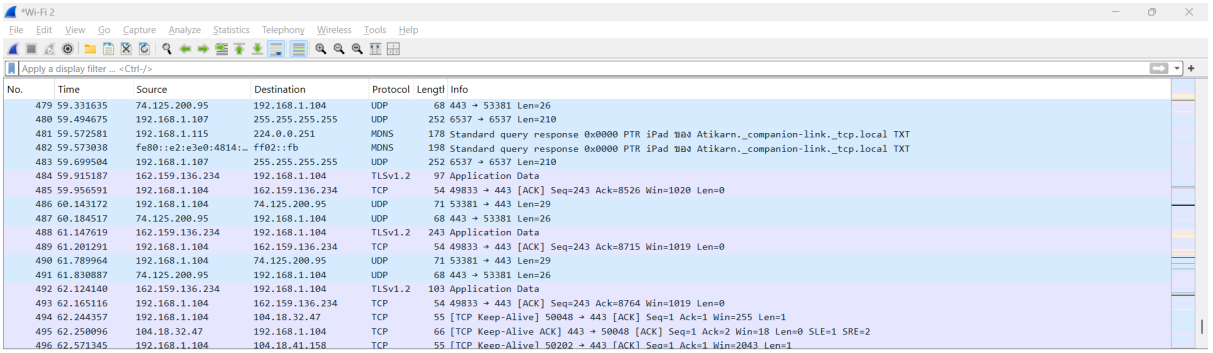
Task 1 – Capturing Traffic

Captureประมาณ 60 วินาที

Packets Total = 498 packets

Protocol = UDP,TCP,TLSv1.2,MDNs,DNS



No.	Time	Source	Destination	Protocol	Length	Info
479	59.331635	74.125.200.95	192.168.1.104	UDP	68	443 → 53381 Len=26
480	59.494675	192.168.1.107	255.255.255.255	UDP	252	6537 → 6537 Len=210
481	59.572581	192.168.1.115	224.0.0.251	MDNS	178	Standard query response 0x0000 PTR iPad ของ Atikarn._companion-link._tcp.local TXT
482	59.573038	fe80::e2:e3e0:4814:…	ff02::fb	MDNS	198	Standard query response 0x0000 PTR iPad ของ Atikarn._companion-link._tcp.local TXT
483	59.699504	192.168.1.107	255.255.255.255	UDP	252	6537 → 6537 Len=210
484	59.915187	162.159.136.234	192.168.1.104	TLSv1.2	97	Application Data
485	59.956591	192.168.1.104	162.159.136.234	TCP	54	49833 → 443 [ACK] Seq=243 Ack=8526 Win=1020 Len=0
486	60.143172	192.168.1.104	74.125.200.95	UDP	71	53381 → 443 Len=29
487	60.184517	74.125.200.95	192.168.1.104	UDP	68	443 → 53381 Len=26
488	61.147619	162.159.136.234	192.168.1.104	TLSv1.2	243	Application Data
489	61.201291	192.168.1.104	162.159.136.234	TCP	54	49833 → 443 [ACK] Seq=243 Ack=8715 Win=1019 Len=0
490	61.789964	192.168.1.104	74.125.200.95	UDP	71	53381 → 443 Len=29
491	61.830887	74.125.200.95	192.168.1.104	UDP	68	443 → 53381 Len=26
492	62.124140	162.159.136.234	192.168.1.104	TLSv1.2	103	Application Data
493	62.165116	192.168.1.104	162.159.136.234	TCP	54	49833 → 443 [ACK] Seq=243 Ack=8764 Win=1019 Len=0
494	62.244357	192.168.1.104	104.18.32.47	TCP	55	[TCP Keep-Alive] 50048 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
495	62.250096	104.18.32.47	192.168.1.104	TCP	66	[TCP Keep-Alive ACK] 443 → 50048 [ACK] Seq=1 Ack=2 Win=18 Len=0 SLE=1 SRE=2
496	62.571345	192.168.1.104	104.18.41.158	TCP	55	[TCP Keep-Alive] 50202 → 443 [ACK] Seq=1 Ack=1 Win=2043 Len=1

