

Cyber Threat Intelligence

👤 From Domain to Phone Numbers and Much More

How Maltego Unveils Hidden Intelligence!

Maltego:

- Maltego is a powerful OSINT (Open-Source Intelligence) tool designed for data mining, visualization, and cyber investigations.
- It helps security professionals uncover hidden relationships between *domains*, *emails*, *social media accounts*, *IP addresses*, and even *employee contact* details.

Why is Maltego Important?

- Maltego is widely used in *cyber threat intelligence*, *OSINT investigations*, *digital forensics*, and *penetration testing*.
- It allows real-time data correlation from various sources like DNS records, social media, breached databases, and more.
- Security professionals, ethical hackers, and law enforcement agencies use it to *trace cybercriminals*, *detect phishing campaigns*, and *analyze digital footprints*.

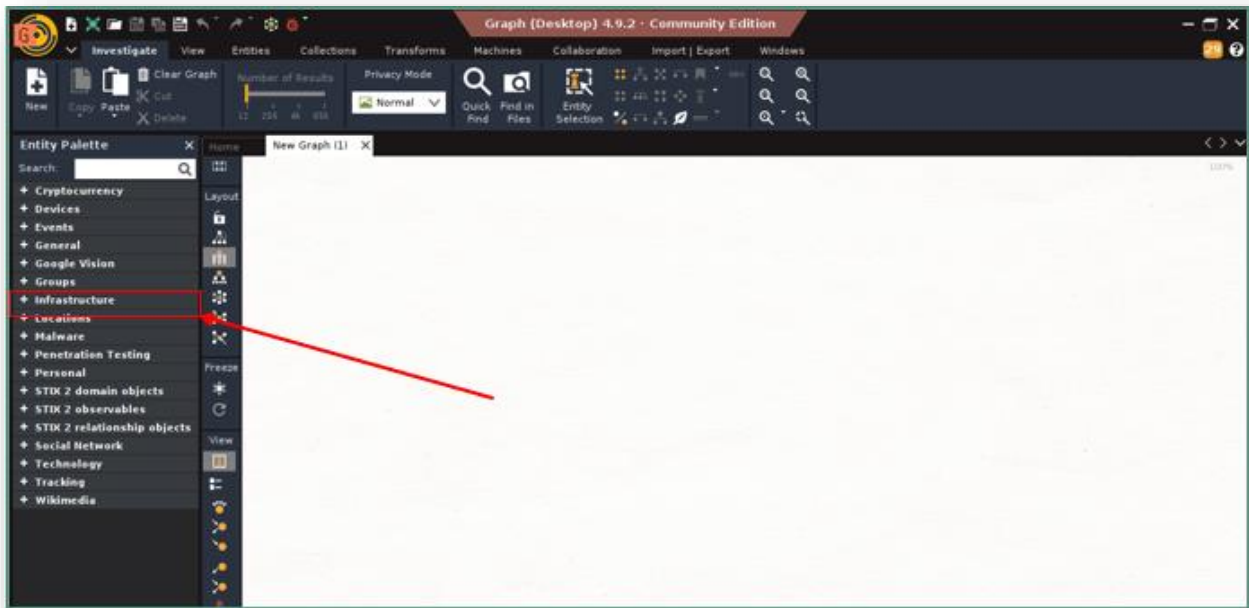
Who Uses Maltego?

- **Cyber Threat Intelligence Analysts:** For tracking cyber threats and adversaries.
- **Law Enforcement Agencies:** To investigate criminal networks.
- **Ethical Hackers & Red Teamers:** For reconnaissance and attack surface mapping.
- **Fraud Detection Teams:** To identify financial fraud and insider threats.

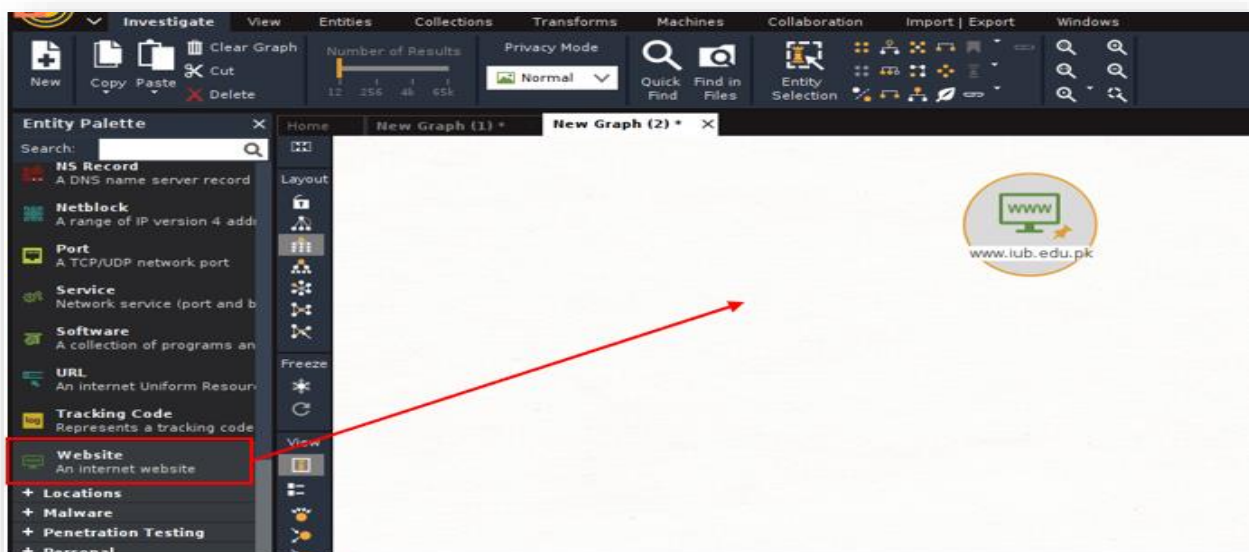
Maltego in Action – Extracting Hidden Intelligence!

