Digital Certificates:

First, we query the Certificate Transparency database at crt.sh for all subdomains of the specified domain and request the response in JSON format from URL: https://crt.sh/?q=%.iiitd.edu.in&output=json, then we extract the subdomains from the data.

```
def get_subdomains(domain):
    url = f"https://crt.sh/?q=%.{domain}&output=json"
    response = requests.get(url)
    if response.status_code != 200:
        print(f"Error: {response.status_code}")
        sys.exit(1)
    data = response.json()
    subdomains = set()
    for entry in data:
        name = entry["name_value"]
        subdomains.add(name)
    return subdomains
```

For getting subdomains, first, we generate an **API-Key** from dnsdumpster.com, after that similarly we request the response in JSON format from URL: https://api.dnsdumpster.com/domain/iiitd.edu.in

```
def get_subdomains_dnsdumpster(domain, api_key):
    url = f"https://api.dnsdumpster.com/domain/{domain}"
    headers = {
        'X-API-KEY': api_key
    }
    response = requests.get(url, headers=headers)
    if response.status_code != 200:
        print(f"Error: {response.status_code}")
        sys.exit(1)
    data = response.json()
```

```
    subdomains = set()
    for i in data['a']:
        subdomains.add(i['host'])
    return subdomains
```

We merge subdomains from both of the above methods to get a unique set of 128 subdomains.
We get the private IP addresses of the subdomain in the provided list and attempt to resolve its IP address using socket.gethostbyname()

```
def get_private_ip(subdomains):
    private_ip = {}
    for subdomain in subdomains:
        try:
            ip = socket.gethostbyname(subdomain)
            if re.match(r'^(10|172|192)\.', ip):
                private_ip[subdomain] = ip
        except:
            pass
    return private_ip
```

Part C:

Leaking private IPs can expose an organization's internal network setup, showing important systems and potential targets. Attackers can use this information to find weaknesses in public-facing services like APIs or VPNs. If they manage to hack one machine, the leaked IPs help them move deeper into the network, gaining access to more systems.