Grupa lab. 3	*Data wykonania* 15.11.2022r.	*Data odbioru*
Temat ćwiczenia Wireshark – Scenariusz nr 1		
Imiona i nazwiska. Maksymilian Kubiczek i Jakub Litewka		*Ocena i uwagi*

Część praktyczna

Opis wykonanego ćwiczenia:

Sprzęt:

Komputer PC

System operacyjny Windows 7

Oprogramowanie:

Wireshark

Schemat ćwiczenia

1. Uruchomić program Wireshark
2. Pole capture filter zostawić puste
3. Wybrać interfejs wykorzystywany do połączenia z siecią poprzez dwukrotne kliknięcie
4. Wykonać następujące czynności
   a. Uruchomić przeglądarkę i wejść na stronę www: http://……. agh.io.pl
   b. Uruchomić linię poleceń (cmd.exe) i wykonać i ping do adresu: ……. agh.io.pl
   c. Wykonać połączenie z serwerem ftp: ftp://……. ftp.agh.edu.pl
5. Po wykonaniu wybranych połączeń należy zakończyć przechwytywanie pakietów
6. Wykorzystując stworzony zapis ruchu sieciowego należy wykonać następujące operacje:
   a. Wykonać zrzut ekran przedstawiający żądanie i odpowiedź DNS dla domen ustalonych w punktach 4a, 4b i 4c
   b. Na podstawie odpowiedzi z serwera DNS określić adresy IP powiązanie z domenami ustalonymi w punktach 4a i 4b
   c. Wykonać zrzut ekranu przedstawiający pakiety odpowiedzialne za nawiązanie połączenia TCP (Three-way handshake) z domeną ustaloną w punkcie 4a
   d. Dla połączenia z punktu 4a wykonać zrzut ekranu przedstawiający żądania HTTP GET oraz odpowiedź na to żądanie
   e. Wykonać zrzut ekranu pakietów Echo Request i Echo Reply powiązanych z wykonanym poleceniem ping do adresu z punktu 4b
   f. Wykonać zrzuty ekranu pakietów zawierających początkową fazę komunikacje z serwerem ftp: wysłanie loginu (+odpowiedź), wysłanie hasła (+odpowiedź), żądanie nazwy, aktualnego katalogu po stronie serwera (+odpowiedź), żądanie o zawartości aktualnego katalogu po stronie serwera (+odpowiedź)

Wyniki pomiarów:

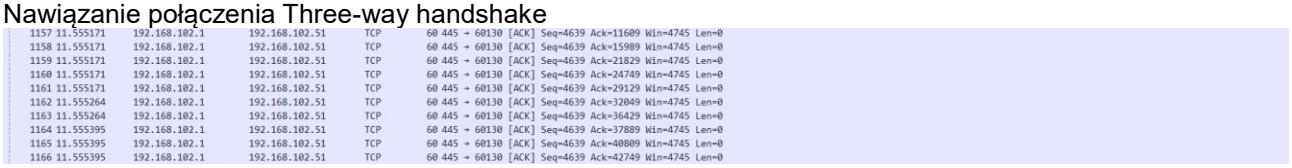
1.