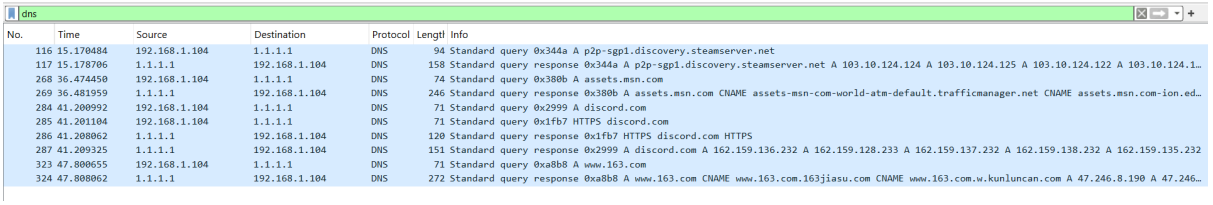
Task 2- Using Filters

using “dns”

p2p-sgp1.discovery.steamserver.net → 103.10.124.124, 103.10.124.125

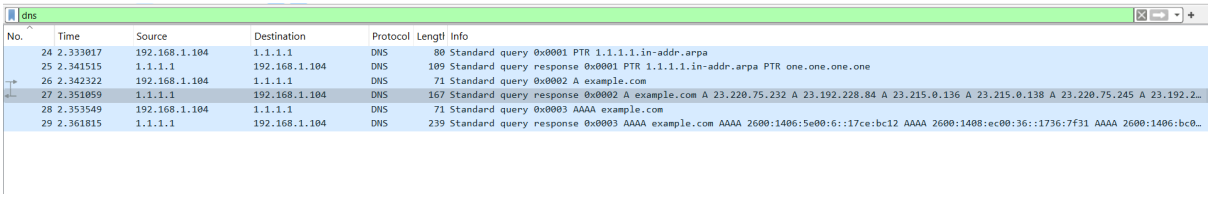
discord.com → 162.159.136.232, 162.159.128.233, 162.159.137.232, 162.159.138.232, 162.159.135.232

