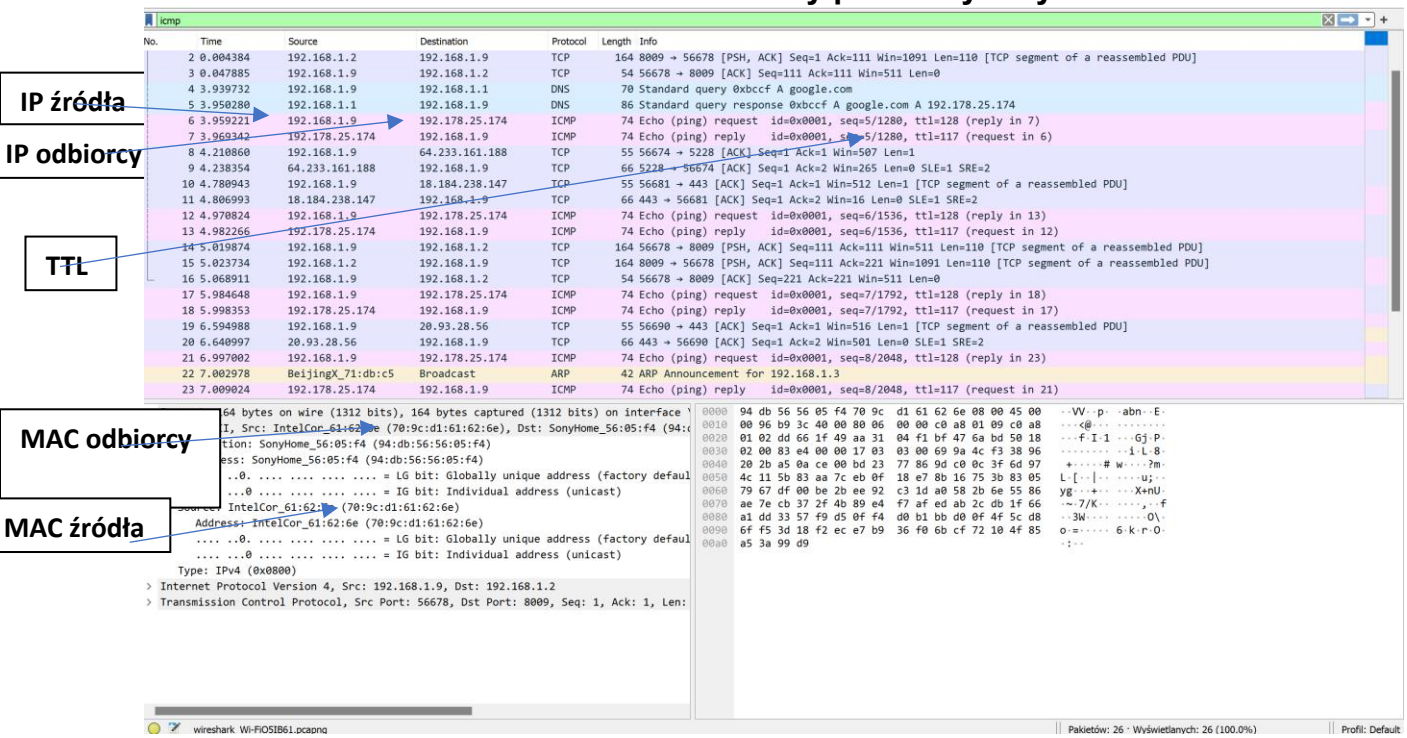
1. **Ile wiadomości i jakiego typu wysłał komputer?**

Polecenie ping wysyła wiadomości ICMP Echo Request do docelowego hosta. Domyślnie wysyłane są cztery takie wiadomości.

2. **Ile wiadomości i jakiego typu otrzymał komputer?**

Po wysłaniu wiadomości ICMP Echo Request, komputer oczekuje na odpowiedź ICMP Echo Reply od docelowego hosta. Jeśli host docelowy jest dostępny i skonfigurowany do odpowiadania na pakiety ping, komputer otrzyma cztery wiadomości ICMP Echo Reply.

3. **Określić adres IP oraz MAC źródła i odbiorcy przechwyconych wiadomości ICMP.**



4. **Jakie są różnice pomiędzy adresem IPv4 i MAC?**

Różnice między adresem IPv4 a adresem MAC zostały opisane wcześniej w odpowiedzi na wcześniejsze pytanie.

