

Wireshark Task 5 - Capture & Analysis Report

This report documents the process and results of Task 5, which involves capturing network packets using Wireshark, identifying protocols, analyzing selected packets, and documenting findings. Attached are packet capture files and screenshots from the analysis.

Methodology:

- 1. Started Wireshark capture on the active network interface.
- 2. Generated network traffic by browsing websites and triggering DNS lookups.
- 3. Used display filters (http, tcp, dns) to isolate relevant packets.
- 4. Saved capture file as 'packet.pcapng'.
- 5. Collected screenshots of protocol-specific analysis.

Protocol	Description	Observed Count (approx.)
HTTP	Hypertext Transfer Protocol - application layer web traffic	Multiple GET/Partial Content requests
TCP	Transmission Control Protocol - reliable transport	Multiple PSH/ACK and reassembled s
DNS	Domain Name System - resolves domain names to IP addresses	Multiple AAAA and A record lookups/r

Packet Analysis:

- 1. HTTP Packet (#550): GET request to /edgedl/diffgen-puffin/... with HTTP/1.1 206 Partial Content response. Large reassembled TCP segment (612,687 bytes) observed.
- 2. TCP Packet (#7907): ACK packet in a TCP stream from 172.20.10.2 to 34.104.35.123, Seq=2777, Ack=4864969, Len=0.
- 3. DNS Packet (#854): Standard query response AAAA kv601.prod.do.dsp.mp.microsoft.com, resolved to multiple addresses.