www.163.com → 47.246.8.190, 47.246.8.191,

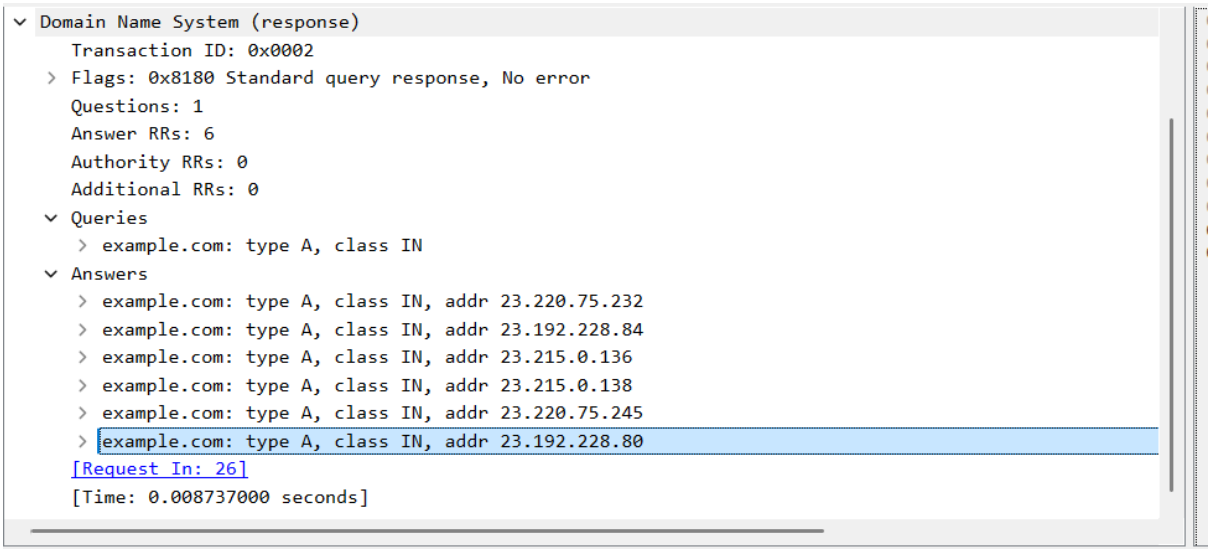


No.	Time	Source	Destination	Protocol	Length	Info
116	15.170484	192.168.1.104	1.1.1.1	DNS	94	Standard query 0x344a A p2p-sgp1.discovery.steamserver.net
117	15.178706	1.1.1.1	192.168.1.104	DNS	158	Standard query response 0x344a A p2p-sgp1.discovery.steamserver.net A 103.10.124.124 A 103.10.124.125 A 103.10.124.122 A 103.10.124.1…
268	36.474450	192.168.1.104	1.1.1.1	DNS	74	Standard query 0x380b A assets.msn.com
269	36.481959	1.1.1.1	192.168.1.104	DNS	246	Standard query response 0x380b A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net CNAME assets.msn.com-ion.ed…
284	41.200992	192.168.1.104	1.1.1.1	DNS	71	Standard query 0x2999 A discord.com
285	41.201104	192.168.1.104	1.1.1.1	DNS	71	Standard query 0x1fb7 HTTPS discord.com
286	41.208062	1.1.1.1	192.168.1.104	DNS	120	Standard query response 0x1fb7 HTTPS discord.com HTTPS
287	41.209325	1.1.1.1	192.168.1.104	DNS	151	Standard query response 0x2999 A discord.com A 162.159.136.232 A 162.159.128.233 A 162.159.137.232 A 162.159.138.232 A 162.159.135.232
323	47.800655	192.168.1.104	1.1.1.1	DNS	71	Standard query 0xa8b8 A www.163.com
324	47.808062	1.1.1.1	192.168.1.104	DNS	272	Standard query response 0xa8b8 A www.163.com CNAME www.163.com.163jiasu.com CNAME www.163.com.w.kunluncan.com A 47.246.8.190 A 47.246…