a) Żądanie i odpowiedź DNS dla wybranych

766	9.293684	192.168.102.51	192.168.102.1	DNS	79 Standard query 0xb2ab A ajax.googleapis.com
769	9.297372	192.168.102.51	192.168.102.1	DNS	69 Standard query 0x8106 AAAA agh-io.pl
770	9.297764	192.168.102.1	192.168.102.51	DNS	120 Standard query response 0x8106 AAAA agh-io.pl SOA dns.home.pl
778	9.320638	192.168.102.51	149.156.111.10	DNS	79 Standard query 0xb2ab A ajax.googleapis.com
779	9.328131	192.168.102.1	192.168.102.51	DNS	95 Standard query response 0xb2ab A ajax.googleapis.com A 216.58.209.10
780	9.328871	192.168.102.51	192.168.102.1	DNS	79 Standard query 0x5907 A ajax.googleapis.com
781	9.329187	192.168.102.1	192.168.102.51	DNS	95 Standard query response 0x5907 A ajax.googleapis.com A 216.58.209.10
782	9.329773	192.168.102.51	192.168.102.1	DNS	79 Standard query 0xef0a AAAA ajax.googleapis.com
799	9.351691	149.156.111.10	192.168.102.51	DNS	95 Standard query response 0xb2ab A ajax.googleapis.com A 142.250.203.202
802	9.351886	192.168.102.51	149.156.111.10	DNS	79 Standard query 0xef0a AAAA ajax.googleapis.com
805	9.352786	149.156.111.10	192.168.102.51	DNS	362 Standard query response 0xef0a AAAA ajax.googleapis.com AAAA 2a00:1450:401b:80e::200a NS ns2.google.com NS ns1.google.com NS ns3.google.com NS ns4.googl…
807	9.362661	192.168.102.1	192.168.102.51	DNS	107 Standard query response 0xef0a AAAA ajax.googleapis.com AAAA 2a00:1450:401b:80e::200a

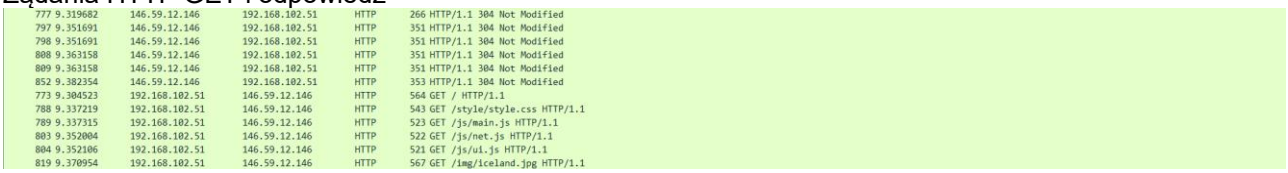
b) Serwer DNS powiązany z adresem agh-io.pl to dns.home.pl o adresie 217.160.80.244

c) Nawiązanie połączenia Three-way handshake



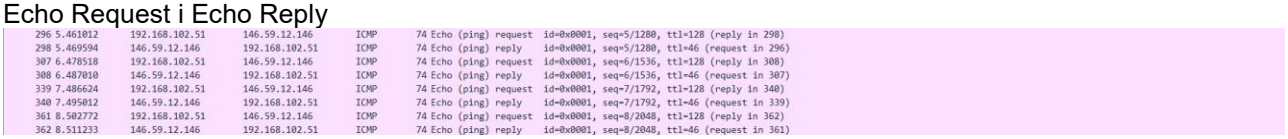
1157	11.555171	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=11609 Win=4745 Len=0
1158	11.555171	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=15989 Win=4745 Len=0
1159	11.555171	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=21829 Win=4745 Len=0
1160	11.555171	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=24749 Win=4745 Len=0
1161	11.555171	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=29129 Win=4745 Len=0
1162	11.555264	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=32049 Win=4745 Len=0
1163	11.555264	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=36429 Win=4745 Len=0
1164	11.555395	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=37889 Win=4745 Len=0
1165	11.555395	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=40809 Win=4745 Len=0
1166	11.555395	192.168.102.1	192.168.102.51	TCP	60 445 → 60130 [ACK] Seq=4639 Ack=42749 Win=4745 Len=0