Screenshots of Analysis:

```

> Frame 7913: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device\NPF_{7FE974A5-B22A-48D9-880D-475E4A303919}, id 0
> Ethernet II, Src: 7a:a7:c7:7a:86:64 (7a:a7:c7:7a:86:64), Dst: LiteonTe_7e:08:e3 (94:08:53:7e:08:e3)
> Internet Protocol Version 4, Src: 34.104.35.123, Dst: 172.20.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 56199, Seq: 4864969, Ack: 2777, Len: 1240
> [495 Reassembled TCP Segments (613346 bytes): #7266(1240), #7267(1240), #7268(1240), #7269(1240), #7271(1240), #7272(1240), #7273(1240), #7274(1240), #7275(1240), #7276(1240), #7277(1240), #7278(1240), #7279(1240), #7280(1240), #7281(1240), #7282(1240), #7283(1240), #7284(1240), #7285(1240), #7286(1240), #7287(1240), #7288(1240), #7289(1240), #7290(1240), #7291(1240), #7292(1240), #7293(1240), #7294(1240), #7295(1240), #7296(1240), #7297(1240), #7298(1240), #7299(1240), #7300(1240), #7301(1240), #7302(1240), #7303(1240), #7304(1240), #7305(1240), #7306(1240), #7307(1240), #7308(1240), #7309(1240), #7310(1240), #7311(1240), #7312(1240), #7313(1240), #7314(1240), #7315(1240), #7316(1240), #7317(1240), #7318(1240), #7319(1240), #7320(1240), #7321(1240), #7322(1240), #7323(1240), #7324(1240), #7325(1240), #7326(1240), #7327(1240), #7328(1240), #7329(1240), #7330(1240), #7331(1240), #7332(1240), #7333(1240), #7334(1240), #7335(1240), #7336(1240), #7337(1240), #7338(1240), #7339(1240), #7340(1240), #7341(1240), #7342(1240), #7343(1240), #7344(1240), #7345(1240), #7346(1240), #7347(1240), #7348(1240), #7349(1240), #7350(1240), #7351(1240), #7352(1240), #7353(1240), #7354(1240), #7355(1240), #7356(1240), #7357(1240), #7358(1240), #7359(1240), #7360(1240), #7361(1240), #7362(1240), #7363(1240), #7364(1240), #7365(1240), #7366(1240), #7367(1240), #7368(1240), #7369(1240), #7370(1240), #7371(1240), #7372(1240), #7373(1240), #7374(1240), #7375(1240), #7376(1240), #7377(1240), #7378(1240), #7379(1240), #7380(1240), #7381(1240), #7382(1240), #7383(1240), #7384(1240), #7385(1240), #7386(1240), #7387(1240), #7388(1240), #7389(1240), #7390(1240), #7391(1240), #7392(1240), #7393(1240), #7394(1240), #7395(1240), #7396(1240), #7397(1240), #7398(1240), #7399(1240), #7400(1240), #7401(1240), #7402(1240), #7403(1240), #7404(1240), #7405(1240), #7406(1240), #7407(1240), #7408(1240), #7409(1240), #7410(1240), #7411(1240), #7412(1240), #7413(1240), #7414(1240), #7415(1240), #7416(1240), #7417(1240), #7418(1240), #7419(1240), #7420(1240), #7421(1240), #7422(1240), #7423(1240), #7424(1240), #7425(1240), #7426(1240), #7427(1240), #7428(1240), #7429(1240), #7430(1240), #7431(1240), #7432(1240), #7433(1240), #7434(1240), #7435(1240), #7436(1240), #7437(1240), #7438(1240), #7439(1240), #7440(1240), #7441(1240), #7442(1240), #7443(1240), #7444(1240), #7445(1240), #7446(1240), #7447(1240), #7448(1240), #7449(1240), #7450(1240), #7451(1240), #7452(1240), #7453(1240), #7454(1240), #7455(1240), #7456(1240), #7457(1240), #7458(1240), #7459(1240), #7460(1240), #7461(1240), #7462(1240), #7463(1240), #7464(1240), #7465(1240), #7466(1240), #7467(1240), #7468(1240), #7469(1240), #7470(1240), #7471(1240), #7472(1240), #7473(1240), #7474(1240), #7475(1240), #7476(1240), #7477(1240), #7478(1240), #7479(1240), #7480(1240), #7481(1240), #7482(1240), #7483(1240), #7484(1240), #7485(1240), #7486(1240), #7487(1240), #7488(1240), #7489(1240), #7490(1240), #7491(1240), #7492(1240), #7493(1240), #7494(1240), #7495(1240), #7496(1240), #7497(1240), #7498(1240), #7499(1240), #7500(1240), #7501(1240), #7502(1240), #7503(1240), #7504(1240), #7505(1240), #7506(1240), #7507(1240), #7508(1240), #7509(1240), #7510(1240), #7511(1240), #7512(1240), #7513(1240), #7514(1240), #7515(1240), #7516(1240), #7517(1240), #7518(1240), #7519(1240), #7520(1240), #7521(1240), #7522(1240), #7523(1240), #7524(1240), #7525(1240), #7526(1240), #7527(1240), #7528(1240), #7529(1240), #7530(1240), #7531(1240), #7532(1240), #7533(1240), #7534(1240), #7535(1240), #7536(1240), #7537(1240), #7538(1240), #7539(1240), #7540(1240), #7541(1240), #7542(1240), #7543(1240), #7544(1240), #7545(1240), #7546(1240), #7547(1240), #7548(1240), #7549(1240), #7550(1240), #7551(1240), #7552(1240), #7553(1240), #7554(1240), #7555(1240), #7556(1240), #7557(1240), #7558(1240), #7559(1240), #7560(1240), #7561(1240), #7562(1240), #7563(1240), #7564(1240), #7565(1240), #7566(1240), #7567(1240), #7568(1240), #7569(1240), #7570(1240), #7571(1240), #7572(1240), #7573(1240), #7574(1240), #7575(1240), #7576(1240), #7577(1240), #7578(1240), #7579(1240), #7580(1240), #7581(1240), #7582(1240), #7583(1240), #7584(1240), #7585(1240), #7586(1240), #7587(1240), #7588(1240), #7589(1240), #7590(1240), #7591(1240), #7592(1240), #7593(1240), #7594(1240), #7595(1240), #7596(1240), #7597(1240), #7598(1240), #7599(1240), #7600(1240), #7601(1240), #7602(1240), #7603(1240), #7604(1240), #7605(1240), #7606(1240), #7607(1240), #7
```

> Frame 7907: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{7FE974A5-B22A-48D9-880D-475E4A303919}, id 0
 > Ethernet II, Src: LiteonTe_7e:08:e3 (94:08:53:7e:08:e3), Dst: 7a:a7:c7:7a:86:64 (7a:a7:c7:7a:86:64)
 > Internet Protocol Version 4, Src: 172.20.10.2, Dst: 34.104.35.123
 > Transmission Control Protocol, Src Port: 56199, Dst Port: 80, Seq: 2777, Ack: 4864969, Len: 0