Task 3 -Analysing DNS

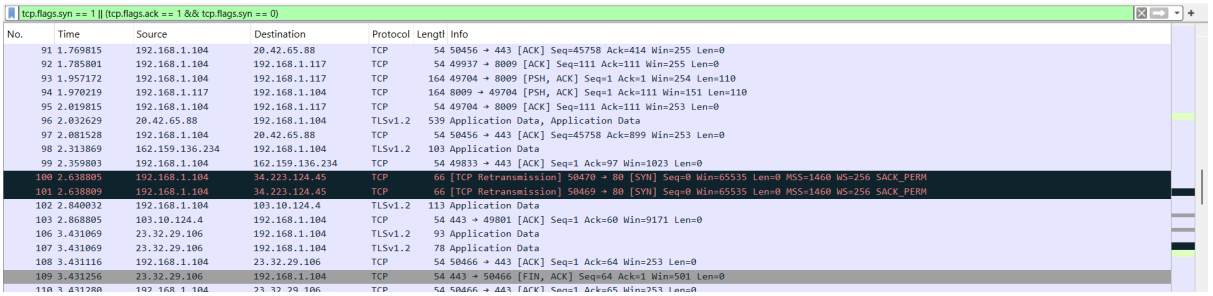


No.	Time	Source	Destination	Protocol	Length	Info
24	2.333017	192.168.1.104	1.1.1.1	DNS	80	Standard query 0x0001 PTR 1.1.1.1.in-addr.arpa
25	2.341515	1.1.1.1	192.168.1.104	DNS	109	Standard query response 0x0001 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one
26	2.342322	192.168.1.104	1.1.1.1	DNS	71	Standard query 0x0002 A example.com
27	2.351059	1.1.1.1	192.168.1.104	DNS	167	Standard query response 0x0002 A example.com A 23.220.75.232 A 23.192.228.84 A 23.215.0.136 A 23.215.0.138 A 23.220.75.245 A 23.192.2…
28	2.353549	192.168.1.104	1.1.1.1	DNS	71	Standard query 0x0003 AAAA example.com
29	2.361815	1.1.1.1	192.168.1.104	DNS	239	Standard query response 0x0003 AAAA example.com AAAA 2600:1406:5e00:6::17ce:bc12 AAAA 2600:1408:ec00:36::1736:7f31 AAAA 2600:1406:bc0…



```
Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > example.com: type A, class IN
  v Answers
    > example.com: type A, class IN, addr 23.220.75.232
    > example.com: type A, class IN, addr 23.192.228.84
    > example.com: type A, class IN, addr 23.215.0.136
    > example.com: type A, class IN, addr 23.215.0.138
    > example.com: type A, class IN, addr 23.220.75.245
    > example.com: type A, class IN, addr 23.192.228.80
    [Request In: 26]
    [Time: 0.008737000 seconds]
```

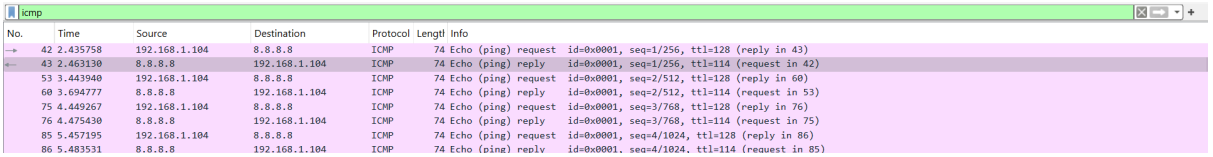
Task 4 – Analysing TCP Handshake



tcp.flags.syn == 1 || (tcp.flags.ack == 1 && tcp.flags.syn == 0)

No.	Time	Source	Destination	Protocol	Length	Info
91	1.769815	192.168.1.104	20.42.65.88	TCP	54	50456 → 443 [ACK] Seq=45758 Ack=414 Win=255 Len=0
92	1.785801	192.168.1.104	192.168.1.117	TCP	54	49937 → 8009 [ACK] Seq=111 Ack=111 Win=255 Len=0
93	1.957172	192.168.1.104	192.168.1.117	TCP	164	49704 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=110
94	1.970219	192.168.1.117	192.168.1.104	TCP	164	8009 → 49704 [PSH, ACK] Seq=1 Ack=111 Win=151 Len=110
95	2.019815	192.168.1.104	192.168.1.117	TCP	54	49704 → 8009 [ACK] Seq=111 Ack=111 Win=253 Len=0
96	2.032629	20.42.65.88	192.168.1.104	TLSv1.2	539	Application Data, Application Data
97	2.081528	192.168.1.104	20.42.65.88	TCP	54	50456 → 443 [ACK] Seq=45758 Ack=899 Win=253 Len=0
98	2.313869	162.159.136.234	192.168.1.104	TLSv1.2	103	Application Data
99	2.359803	192.168.1.104	162.159.136.234	TCP	54	49833 → 443 [ACK] Seq=1 Ack=97 Win=1023 Len=0
100	2.638805	192.168.1.104	34.223.124.45	TCP	66	[TCP Retransmission] 50470 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
101	2.638809	192.168.1.104	34.223.124.45	TCP	66	[TCP Retransmission] 50469 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
102	2.840032	192.168.1.104	103.10.124.4	TLSv1.2	113	Application Data
103	2.868805	103.10.124.4	192.168.1.104	TCP	54	443 → 49801 [ACK] Seq=1 Ack=60 Win=9171 Len=0
106	3.431069	23.32.29.106	192.168.1.104	TLSv1.2	93	Application Data
107	3.431069	23.32.29.106	192.168.1.104	TLSv1.2	78	Application Data
108	3.431116	192.168.1.104	23.32.29.106	TCP	54	50466 → 443 [ACK] Seq=1 Ack=64 Win=253 Len=0
109	3.431256	23.32.29.106	192.168.1.104	TCP	54	443 → 50466 [FIN, ACK] Seq=64 Ack=1 Win=501 Len=0
110	3.431280	192.168.1.104	23.32.29.106	TCP	54	50466 → 443 [ACK] Seq=1 Ack=65 Win=253 Len=0