5. **Określić wartość parametru TTL.**

TTL (Time to Live) to parametr, który jest używany w pakietach IP. Określa maksymalną liczbę skoków (routingu) jakie pakiet może przejść, zanim zostanie odrzucony. Każdy router, przez który przechodzi pakiet, dekrementuje wartość TTL o 1. Jeśli wartość TTL osiągnie 0, pakiet jest odrzucany.

6. **Co to jest TTL i dlaczego jest ustawiany w pakietach IP?**

TTL jest ustawiany w pakietach IP, aby zapobiec nieskończonym pętlom pakietów w sieci. Działa jako mechanizm zapobiegający zbyt długiemu przetrzymywaniu pakietów w sieci, gdyż w przypadku awarii routera lub pętli w sieci, pakiety z TTL równym 0 są odrzucane.

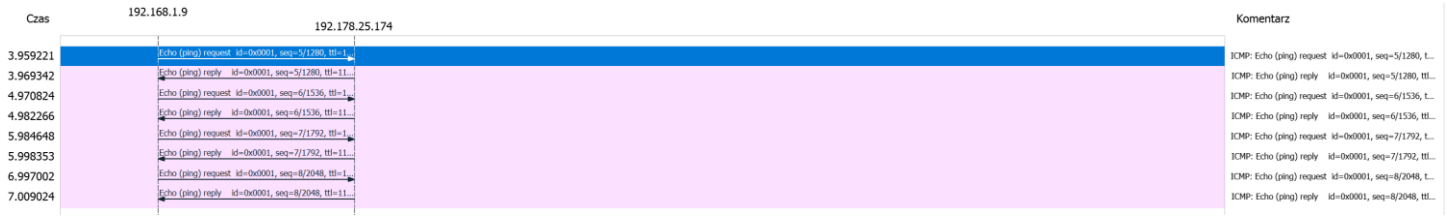
7. **Czy pole o podobnym znaczeniu znajduje się w ramce Ethernetowej?**

W ramce Ethernetowej pole o podobnym znaczeniu to pole Length/Type, które określa długość ramki lub typ protokołu warstwy wyższej, jak IP. Nie ma jednak bezpośredniego pola TTL w ramce Ethernetowej.

8. **Co się stanie jeżeli polecenie ping zostanie użyte z przełącznikiem –i 2: ping google.com –i 2**

Przełącznik "-i 2" oznacza, że zostaną wysłane pakiety ping co 2 sekundy, zamiast standardowego czasu oczekiwania. Oznacza to, że komputer będzie wysyłał wiadomości ICMP Echo Request co 2 sekundy, a nie czekał na odpowiedzi. Może to prowadzić do większej ilości przesyłanych pakietów.