d) Żądania HTTP GET i odpowiedź



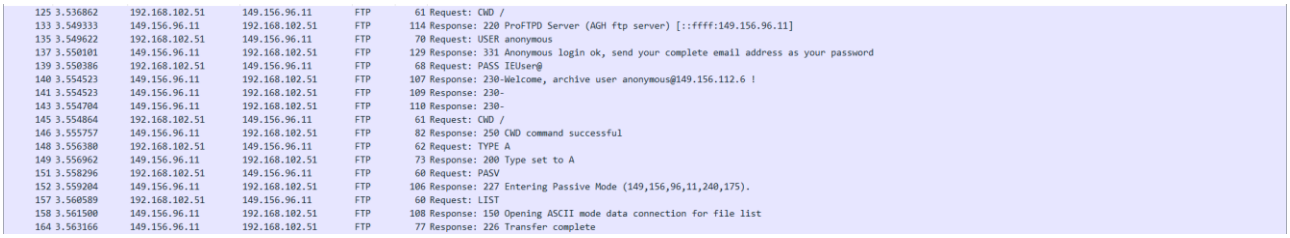
```
777 9.319682    146.59.12.146     192.168.102.51    HTTP    266 HTTP/1.1 304 Not Modified
797 9.351691    146.59.12.146     192.168.102.51    HTTP    351 HTTP/1.1 304 Not Modified
798 9.351691    146.59.12.146     192.168.102.51    HTTP    351 HTTP/1.1 304 Not Modified
808 9.363158    146.59.12.146     192.168.102.51    HTTP    351 HTTP/1.1 304 Not Modified
809 9.363158    146.59.12.146     192.168.102.51    HTTP    351 HTTP/1.1 304 Not Modified
852 9.382354    146.59.12.146     192.168.102.51    HTTP    353 HTTP/1.1 304 Not Modified
773 9.304523    192.168.102.51    146.59.12.146     HTTP    564 GET / HTTP/1.1
788 9.337219    192.168.102.51    146.59.12.146     HTTP    543 GET /style/style.css HTTP/1.1
789 9.337315    192.168.102.51    146.59.12.146     HTTP    523 GET /js/main.js HTTP/1.1
803 9.352004    192.168.102.51    146.59.12.146     HTTP    522 GET /js/net.js HTTP/1.1
804 9.352106    192.168.102.51    146.59.12.146     HTTP    521 GET /js/ui.js HTTP/1.1
819 9.370954    192.168.102.51    146.59.12.146     HTTP    567 GET /img/iceland.jpg HTTP/1.1
```

e) Echo Request i Echo Reply



```
296 5.461012    192.168.102.51    146.59.12.146     ICMP     74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 298)
298 5.469594    146.59.12.146     192.168.102.51    ICMP     74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=46 (request in 296)
307 6.478518    192.168.102.51    146.59.12.146     ICMP     74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 308)
308 6.487010    146.59.12.146     192.168.102.51    ICMP     74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=46 (request in 307)
339 7.486624    192.168.102.51    146.59.12.146     ICMP     74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 340)
340 7.495012    146.59.12.146     192.168.102.51    ICMP     74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=46 (request in 339)
361 8.502772    192.168.102.51    146.59.12.146     ICMP     74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (reply in 362)
362 8.511233    146.59.12.146     192.168.102.51    ICMP     74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=46 (request in 361)
```

f) FTP



```
125 3.536862    192.168.102.51    149.156.96.11     FTP      61 Request: CWD /
133 3.549333    149.156.96.11     192.168.102.51    FTP     114 Response: 220 ProFTPD Server (AGH ftp server) [::ffff:149.156.96.11]
135 3.549622    192.168.102.51    149.156.96.11     FTP      70 Request: USER anonymous
137 3.550101    149.156.96.11     192.168.102.51    FTP     129 Response: 331 Anonymous login ok, send your complete email address as your password
139 3.550386    192.168.102.51    149.156.96.11     FTP      68 Request: PASS IEUser@
140 3.554523    149.156.96.11     192.168.102.51    FTP     107 Response: 230-Welcome, archive user anonymous@149.156.112.6 !
141 3.554523    149.156.96.11     192.168.102.51    FTP     109 Response: 230-
143 3.554704    149.156.96.11     192.168.102.51    FTP     110 Response: 230-
145 3.554864    192.168.102.51    149.156.96.11     FTP      61 Request: CWD /
146 3.555757    149.156.96.11     192.168.102.51    FTP      82 Response: 250 CWD command successful
148 3.556380    192.168.102.51    149.156.96.11     FTP      62 Request: TYPE A
149 3.556962    149.156.96.11     192.168.102.51    FTP      73 Response: 200 Type set to A
151 3.558296    192.168.102.51    149.156.96.11     FTP      60 Request: PASV
152 3.559204    149.156.96.11     192.168.102.51    FTP     106 Response: 227 Entering Passive Mode (149,156,96,11,240,175).
157 3.560589    192.168.102.51    149.156.96.11     FTP      60 Request: LIST
158 3.561500    149.156.96.11     192.168.102.51    FTP     108 Response: 150 Opening ASCII mode data connection for file list
164 3.563166    149.156.96.11     192.168.102.51    FTP      77 Response: 226 Transfer complete
```

2.