Task 5 – ICMP (Ping Test)

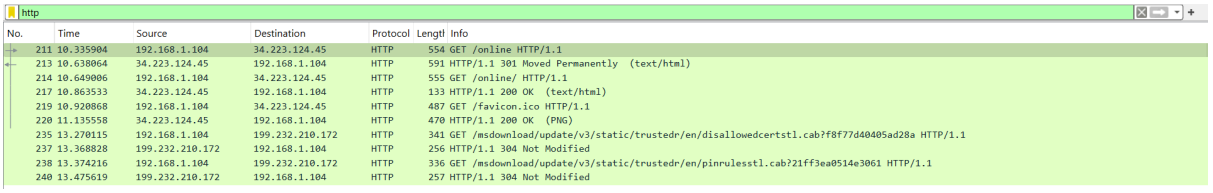


icmp

No.	Time	Source	Destination	Protocol	Length	Info
42	2.435758	192.168.1.104	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 43)
43	2.463130	8.8.8.8	192.168.1.104	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=114 (request in 42)
53	3.443940	192.168.1.104	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 60)
60	3.694777	8.8.8.8	192.168.1.104	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=114 (request in 53)
75	4.449267	192.168.1.104	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 76)
76	4.475430	8.8.8.8	192.168.1.104	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=114 (request in 75)
85	5.457195	192.168.1.104	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 86)
86	5.483531	8.8.8.8	192.168.1.104	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=114 (request in 85)

RTT = Time(Echo Reply) - Time(Echo Request)
RTT = 2.463130 - 2.435758
RTT = 0.027372 s ≈ 27.37 ms
TTL =114

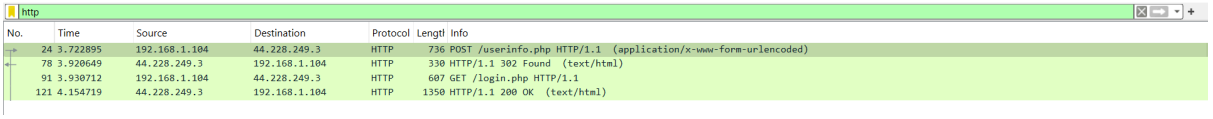
Task 6 – Application Layer Protocol Analysis