9. **Narysuj graf przepływu.**



Wireshark Tracert

6	4.524882	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=39/9984, ttl=1 (no response found!)
7	4.527605	192.168.1.1	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
8	4.528458	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=40/10240, ttl=1 (no response found!)
9	4.529326	192.168.1.1	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
10	4.529948	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=41/10496, ttl=1 (no response found!)
11	4.530663	192.168.1.1	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
17	5.539262	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=42/10752, ttl=2 (no response found!)
18	5.548325	213.158.195.232	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
19	5.549296	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=43/11008, ttl=2 (no response found!)
20	5.555705	213.158.195.232	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
21	5.556452	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=44/11264, ttl=2 (no response found!)
22	5.564708	213.158.195.232	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
38	11.520838	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=45/11520, ttl=3 (no response found!)
45	15.269297	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=46/11776, ttl=3 (no response found!)
47	19.277132	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=47/12032, ttl=3 (no response found!)
54	23.271286	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=48/12288, ttl=4 (no response found!)
55	23.282563	213.158.215.72	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
56	23.283815	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=49/12544, ttl=4 (no response found!)
57	23.292269	213.158.215.72	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
58	23.293307	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=50/12800, ttl=4 (no response found!)
59	23.302666	213.158.215.72	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
76	29.263652	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=51/13056, ttl=5 (no response found!)
77	29.274984	157.25.255.211	192.168.1.9	ICMP	182 Time-to-live exceeded (Time to live exceeded in transit)
78	29.276204	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=52/13312, ttl=5 (no response found!)
79	29.286641	157.25.255.211	192.168.1.9	ICMP	182 Time-to-live exceeded (Time to live exceeded in transit)
80	29.287959	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=53/13568, ttl=5 (no response found!)
81	29.298669	157.25.255.211	192.168.1.9	ICMP	182 Time-to-live exceeded (Time to live exceeded in transit)
94	35.263597	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=54/13824, ttl=6 (no response found!)
98	35.274724	157.25.255.240	192.168.1.9	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
99	35.275777	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=55/14080, ttl=6 (no response found!)
100	35.283949	157.25.255.240	192.168.1.9	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
101	35.285146	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=56/14336, ttl=6 (no response found!)
102	35.294351	157.25.255.240	192.168.1.9	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
106	35.736742	157.25.255.240	192.168.1.9	ICMP	110 Destination unreachable (Port unreachable)
108	37.247292	157.25.255.240	192.168.1.9	ICMP	110 Destination unreachable (Port unreachable)
110	38.758725	157.25.255.240	192.168.1.9	ICMP	110 Destination unreachable (Port unreachable)
114	41.253217	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=57/14592, ttl=7 (no response found!)
115	41.267758	213.158.211.69	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
116	41.277557	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=58/14848, ttl=7 (no response found!)
117	41.285471	213.158.211.69	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
118	41.286992	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=59/15104, ttl=7 (no response found!)
119	41.296242	213.158.211.69	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
121	42.305201	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=60/15360, ttl=8 (no response found!)
122	42.315620	142.251.65.249	192.168.1.9	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
123	42.316456	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=61/15616, ttl=8 (no response found!)
124	42.327189	142.251.65.249	192.168.1.9	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
125	42.328074	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=62/15872, ttl=8 (no response found!)
126	42.337414	142.251.65.249	192.168.1.9	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
137	48.282969	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=63/16128, ttl=9 (no response found!)
138	48.294681	142.251.234.57	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
139	48.303882	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=64/16384, ttl=9 (no response found!)
140	48.314439	142.251.234.57	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
141	48.315352	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=65/16640, ttl=9 (no response found!)
142	48.323114	142.251.234.57	192.168.1.9	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
154	54.304012	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=66/16896, ttl=10 (reply in 155)
155	54.315746	192.178.25.174	192.168.1.9	ICMP	106 Echo (ping) reply id=0x0001, seq=66/16896, ttl=117 (request in 154)
156	54.316939	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=67/17152, ttl=10 (reply in 157)
157	54.325572	192.178.25.174	192.168.1.9	ICMP	106 Echo (ping) reply id=0x0001, seq=67/17152, ttl=117 (request in 156)
158	54.326401	192.168.1.9	192.178.25.174	ICMP	106 Echo (ping) request id=0x0001, seq=68/17408, ttl=10 (reply in 159)
159	54.335133	192.178.25.174	192.168.1.9	ICMP	106 Echo (ping) reply id=0x0001, seq=68/17408, ttl=117 (request in 158)

