Wireshark Analysis Instructions

1. **Opening the Capture File:**

- Launch Wireshark and open the provided .pcap file.
- Familiarize yourself with the Wireshark interface: the filter toolbar at the top, the packet list pane below the filter toolbar, the details pane in the middle, and the packet bytes pane at the bottom.

0 0	🔺 🔳 🙇	B 🗎 X 2	9, 🗢 🗢 🐴 🚽		
Filter: Expression Clear Apply Save					
No.	Time	Source	Destination	Protocol	Info
1827	8.598721	192.168.1.101	74.125.200.94	TCP	49246.443 [ACK] Seq=3161453776 Ack=3708602291 Win=4150 Len=0 TSval=595569656 TSecr=3513932058
1828	8.599091	192.168.1.101	74.125.200.94	TLSv1.2	Application Data
1829	8.631177	216.58.220.46	192.168.1.101	TCP	44349251 [ACK] Seq=1298278402 Ack=1710850208 Win=371 Len=0 TSval=1704563776 TSecr=595569582
1830	8.644211	74.125.200.94	192.168.1.101	TCP	443_49246 [ACK] Seq=3708602291 Ack=3161453776 Win=547 Len=0 TSval=3513932109 TSecr=595569629
1831	8.658656	216.58.196.132	192.168.1.101	TCP	443-49249 [ACK] Seq=2905517011 Ack=521756204 Win=366 Len=0 TSval=1415568817 TSecr=595569630
1832	8.696484	74.125.200.94	192.168.1.101	TCP	443_49246 [ACK] Seq=3708602291 Ack=3161453845 Win=547 Len=0 T5val=3513932161 T5ecr=595569656
1833	8.697547	216.58.220.46	192.168.1.101	TCP	443-49251 [ACK] Seg=1298278402 Ack=1710850277 Win=371 Len=0 T5val=1704563842 T5ecr=595569642
1834	9.846595	192.168.1.101	216.239.98.121	2 Packet	Pint Pint Ack Seq 1030802300 Ack=360272818 Win=4096 Len=0 Tsval=595570899 Tsecr=3031662643
1835	10.201531	216.239.98.121	192.168.1.101	Z. Fachel	LISU/F dirC 1=3002/2818 ACK=1030802301 Win=1/3 Len=0 15va(=303106/5/8 15ecr=5955/0899
1836	11.798841	192.168.1.101	111.221.29.129	SSL	AND CREATE CARRY COMPARING AND INCOMPANY AND
1837	12.045007	102 168 1 101	192.108.1.101	ICP EEL	442-02142 Terrel Data Continuation Data
1030	12.045004	192.100.1.101	102 169 1 101	35L	Conclusation Data
1859	12.125740	102 369 1 303	192.108.1.101	16591.2	Application Data 6534 443 [AVI] Con-1140733330 Ack-41377616 Min-4001 [an-0 TC+3]=665573171 TC+42-313041103
1040	13 033007	192.100.1.101	17 253 26 253	NTD	0393-493 [ACK] SEGTIM972220 ACK=4127/010 WIN=4091 LEN=0 13V4(-393373171 15ECT=212941102
1041	14 207002	17 253 26 253	102 160 1 101	N TP	NTP Version 4, collect
1042	16 343592	foR0::1	192.100.1.101 ff021	TCMPu6	nir version 4, server
b Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) b Ethernet II, Src: 28:cf:e9:1e:df:a9 (28:cf:e9:1e:df:a9), Dst: 94:fb:b2:b8:df:d8 (94:fb:b2:b8:df:d8) b Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 192.168.1 1 b User Datagram Protocol, Src Port: 49940 (49940), Dst Port: 53 (53) b Domain Name System (query)					
0000 94 f 0010 00 4 0020 01 0 0030 00 0 0040 6f 6 0050 03 6	b b2 b8 df d8 28 b db ee 00 00 ff 1 c3 14 00 35 00 0 00 00 00 00 07 if 67 6c 65 73 79 3 6f 6d 00 00 01	cf e9 le df a9 08 00 4 11 5b fc c0 a8 01 65 0 37 95 bc 07 bf 01 00 0 70 61 67 65 61 64 32 1 6e 64 69 63 61 74 69 6 00 01	5 00E. 0 a8 .KE. 0 01	4. Packet	Byte Pane

2. Applying Display Filters:

- Use display filters to narrow down the traffic. For example, if you know the communication involves a specific IP address or port, enter a filter like:
 - ip.addr == x.x.x.x (replace x.x.x.x with an IP address of interest)
 - tcp.port == 5000 or udp.port == 5000
- Or you can use TCP to display packets only for the TCP protocol when you have different protocols in the traffic.

3. Following Streams:

- Right-click on a packet that appears to contain relevant data and select "Follow TCP Stream" (or UDP Stream if applicable). This feature allows you to see the entire conversation in one window.
- Analyze the stream to observe if and when the data changes or if there is any evidence of interference.

5. **Comparing Packets:**

- Identify and compare packets that are supposed to be similar. Look for any discrepancies in the payloads, such as differences in coordinate values.
- Note the timestamps and sequence numbers to understand the order of packets and pinpoint when changes occur.
- 6. Noting Anomalies:

- Document any anomalies you find. For instance, if the same communication shows different coordinate values in different packets, this might indicate data manipulation.
- Pay attention to the source IP addresses—if you see unexpected or repeated IPs, that could be a sign of an attacker's involvement.

7. Utilizing Wireshark Tools:

- **Statistics:** Use Wireshark's statistics features (e.g., "Protocol Hierarchy" or "Endpoints") to get an overview of the traffic and identify unusual patterns.
- **Exporting Data:** If needed, export specific packets or streams to review in more detail or to include as part of your report.

8. General Approach:

- Start by getting an overview of the traffic.
- Narrow down to the segments relevant to GPS data.
- Compare "before" and "after" states of the data.
- Focus on identifying the attacker's IP and any manipulation in the payload.