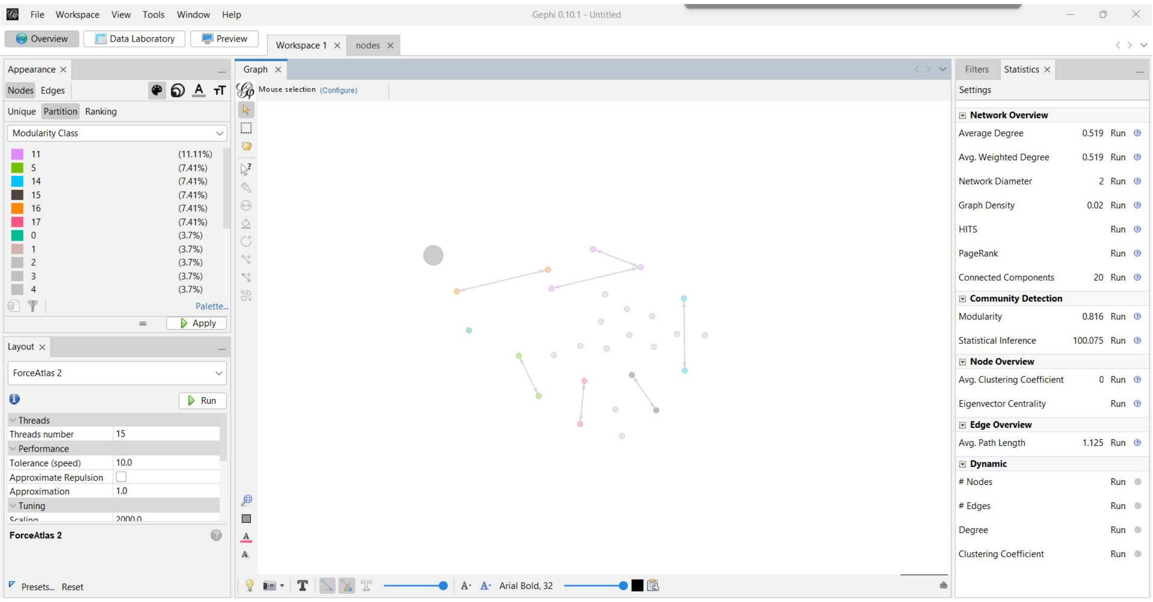
Comparative Social Network Analysis Report
Sample 27: 5G Conspiracy vs Non- Conspiracy
Ziad Mahmoud Ahmed Abdelgwad

2205021

Results Overview

Sample 27 — 5G Conspiracy Graph:



Modularity Class

🟪	11	(11.11%)
🟩	5	(7.41%)
🟦	14	(7.41%)
⬛	15	(7.41%)
🟧	16	(7.41%)
🟥	17	(7.41%)
🟩	0	(3.7%)
▨	1	(3.7%)
▨	2	(3.7%)
▨	3	(3.7%)
▨	4	(3.7%)

ForceAtlas 2

Threads	
Threads number	15
Performance	
Tolerance (speed)	10.0
Approximate Repulsion	□
Approximation	1.0
Tuning	
Scaling	2000.0

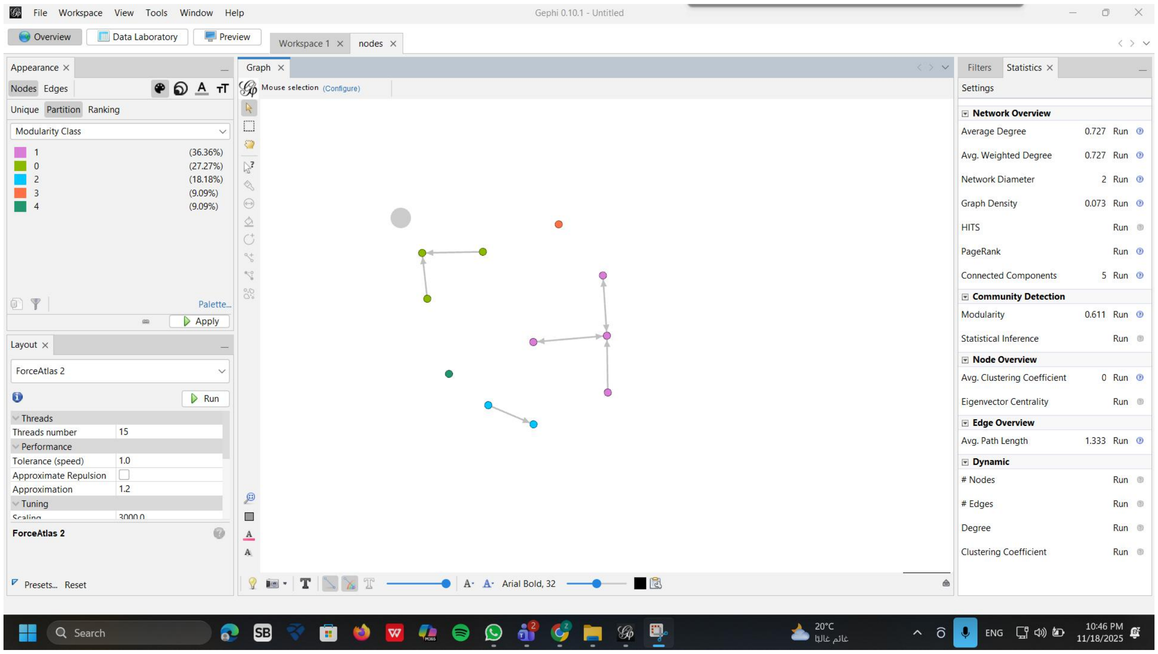
ForceAtlas 2

Network Overview		
Average Degree	0.519	Run
Avg. Weighted Degree	0.519	Run
Network Diameter	2	Run
Graph Density	0.02	Run
HITS		Run
PageRank		Run
Connected Components	20	Run
Community Detection		
Modularity	0.816	Run
Statistical Inference	100.075	Run
Node Overview		
Avg. Clustering Coefficient	0	Run
Eigenvector Centrality		Run
Edge Overview		
Avg. Path Length	1.125	Run
Dynamic		
# Nodes		Run
# Edges		Run
Degree		Run
Clustering Coefficient		Run