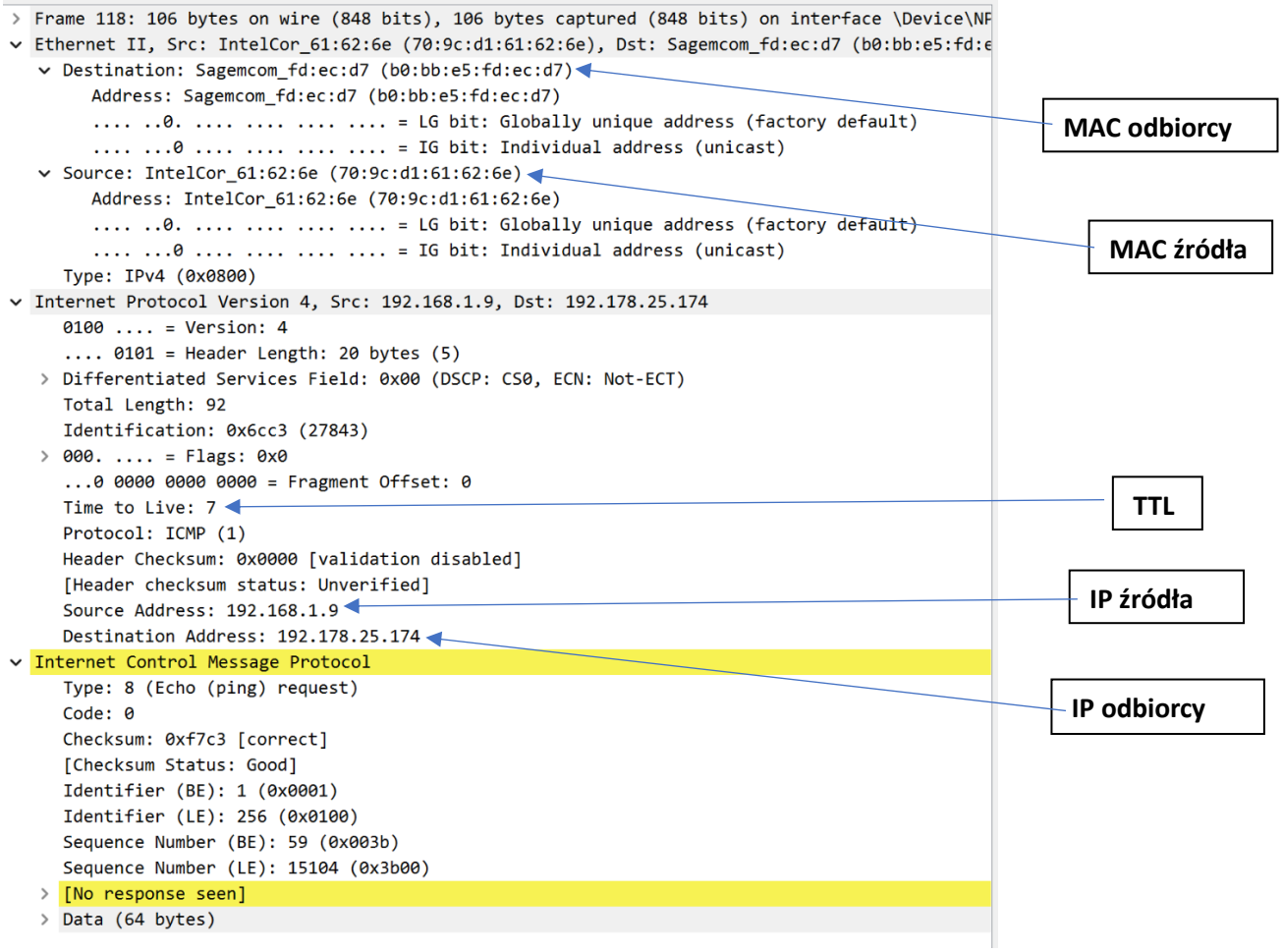
1. **Ile wiadomości i jakiego typu wysłał komputer?**

Polecenie tracert wysyła wiadomości ICMP Echo Request (czasami nazywane Time Exceeded) z rosnącymi wartościami TTL. Liczba wysłanych wiadomości zależy od liczby routerów (hopów) między komputerem a docelowym adresem IP.

2. **Ile wiadomości i jakiego typu odebrał komputer?**

Komputer odbierze odpowiedzi ICMP Time Exceeded (czasami ICMP Echo Reply), które są generowane przez routery, gdy pakiet przekracza wartość TTL. Liczba odebranych wiadomości zależy od liczby routerów między komputerem a docelowym adresem IP oraz od konfiguracji tych routerów.