0000 7a a7 c7 7a 86 64 94 08 53 7e 08 e3
 0010 00 34 ea a2 40 00 80 06 14 28 ac 14
 0020 23 7b db 87 00 50 14 df 98 de 1a 4c
 0030 04 59 dc 10 00 00 01 01 05 0a 1a 4c
 0040 55 b7

Transmission Control Protocol: Protocol

Packets: 12935 · Displayed: 12914 (99.8%) · Dropped: 0 (0.0%)

Profile: Default

dns						
No.	Time	Source	Destination	Protocol	Length	Info
301	0.769782	fe80::f870:a2d7:3a2...	fe80::78a7:c7ff:fe7...	DNS	109	Standard query 0x8357 A v10.events.data.microsoft.com
302	0.769925	fe80::f870:a2d7:3a2...	fe80::78a7:c7ff:fe7...	DNS	109	Standard query 0x90d8 AAAA v10.events.data.microsoft.com
336	0.802981	fe80::f870:a2d7:3a2...	fe80::78a7:c7ff:fe7...	DNS	115	Standard query 0x9355 A geover.prod.do.dsp.mp.microsoft.com
337	0.803616	fe80::f870:a2d7:3a2...	fe80::78a7:c7ff:fe7...	DNS	115	Standard query 0xfe1f AAAA geover.prod.do.dsp.mp.microsoft.com
363	0.833571	fe80::78a7:c7ff:fe7...	fe80::f870:a2d7:3a2...	DNS	270	Standard query response 0x90d8 AAAA v10.events.data.microsoft.com CNAME win-glob
380	0.859391	fe80::78a7:c7ff:fe7...	fe80::f870:a2d7:3a2...	DNS	226	Standard query response 0x9355 A geover.prod.do.dsp.mp.microsoft.com CNAME geover
381	0.859391	fe80::78a7:c7ff:fe7...	fe80::f870:a2d7:3a2...	DNS	238	Standard query response 0xfe1f AAAA geover.prod.do.dsp.mp.microsoft.com CNAME gec
417	0.888436	fe80::78a7:c7ff:fe7...	fe80::f870:a2d7:3a2...	DNS	258	Standard query response 0x8357 A v10.events.data.microsoft.com CNAME win-global-i
676	1.376224	fe80::f870:a2d7:3a2...	fe80::78a7:c7ff:fe7...	DNS	114	Standard query 0x0eac A kv601.prod.do.dsp.mp.microsoft.com
677	1.376363	fe80::f870:a2d7:3a2...	fe80::78a7:c7ff:fe7...	DNS	114	Standard query 0x3652 AAAA kv601.prod.do.dsp.mp.microsoft.com
807	1.445929	fe80::78a7:c7ff:fe7...	fe80::f870:a2d7:3a2...	DNS	224	Standard query response 0x0eac A kv601.prod.do.dsp.mp.microsoft.com CNAME kv601.f
854	1.471423	fe80::78a7:c7ff:fe7...	fe80::f870:a2d7:3a2...	DNS	236	Standard query response 0x3652 AAAA kv601.prod.do.dsp.mp.microsoft.com CNAME kv6

> Frame 854: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits) on interface \Device\NPF_{7FE974A5-B22A-48D9-880D-475E4A303919}, id 0
 > Ethernet II, Src: 7a:a7:c7:7a:86:64 (7a:a7:c7:7a:86:64), Dst: LiteonTe_7e:08:e3 (94:08:53:7e:08:e3)
 > Internet Protocol Version 6, Src: fe80::78a7:c7ff:fe7a:8664, Dst: fe80::f870:a2d7:3a28:f127
 > User Datagram Protocol, Src Port: 53, Dst Port: 59963
 > Domain Name System (response)

Conclusion:

The capture contained common protocols such as HTTP, TCP, and DNS. Analysis showed partial content HTTP responses, reassembled TCP segments indicating large file transfers, and DNS lookups to Microsoft-related domains. No suspicious or malicious traffic was detected in this session.