Step by Step Guidance:

1- Main Interface of Maltego:

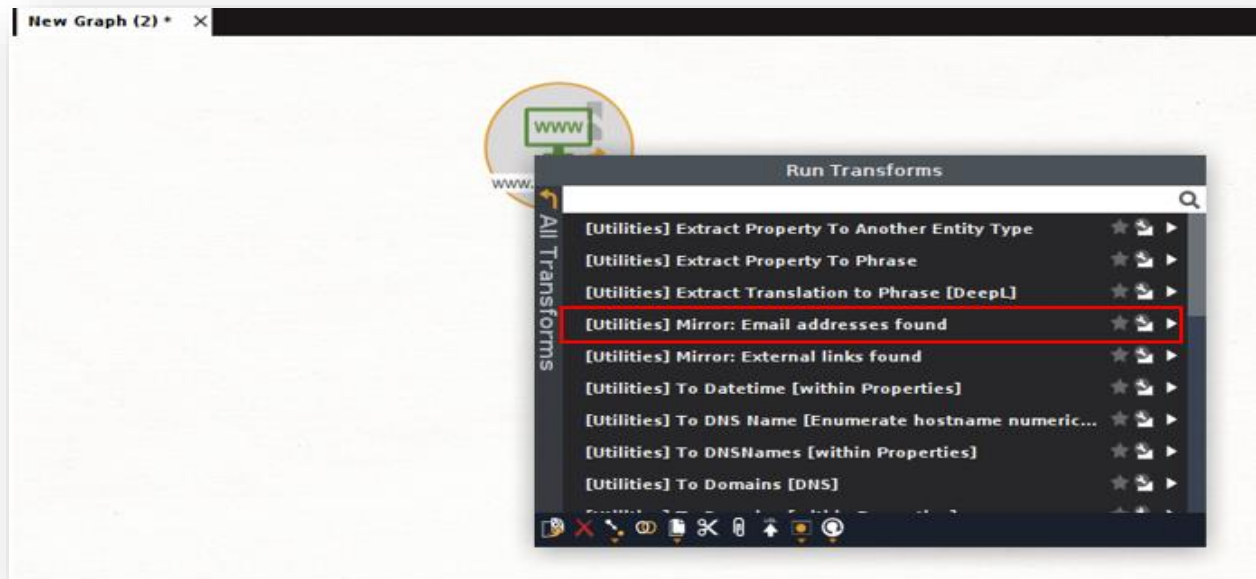


2- Uncovering Infrastructure:



- ✚ Uncover **Infrastructure**, go to **Website** entity, drag & drop it into graph section, rename it with target domain.

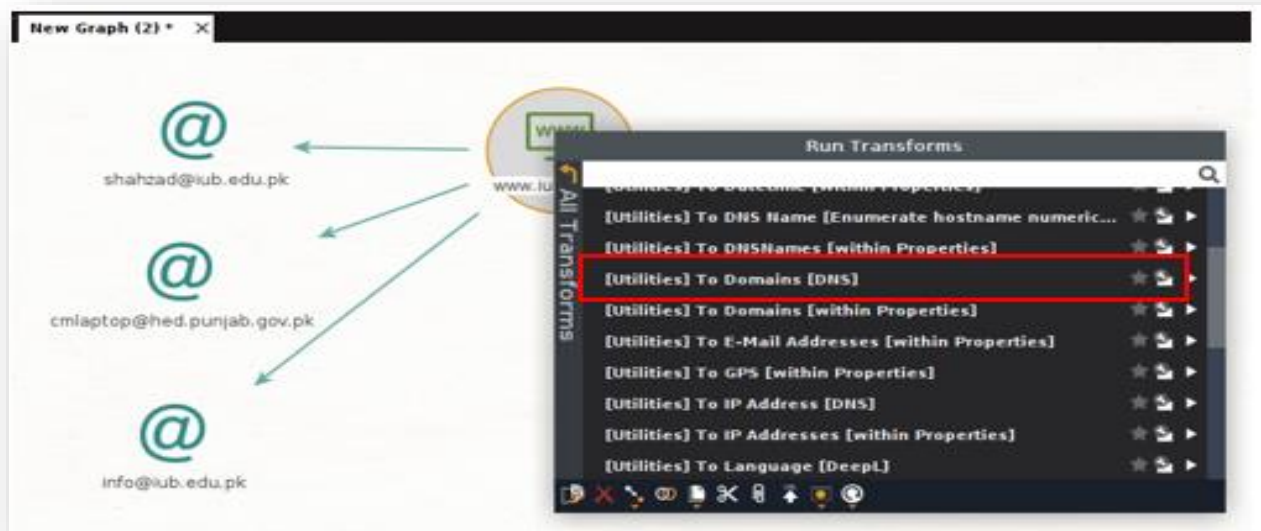
3- Finding Emails Associate with Domain:



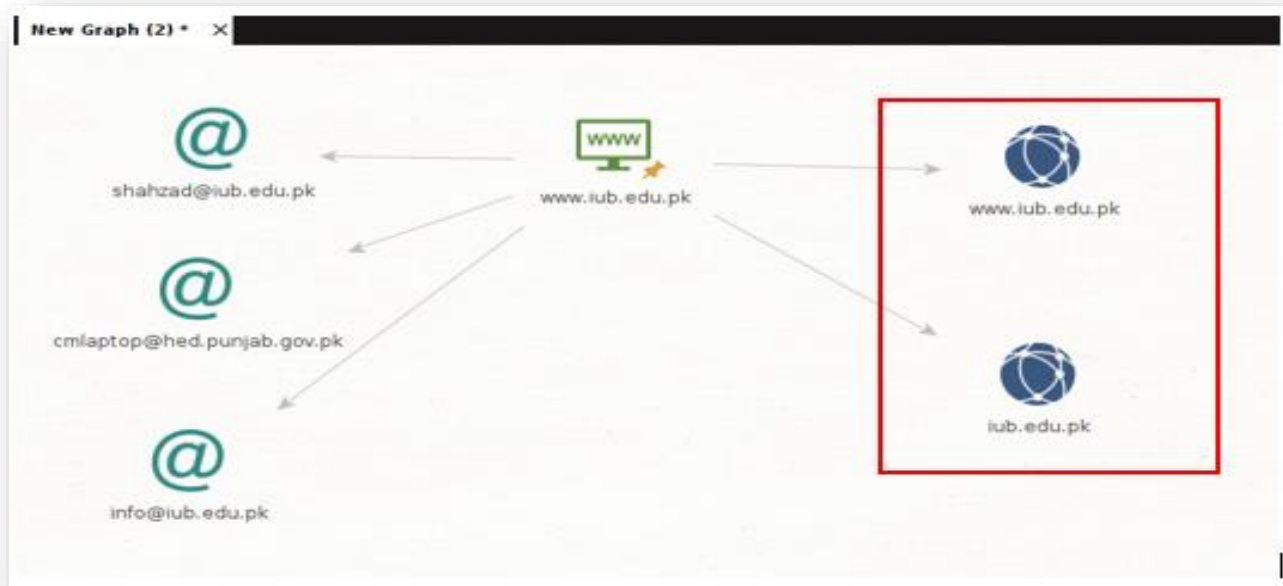
- ✚ Right click on domain and run above transform.
- ✚ It will provide the publicly available **Email addresses** associated to that domain.



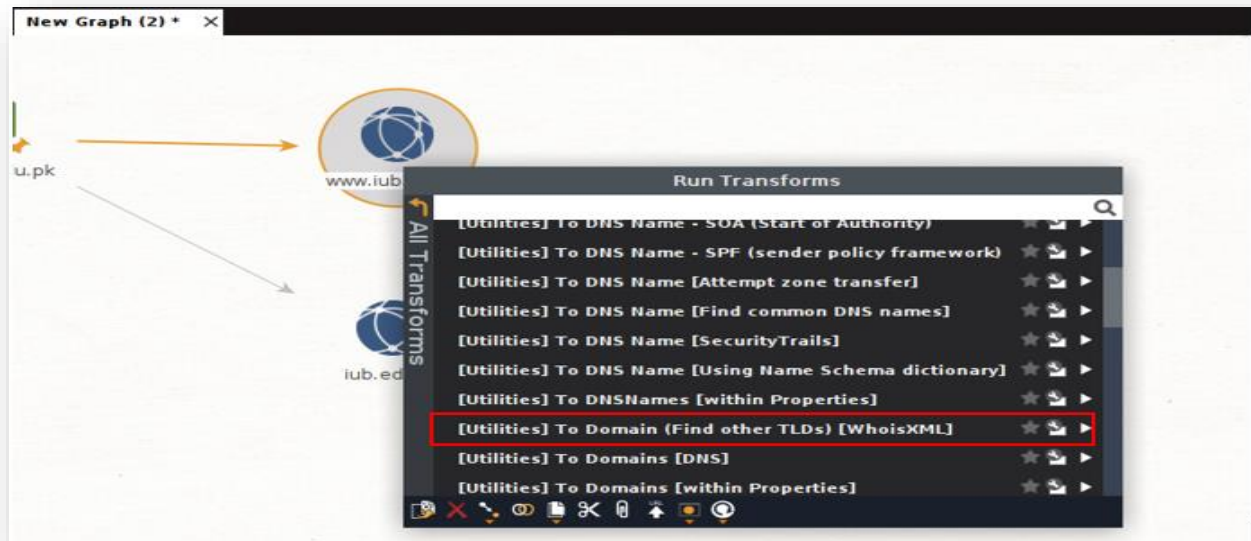
4- Finding Registered Domains of Target Domain:



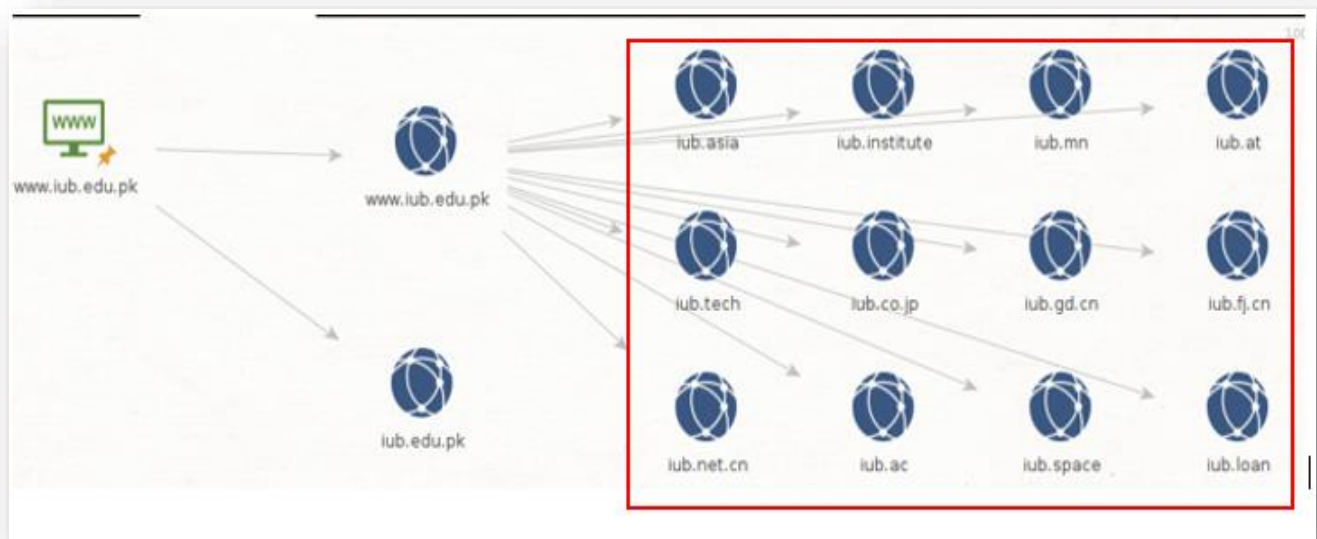
- ✚ Right click on Website entity and run above transform.
- ✚ It will extract the actual registered domains.
- ✚ It provides information that www.iub.edu.pk is the **subdomain of root domain (iub.edu.pk)**.
- ✚ It helps in identifying potential entry points for further intelligence gathering.



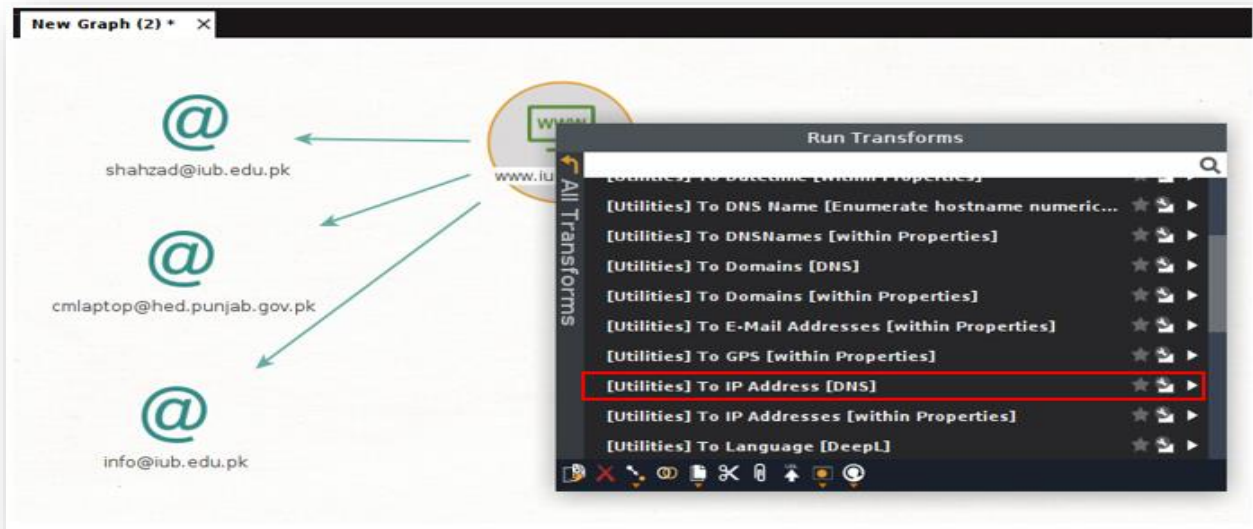
5- Finding Top Level Domains of Target Domain:



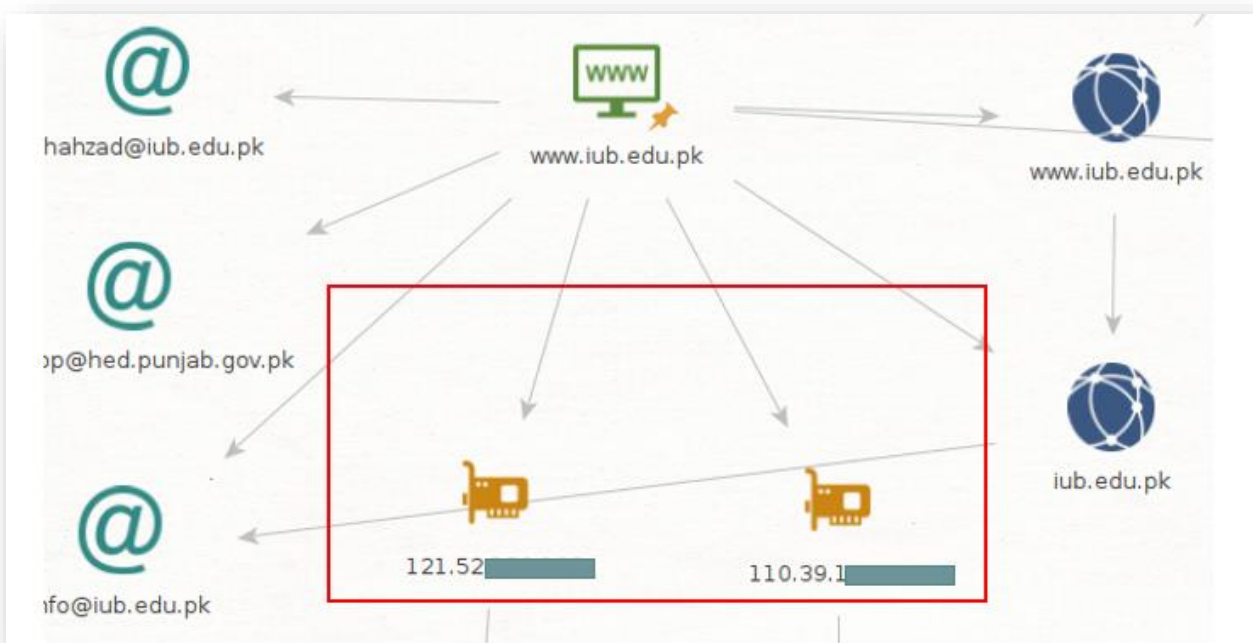
- Maltego identified several TLDs linked to the primary domain, including iub.asia, iub.institute, iub.net.cn and many more.
- These variations could be **officially registered by the organization** or might be potential typosquatting or **phishing domains created by malicious actors**.
- Such domains are also **used in brand impersonation, fraud, and cyber-espionage campaigns**.