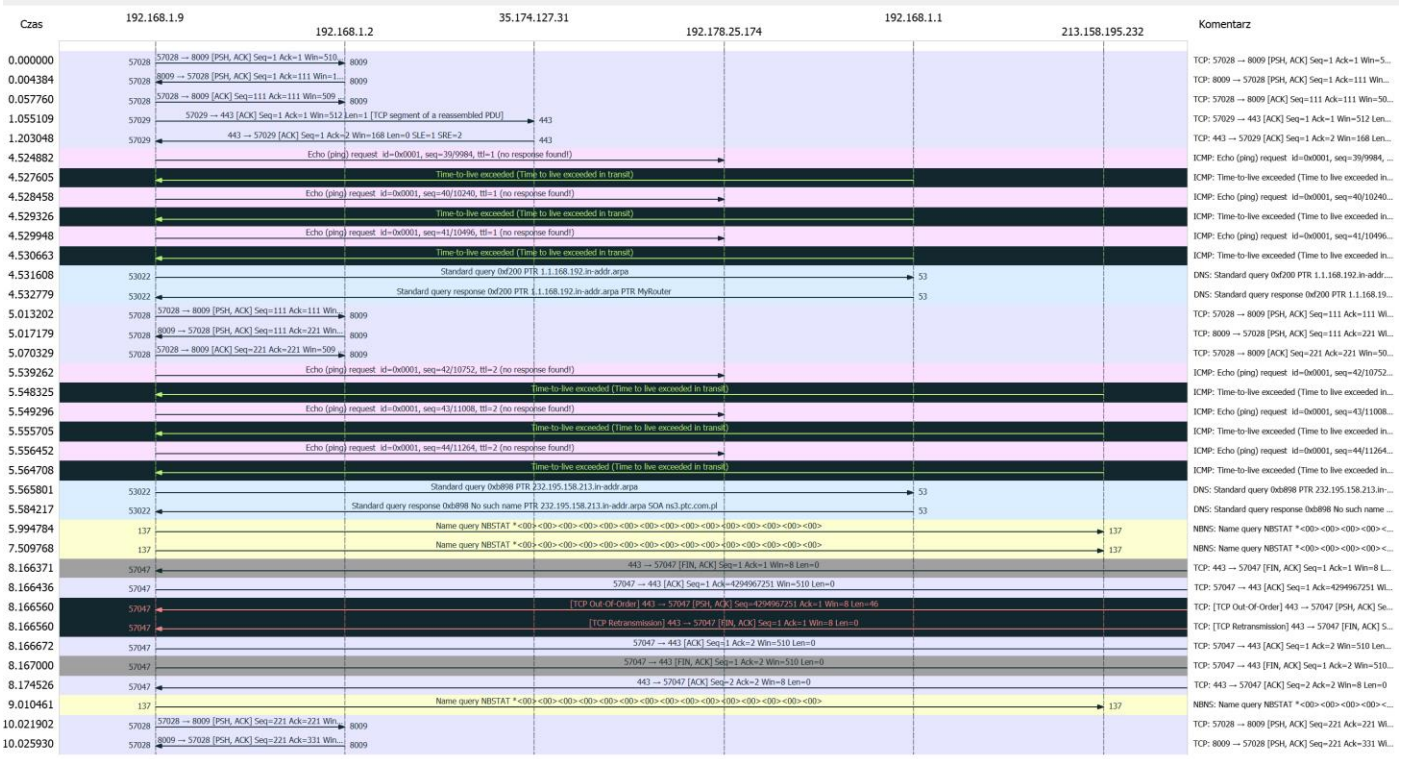
3. Określić adres IP oraz MAC źródła i odbiorcy przechwyconych wiadomości ICMP.