- Nodes: 27
- Edges: 14
- Average degree: ~1.04
- Density: 0.0199
- Average clustering coefficient: 0.0
- Modularity (Q): 0.8163
- Number of communities: 20
- Betweenness centrality: extremely low (max ~0.00308)
- Closeness centrality: very low (max ~0.0769)
- Connected components: 20

Interpretation:
The network is extremely fragmented with low interaction levels and minimal cohesion, indicating possible artificial or automated behavior typical of misinformation clusters.

Sample 27 — Non- Conspiracy Graph



Modularity Class

🟪	1	(36.36%)
🟩	0	(27.27%)
🟦	2	(18.18%)
🟧	3	(9.09%)
🟩	4	(9.09%)

ForceAtlas 2

Threads	
Threads number	15
Performance	
Tolerance (speed)	1.0
Approximate Repulsion	□
Approximation	1.2
Tuning	
Scaling	3000.0

ForceAtlas 2

Network Overview		
Average Degree	0.727	Run
Avg. Weighted Degree	0.727	Run
Network Diameter	2	Run
Graph Density	0.073	Run
HITS		Run
PageRank		Run
Connected Components	5	Run
Community Detection		
Modularity	0.611	Run
Statistical Inference		Run
Node Overview		
Avg. Clustering Coefficient	0	Run
Eigenvector Centrality		Run
Edge Overview		
Avg. Path Length	1.333	Run
Dynamic		
# Nodes		Run
# Edges		Run
Degree		Run
Clustering Coefficient		Run

- Nodes: 11
- Edges: 8
- Average degree: ~1.45
- Density: 0.0727
- Average clustering coefficient: 0.0
- Modularity (Q): 0.6111
- Number of communities: 5
- Betweenness centrality: higher and meaningful (max ~0.04444)
- Closeness centrality: stronger (max 0.3)
- Connected components: 5

Interpretation:
This graph exhibits healthier connectivity and more natural grouping, consistent with organic, human-driven social interactions.

Comparative Analysis

The comparison between both networks reveals several key differences:

- The conspiracy graph is sparse and fragmented with weak connections, indicating a lack of genuine interaction between accounts.

- The non-conspiracy graph forms clearer communities and demonstrates stronger internal cohesion.

- The high modularity and large number of components in the conspiracy graph suggest artificially segmented or disposable accounts often used in misinformation campaigns.

- Natural social behaviors—such as strong hubs, higher centrality values, and organic clustering—appear only in the non-conspiracy network.

Table 1: Comparative Analysis

Criteria	Conspiracy Graph (5G Sample 27)	Non-Conspiracy Graph (Sample 27)
Network Shape	Very sparse and highly fragmented	More connected and coherent
Internal Interaction Strength	Very weak – interactions appear unnatural	Stronger, natural internal interaction
Community Structure	20 weak, poorly connected communities	5 clear, cohesive communities
Modularity (Q)	Very high → unnatural segmentation	Moderate → organic segmentation
Connected Components	20 components out of 27 nodes	5 components
Clustering Coefficient	0.0 → no natural clustering	0.0 but clearer structure
Centrality Values	Extremely low, no influential nodes	Higher values, natural hubs exist
Behavior Pattern	Artificial/automated behavior	Genuine human interaction
Overall Interpretation	Engineered misinformation network	Normal, natural social network

Security Interpretation

From a cybersecurity perspective, the conspiracy graph displays multiple red flags associated with coordinated inauthentic activity:

- Extremely high fragmentation (20 components for 27 nodes)
- Lack of clustering or natural group formation
- Weak centrality values suggesting minimal real interaction
- High modularity, indicating unnatural segmentation

These characteristics are commonly observed in:

- Bot networks
- Sockpuppet accounts
- Coordinated amplification groups
- Astroturfing campaigns

Meanwhile, the non-conspiracy graph behaves like a normal human interaction network.

Table 2: Security Interpretation

Security Indicator	Conspiracy Graph	Security Interpretation
Fragmentation	Extremely high (20/27)	Indicates artificial or disposable accounts
Clustering	Almost none	Suspicious lack of natural grouping
Centrality	Very low	Accounts do not bridge or connect groups
Modularity	Very high	Unnatural segmentation typical in coordinated activity
Interaction Level	Very low	Accounts amplify content rather than interact
Threat Indicators	Botnets, sockpuppets, amplification patterns	Matches misinformation operation profiles

Conclusion

The structural differences between the conspiracy and non-conspiracy graphs are clear and consistent with known patterns of misinformation communities. The conspiracy graph shows structural signs of artificial amplification, while the non-conspiracy graph exhibits natural social behavior. This demonstrates the value of social network analysis as a tool for detecting misinformation networks on online platforms.

Table 3: Final Conclusion

Aspect	Conspiracy Network	Non-Conspiracy Network
Overall Behavior	Artificial, manipulated network	Natural social behavior
User Interaction	Weak, non-human-like	Normal human interaction
Network Purpose	Spreading/amplifying misinformation	Regular conversation
Security Assessment	Matches malicious misinformation patterns	No malicious indicators
Final Verdict	Synthetic misinformation-driven network	Healthy, legitimate network