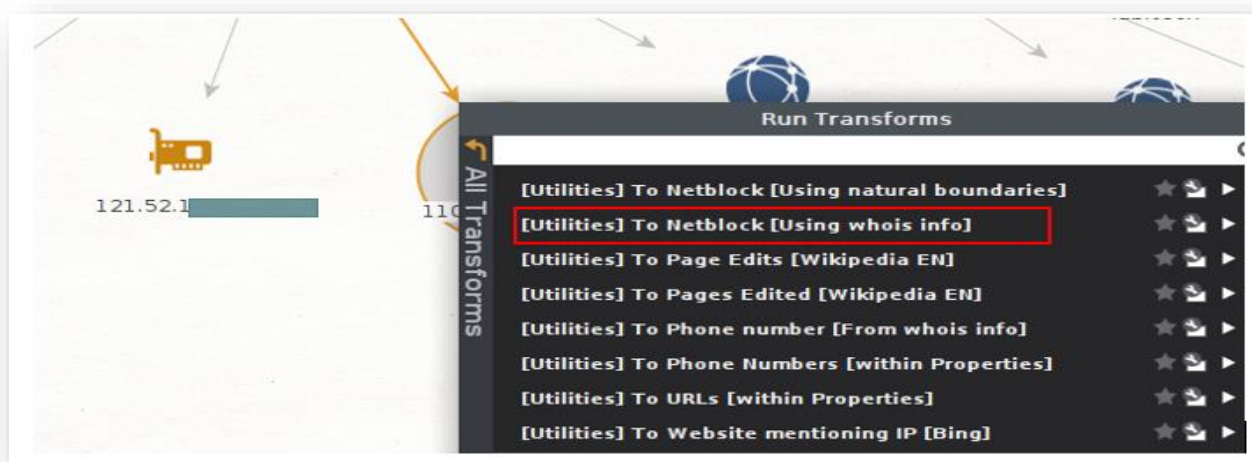
6- Finding IP Addresses of Target Domain:



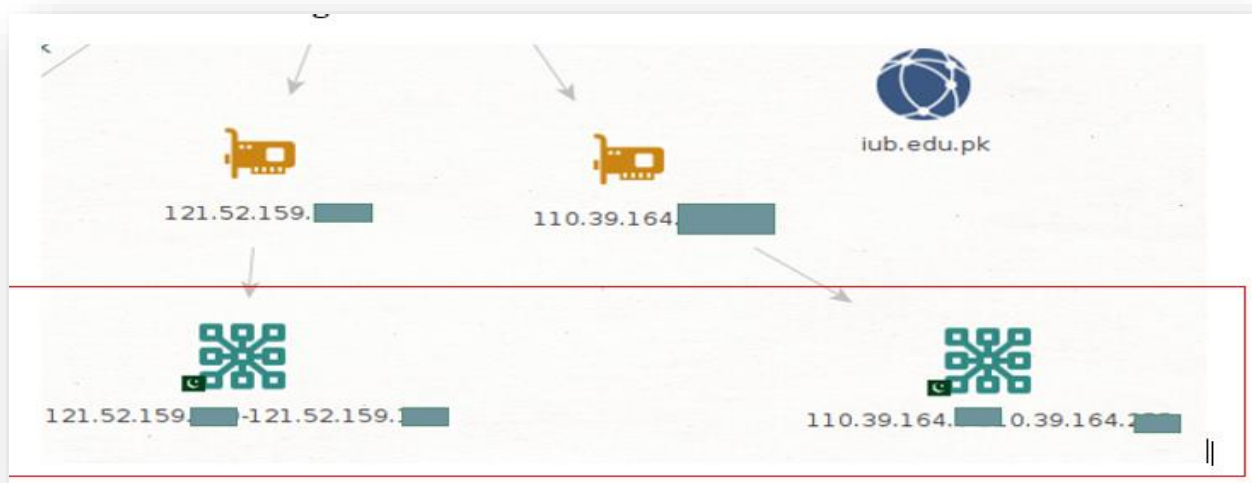
- ✚ It will extract the **IP addresses** of both root domain (iub.edu.pk) & sub domain (www.iub.edu.pk).