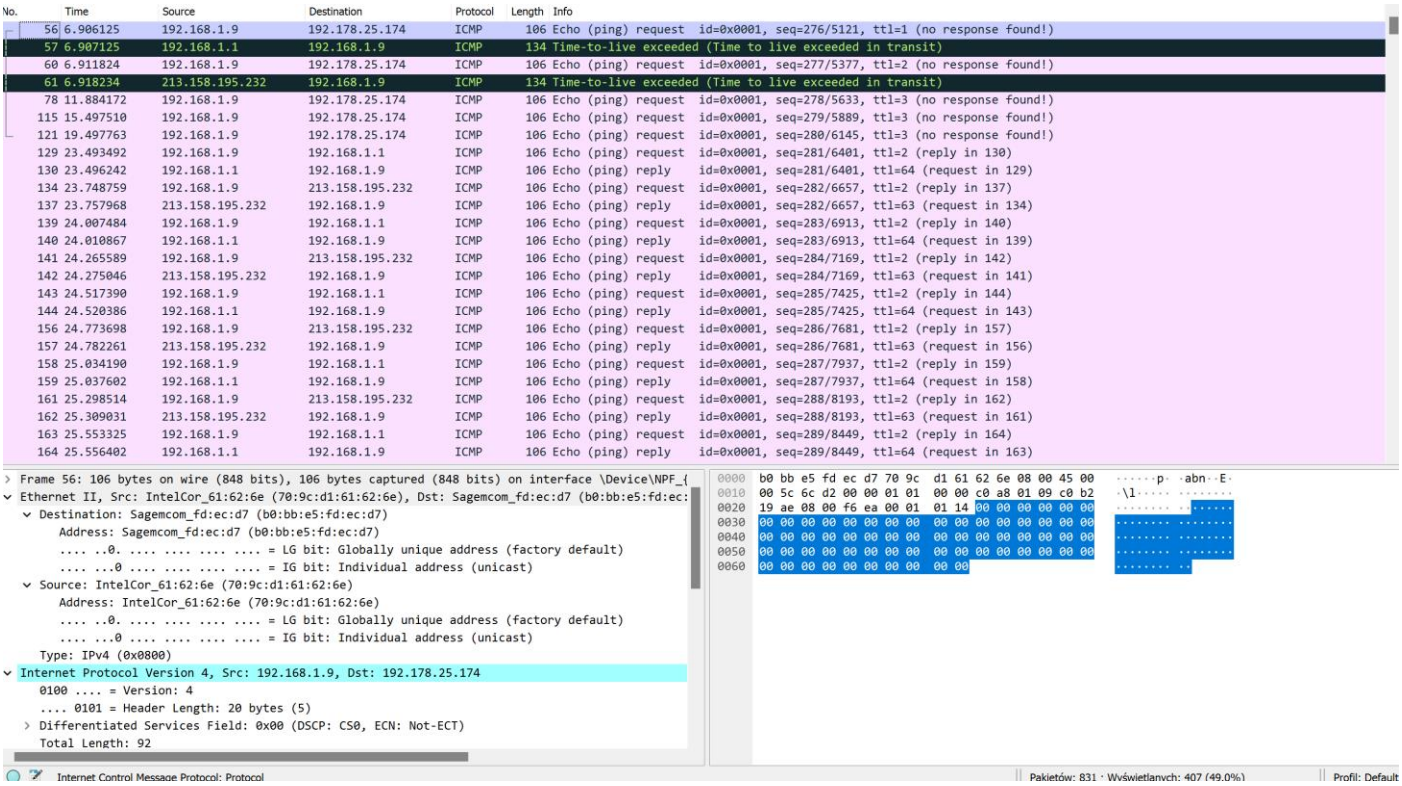
4. Określić wartość parametru TTL w poszczególnych pakietach.

Wartość parametru TTL w poszczególnych pakietach będzie rosnąca w miarę przesyłania ich przez routery. Każdy router dekrementuje wartość TTL o 1. Można śledzić wartość TTL w przechwyconych pakietach w programie Wireshark.

5. Narysuj graf przepływu pakietów (na podstawie grafu wygenerowanego przez Wireshark).



Wireshark Patchping



1. Ile wiadomości i jakiego typu wysłał komputer?

Polecenie pathping wysyła wiadomości ICMP Echo Request (ping) do docelowego hosta. Liczba wysłanych wiadomości zależy od ustawień domyślnych systemu operacyjnego, ale zazwyczaj są wysyłane trzy pakiety ICMP Echo Request na każdy router na ścieżce do docelowego hosta.

2. Ile wiadomości i jakiego typu odebrał komputer?

Komputer odbiera odpowiedzi ICMP Echo Reply od docelowego hosta oraz wiadomości ICMP Time Exceeded (czasami ICMP Echo Reply) generowane przez routery, gdy pakiet przekracza wartość

TTL. Liczba odebranych wiadomości zależy od liczby routerów między komputerem a docelowym adresem IP oraz od konfiguracji tych routerów.