- Zawartość nagłówków IP, UDP, DNS dla żądania do serwera DNS

IP (Warstwa Internetowa)					
0-3	4-7	8-13	14-15	16-18	19-31
Wersja: 4	Dł.nag: 20	DSF: 0x00	ECN: 0	Dł.całkowita: 55	
Nr. Ident: 0x5589				Flagi: 0x0	Przesunięcie: 0
TTL: 128		Prot: UDP		Suma kontrolna: 0x0000	
Adres źródłowy: 192.168.102.51					
Adres docelowy: 192.168.102.1					
Opcje IP				Wypełnienie	

UDP (Warstwa transportowa)	
0-15	16-31
Port źródłowy: 56475	Port docelowy: 53
Długość datagramu: 35	Suma kontrolna: 0x4DBA

DNS (Warstwa aplikacji)							
0	1-4	5	6	7	8	9-11	12-15
ID: 0x8106							
QR: 0	OPCODE: 0	AA: 0	TC: 1	RD: 0	RA: 0	Z: 0	RCODE: 0
QDCOUNT: 1							
ANCOUNT: 0							
NSCOUNT: 0							
ARCOUNT: 0							

- Zawartość nagłówków IP, UDP, DNS dla odpowiedzi z serwera DNS

IP (Warstwa Internetowa)					
0-3	4-7	8-13	14-15	16-18	19-31
Wersja: 4	Dł.nag: 20	DSF: 0x00	ECN: 0	Dł.całkowita: 106	
Nr. Ident: 0x3A17				Flagi: 0x0	Przesunięcie: 0
TTL: 128		Prot: UDP		Suma kontrolna: 0xB2E6	
Adres źródłowy: 192.168.102.1					
Adres docelowy: 192.168.102.51					
Opcje IP				Wypełnienie	

UDP (Warstwa transportowa)	
0-15	16-31
Port źródłowy: 56475	Port docelowy: 53
Długość datagramu: 86	Suma kontrolna: 0xEA07

DNS (Warstwa aplikacji)							
0	1-4	5	6	7	8	9-11	12-15
ID: 0x8106							
QR: 1	OPCODE: 0	AA: 0	TC: 1	RD: 1	RA: 0	Z: 0	RCODE: 0
QDCOUNT: 1							
ANCOUNT: 0							
NSCOUNT: 1							
ARCOUNT: 0							

- Zawartość nagłówków IP i TCP pakietów odpowiedzialnych za nawiązanie połączenia TCP

IP (Warstwa Internetowa)					
0-3	4-7	8-13	14-15	16-18	19-31
Wersja: 4	Dł.nag: 20	DSF: 0x00	ECN: 0	Dł.całkowita: 40	
Nr. Ident: 0x5567				Flagi: 0x2	Przesunięcie: 0
TTL: 128		Prot: TCP		Suma kontrolna: 0x0000	
Adres źródłowy: 192.168.102.51					
Adres docelowy: 192.168.102.1					
Opcje IP				Wypełnienie	

TCP (Warstwa transportowa)			
0-3	4-9	10-15	16-31
Port źródłowy: 60130			Port docelowy: 445
Numer sekwencji: 645			
Numer potwierdzenia: 155			
Dł. nag: 20	Zarezerwowane: 0	Flagi: 0x10 (ACK)	Szerokość okna: 8207
Suma kontrolna: 0x4DA0			Wskaźnik priorytetu: 0
Opcje			

- Zawartość nagłówków IP, TCP i HTTP dla żądania i odpowiedzi HTTP GET

Żądanie

IP (Warstwa Internetowa)					
0-3	4-7	8-13	14-15	16-18	19-31
Wersja: 4	Dł.nag: 20	DSF: 0x00	ECN: 0	Dł.całkowita: 553	
Nr. Ident: 0x52D6				Flagi: 0x2	Przesunięcie: 0
TTL: 128		Prot: TCP		Suma kontrolna: 0x0000	
Adres źródłowy: 192.168.102.51					
Adres docelowy: 146.59.12.146					
Opcje IP				Wypełnienie	