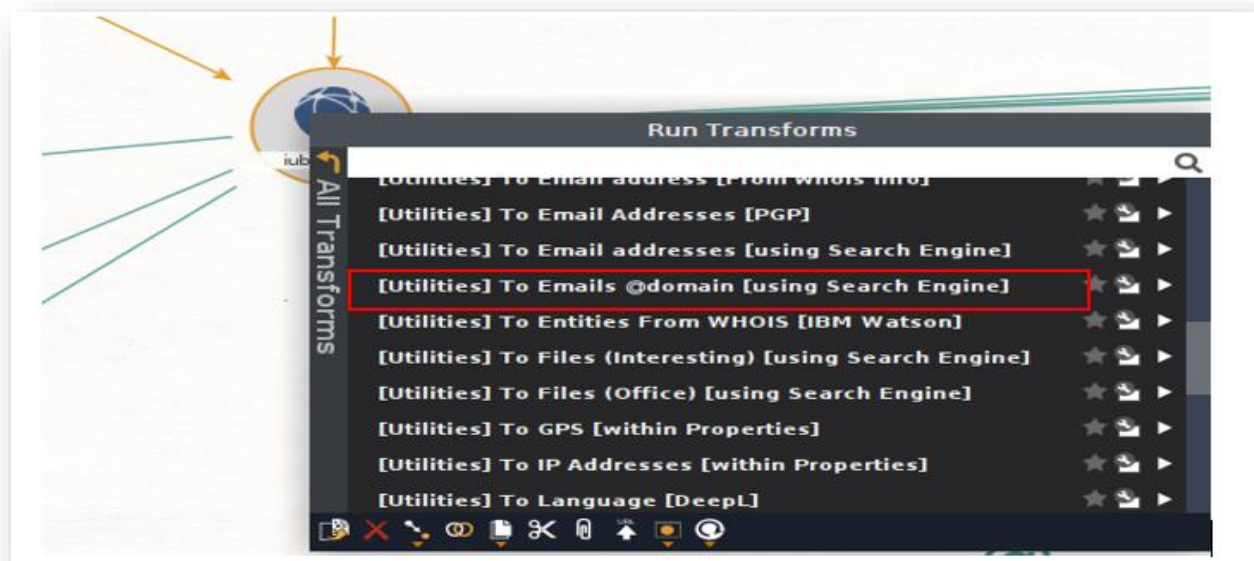
7- Finding IP Blocks used by Target Domain:



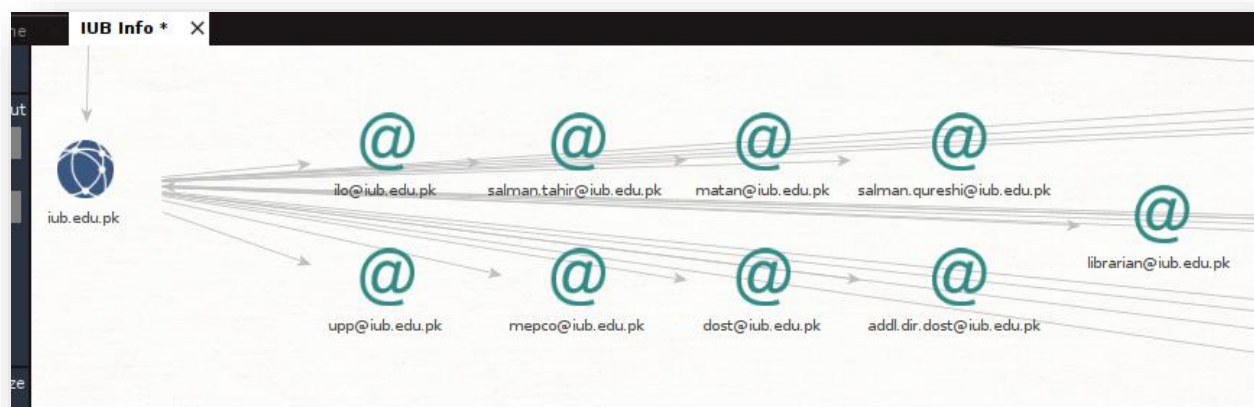
- Click on extracted IP address and run above transform.
- It extracts **IP address blocks** associated with the target domain. This reveals the network infrastructure, showing which **IP ranges are assigned to the organization**.
- These blocks help in:
 - Understanding the **target's network footprint**.
 - Identifying **potential attack surfaces** (e.g., web servers, mail servers).
 - Mapping out **related domains or subdomains hosted within the same IP range**.



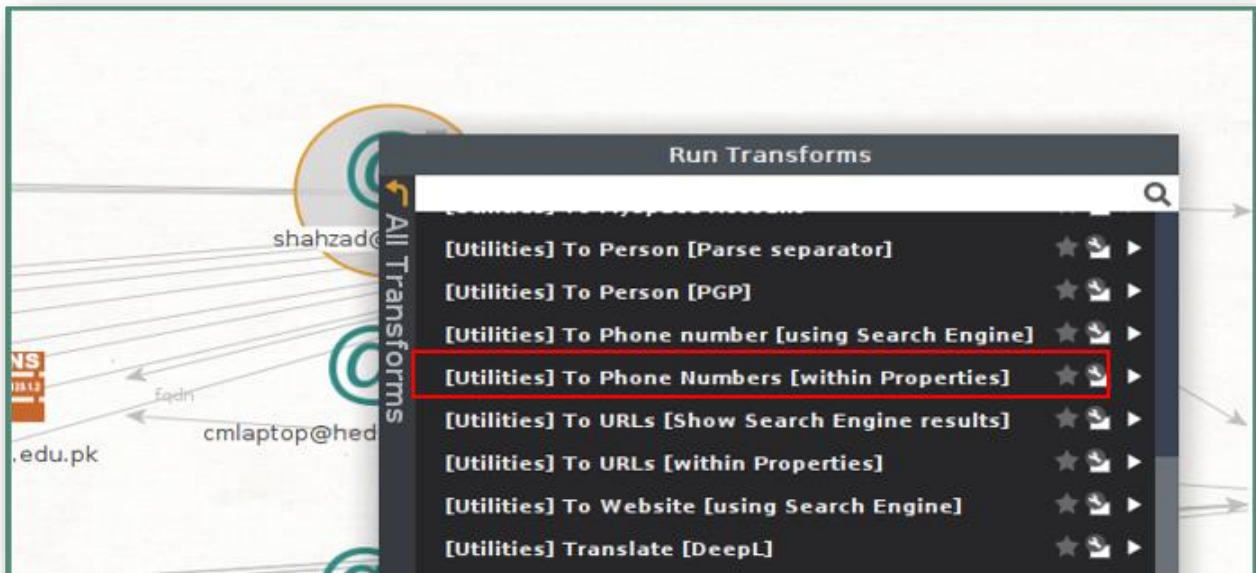
8- Finding Employees Email Addresses from Root Domain:



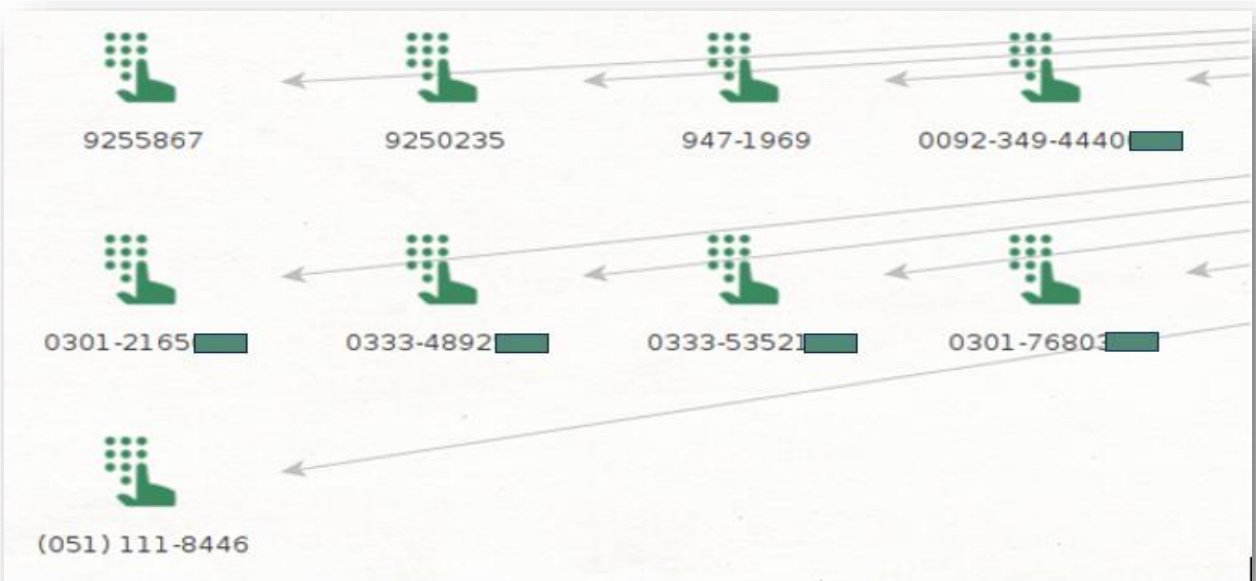
After running the above transform, it will extract the **Email addresses** of some employees:



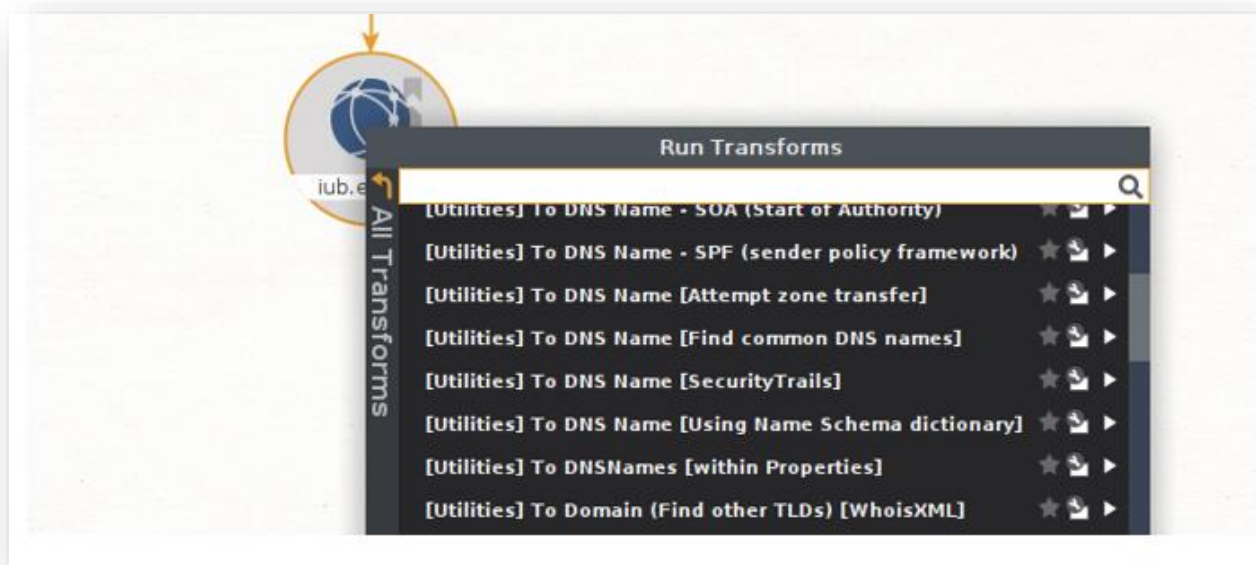
9- Finding Mobile Numbers of Employees:



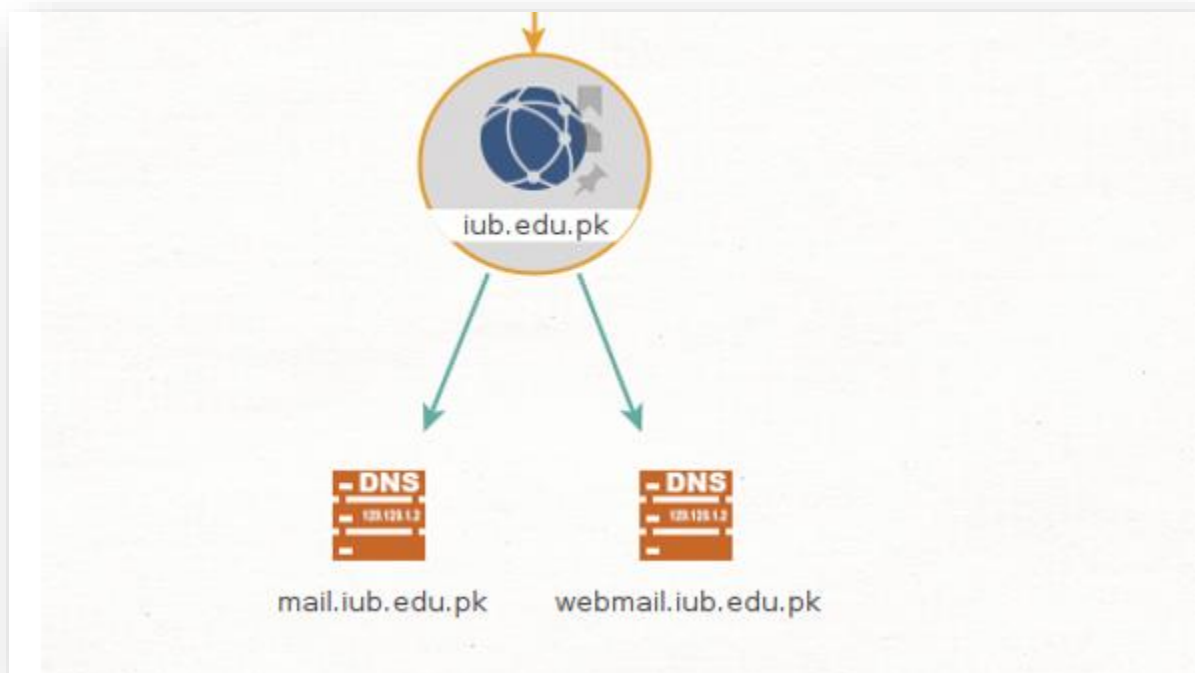
- Select Email address, and run above transform.
- It will extract the **Mobile Numbers** of that person.



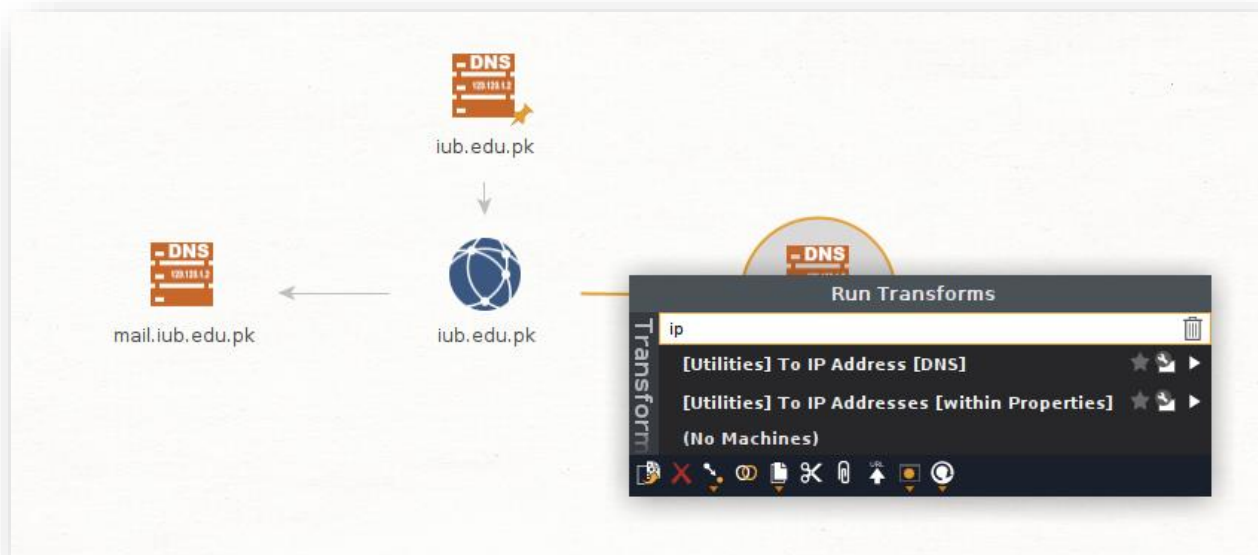
10- Finding Servers of Target Domain:



- ✚ Right Click and run the above transform.
- ✚ It will extract the web mail server of target domain.



11- Finding the IP address of Webmail Server:



After running the above transform, it will extract the IP of these servers.