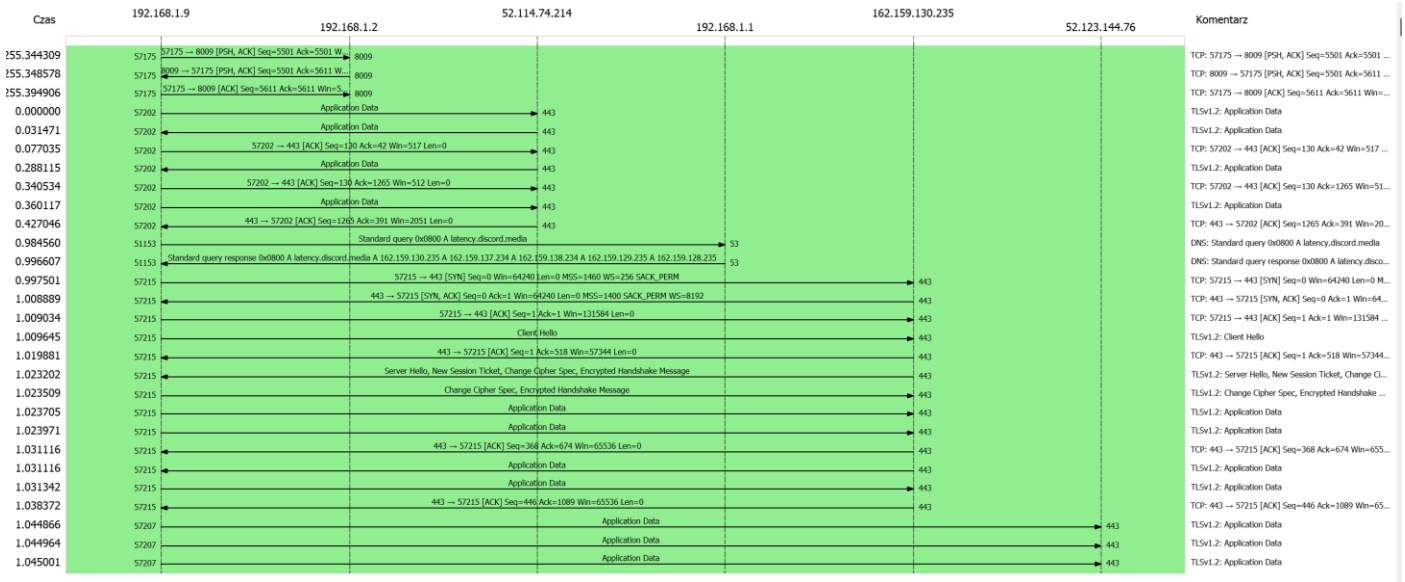
3. **Czy w wysyłanych (odbieranych) pakietach zmieniana jest wartość parametru TTL, jeśli tak to w jaki sposób?**

Wysyłane pakiety ICMP Echo Request mają wartość TTL zwiększaną o 1 na każdym hopie, czyli na każdym routerze na trasie do docelowego hosta. Odbierane pakiety mogą mieć różne wartości TTL, ponieważ są generowane przez routery i zależą od konfiguracji tych routerów.

4. **Na podstawie przechwyconych pakietów z wiadomościami protokołu ICMP przedstaw zasadę działania polecenia pathping.**

Polecenie pathping jest hybrydą polecenia ping i tracert. Wysyła ono pakiety ICMP Echo Request do docelowego hosta, jak w przypadku ping, ale jednocześnie analizuje odpowiedzi Time Exceeded (czasami ICMP Echo Reply) generowane przez routery, jak w przypadku tracert. Pathping śledzi ścieżkę pakietów i oblicza statystyki opóźnień i utraty pakietów na każdym hopie między komputerem a docelowym adresem IP.

5. **Narysuj uproszczony graf przepływu.**



Wireshark Telnet oraz SSH

Telnet

1. **Jakie informacje przedstawia program po wyborze opcji Follow TCP Stream?**

Po wybraniu opcji "Follow TCP Stream" w programie Wireshark, zostanie otwarte nowe okno, w którym wyświetlane są wszystkie przepływające pakiety TCP w ramach tego strumienia. W tym oknie można zobaczyć zarówno dane wysyłane przez klienta (np. polecenia, login, hasło) oraz dane otrzymywane z serwera (np. odpowiedzi, komunikaty).

2. **Co można powiedzieć o protokole telnet?**

Protokół telnet jest protokołem sieciowym używanym do zdalnego logowania na serwery. Umożliwia zdalny dostęp do wiersza poleceń na zdalnym hoście i przesyłanie danych tekstowych między klientem a serwerem. Protokół telnet działa na warstwie aplikacji modelu OSI i używa protokołu TCP do nawiązywania połączenia.