TCP (Warstwa transportowa)			
0-3	4-9	10-15	16-31
Port źródłowy: 63657			Port docelowy: 80
Numer sekwencji: 1			
Numer potwierdzenia: 1			
Dł. nag: 20	Zarezerwowane: 0	Flagi: 0x18 (PSH, ACK)	Szerokość okna: 262656
Suma kontrolna: 0xC7C4			Wskaźnik priorytetu: 0
Opcje			

Odpowiedź

IP (Warstwa Internetowa)					
0-3	4-7	8-13	14-15	16-18	19-31
Wersja: 4	Dł.nag: 20	DSF: 0x00	ECN: 0	Dł.całkowita: 339	
Nr. Ident: 0xAFB7				Flagi: 0x2	Przesunięcie: 0
TTL: 46		Prot: TCP		Suma kontrolna: 0xD644	
Adres źródłowy: 146.59.12.146					
Adres docelowy: 192.168.102.51					
Opcje IP				Wypełnienie	

TCP (Warstwa transportowa)			
0-3	4-9	10-15	16-31
Port źródłowy: 80			Port docelowy: 63657
Numer sekwencji: 1			
Numer potwierdzenia: 514			
Dł. nag: 20	Zarezerwowane: 0	Flagi: 0x18 (PSH, ACK)	Szerokość okna: 64128
Suma kontrolna: 0xA546			Wskaźnik priorytetu: 0
Opcje			

- Zawartość nagłówków ICMP Echo Request i Echo Reply

ICMP Request (Warstwa Internetowa)			
0-7	0-15	16-23	24-31
Typ: 8	Kod: 0	Suma kontrolna: 0x4D52	
ID: 0x0001(BE) 0x0100(LE)		Numer sekwencji : 0x0009(BE) 0x0900(LE)	
Dane: 61626364656667686 9a6b6c6d6e6f707172737475767761626364656667686 9			

ICMP Reply (Warstwa Internetowa)			
0-7	0-15	16-23	24-31
Typ: 0	Kod: 0	Suma kontrolna: 0x555A	
ID: 0x0001(BE) 0x0100(LE)		Numer sekwencji : 0x0009(BE) 0x0900(LE)	
Dane: 61626364656667686 9a6b6c6d6e6f707172737475767761626364656667686 9			

3. Adresy IP odpowiadające domenom

host	192.168.102.51	(LAN)
serwer	192.168.102.1	(LAN)
agh-io.pl	149.59.12.146	(WAN)
dns.home.pl	217.160.80.244	(WAN)
ftp.agh.edu.pl	149.156.96.11	(WAN)

4. HTTP GET

Response Version: http/1.1
Status Code: 304
Response Phrase: Not Modified
X-Powered-By: Express
Access-Control-Allow-Origin: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
ETag: W/”7c1f1-183de75d1e2”
Date: Tue, 15 Nov 2022
Keep-Alive: timeout=5
[Time since request: 0.0114 sec]
[Request URI: http://agh-io.pl/img/iceland.jpg]

5. FTP nie jest bezpiecznym protokołem, gdyż nie używa żadnego szyfrowania, a przy użyciu programu Wireshark, można uzyskać podgląd do loginu oraz hasła używanych przy logowania do serwera FTP.

6. Nagłówek TCP(10B lub więcej) jest o wiele większy od nagłówka UDP(8B), przez co przekazuje o wiele więcej informacji, oraz może sprawdzać poprawne przesłanie pakietu z serwera do klienta (Three-way handshake). FTP nie jest bezpiecznym protokołem, dlatego przy poufnych danych, lepiej wykorzystywać FTPS, czyli szyfrowaną wersję FTP. Przy wykorzystaniu programu Wireshark, można uzyskać wiele informacji dotyczących ruchu sieciowego. Możliwe jest uzyskanie adresu IP domeny, bądź strony, oraz rodzaju używanego protokołu przy konkretnej operacji.