http

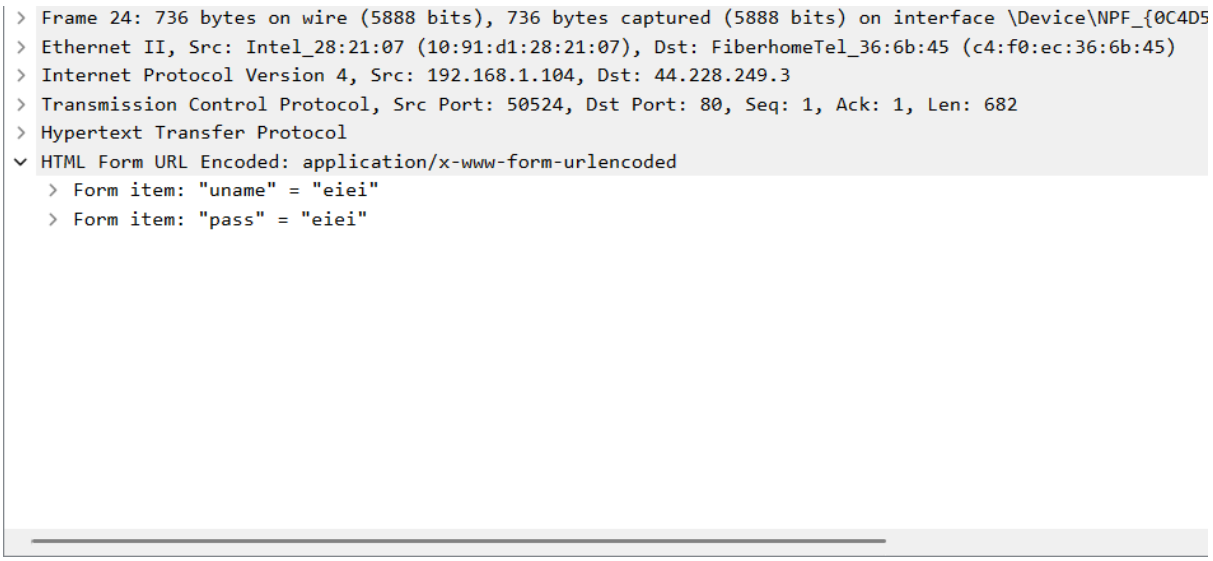
No.	Time	Source	Destination	Protocol	Length	Info
211	10.335904	192.168.1.104	34.223.124.45	HTTP	554	GET /online HTTP/1.1
213	10.638064	34.223.124.45	192.168.1.104	HTTP	591	HTTP/1.1 301 Moved Permanently (text/html)
214	10.649006	192.168.1.104	34.223.124.45	HTTP	555	GET /online/ HTTP/1.1
217	10.863533	34.223.124.45	192.168.1.104	HTTP	133	HTTP/1.1 200 OK (text/html)
219	10.920868	192.168.1.104	34.223.124.45	HTTP	487	GET /favicon.ico HTTP/1.1
220	11.135558	34.223.124.45	192.168.1.104	HTTP	470	HTTP/1.1 200 OK (PNG)
235	13.270115	192.168.1.104	199.232.210.172	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f8f77d40405ad28a HTTP/1.1
237	13.368828	199.232.210.172	192.168.1.104	HTTP	256	HTTP/1.1 304 Not Modified
238	13.374216	192.168.1.104	199.232.210.172	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?21ff3ea0514e3061 HTTP/1.1
240	13.475619	199.232.210.172	192.168.1.104	HTTP	257	HTTP/1.1 304 Not Modified

Task 7 – Security-Oriented Analysis



http

No.	Time	Source	Destination	Protocol	Length	Info
24	3.722895	192.168.1.104	44.228.249.3	HTTP	736	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
78	3.920649	44.228.249.3	192.168.1.104	HTTP	330	HTTP/1.1 302 Found (text/html)
91	3.930712	192.168.1.104	44.228.249.3	HTTP	607	GET /login.php HTTP/1.1
121	4.154719	44.228.249.3	192.168.1.104	HTTP	1350	HTTP/1.1 200 OK (text/html)



```
> Frame 24: 736 bytes on wire (5888 bits), 736 bytes captured (5888 bits) on interface \Device\NPF_{0C4D5
> Ethernet II, Src: Intel_28:21:07 (10:91:d1:28:21:07), Dst: FiberhomeTel_36:6b:45 (c4:f0:ec:36:6b:45)
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 50524, Dst Port: 80, Seq: 1, Ack: 1, Len: 682
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "eiei"
  > Form item: "pass" = "eiei"
```

1. What is the difference between a capture filter and a display filter?

Capture filter: choose which packets to capture before starting.

Display filter: choose which packets to show after capturing.

2. How does Wireshark help detect network intrusions or malware activity?

It shows all packets so you can see unusual traffic.

Helps find attacks like port scans or malware sending data.

3. What security risks arise from using unsecured (HTTP) connections?

Information like usernames and passwords can be seen by attackers.

Data can be changed or stolen because it is not encrypted.

4. How can Wireshark be applied in digital forensics investigations?

It can check network traffic after a security incident.

Helps find attackers, malware, or stolen data.

Can be used as digital evidence.

5. Compare ICMP packet analysis with TCP packet analysis—what key differences exist?

ICMP: used to check if a host is reachable and measure response time.

TCP: used to make a reliable connection and send data.

ICMP is simple; TCP is more complex and tracks connections.