3. **W jaki sposób przesyłane są login i hasło?**

Login i hasło przesyłane są w formie niezaszyfrowanej (plain text) przez protokół telnet. Oznacza to, że dane są przesyłane w postaci zrozumiałej dla człowieka i mogą być odczytane przez osoby podsłuchujące ruch sieciowy. Dlatego korzystanie z protokołu telnet w sieciach publicznych lub niezaufanych jest niebezpieczne, ponieważ może prowadzić do przechwycenia poufnych informacji uwierzytelniających. W celu zapewnienia bezpieczeństwa przesyłanych danych, zaleca się

stosowanie protokołu SSH (Secure Shell) zamiast telnetu, ponieważ SSH szyfruje dane i zapewnia bezpieczne zdalne logowanie i przesyłanie informacji.

SSH

1. **Jakie informacje przedstawia program po wyborze opcji Follow TCP Stream?**

Po wybraniu opcji "Follow TCP Stream" w programie Wireshark, zostanie otwarte nowe okno, w którym wyświetlane są wszystkie przepływające pakiety TCP w ramach tego strumienia. W tym oknie można zobaczyć dane wysyłane i otrzymywane między klientem a serwerem, w formacie zrozumiałym dla człowieka.

2. **Co można powiedzieć o protokole telnet**

Protokół SSH (Secure Shell) jest protokołem sieciowym, który zapewnia bezpieczne zdalne logowanie i przesyłanie danych. W przeciwieństwie do protokołu telnet, SSH używa szyfrowania, takiego jak asymetryczne szyfrowanie klucza publicznego, aby chronić poufne informacje uwierzytelniające, takie jak login i hasło. SSH również zapewnia integralność i uwierzytelnianie serwera.

3. **W jaki sposób przesyłane są login i hasło?**

W protokole SSH login i hasło przesyłane są w formie zaszyfrowanej, co oznacza, że dane są nieczytelne dla osób podsłuchujących ruch sieciowy. Protokół SSH wykorzystuje protokoły kryptograficzne do nawiązywania bezpiecznego połączenia i wymiany kluczy kryptograficznych, a następnie szyfruje dane przesyłane między klientem a serwerem.

Który sposób łączenia się z serwerem jest bardziej bezpieczny?
Protokół SSH jest znacznie bardziej bezpieczny niż protokół telnet. Protokół SSH zapewnia uwierzytelnienie i szyfrowanie, co oznacza, że dane przesyłane przez SSH są chronione przed przechwyceniem i odczytaniem przez osoby nieuprawnione. W porównaniu, protokół telnet przesyła dane w formie niezaszyfrowanej, co sprawia, że są one podatne na przechwycenie i odczytanie przez osoby trzecie. W związku z tym zaleca się korzystanie z protokołu SSH zamiast telnetu, zwłaszcza w przypadku przesyłania poufnych informacji.

Wireshark FTP

Podczas analizy pakietów związanych z połączeniem FTP można zobaczyć, że dane uwierzytelniające, takie jak login i hasło, są przesyłane w postaci zrozumiałej dla człowieka (plain text). Protokół FTP nie zapewnia domyślnie szyfrowania danych ani uwierzytelniania serwera, co oznacza, że dane przesyłane za pomocą FTP są narażone na przechwycenie i odczytanie przez osoby trzecie.

W odniesieniu do pytania, czy istnieje bezpieczniejszy sposób przesyłania plików niż FTP, odpowiedź brzmi tak. Protokół FTP nie jest uważany za bezpieczny ze względu na brak szyfrowania i uwierzytelniania. Istnieje jednak wiele innych protokołów, które zapewniają bezpieczne przesyłanie plików, takie jak FTPS (FTP over SSL/TLS) i SFTP (SSH File Transfer Protocol).

FTPS to rozszerzenie protokołu FTP, które dodaje warstwę SSL/TLS do komunikacji FTP, umożliwiając szyfrowanie danych i uwierzytelnianie serwera. SFTP natomiast jest integralną częścią protokołu SSH i zapewnia bezpieczne przesyłanie plików poprzez szyfrowanie i uwierzytelnianie.

Wniosek: Jeśli chodzi o bezpieczeństwo przesyłania plików, FTP nie jest zalecanym protokołem ze względu na brak zabezpieczeń. Bezpieczniejsze opcje to korzystanie z FTPS lub SFTP, które oferują szyfrowanie i uwierzytelnianie.