HW 4 Using Footprinting Tools.

What are the IP addresses and name servers listed for the domains?

gob.mx:

IP Address: N/A one of the main reasons why the IP address might not be displayed is likely due to privacy or security settings. Many organizations, especially government entities, use services like content delivery networks (CDNs) or proxy servers to hide or mask the real IP addresses.

Name Servers:

* + m.mx-ns.mx – 200.94.176.1
  + e.mx-ns.mx – 189.201.244.1
  + x.mx-ns.mx – 201.131.252.1
  + i.mx-ns.mx – 207.248.68.1
  + c.mx-ns.mx – 192.100.224.1, 2001:1258:0:0:0:0:0:1
  + o.mx-ns.mx – 200.23.1.1

Registrant:

* + Name: Network Information Center, S.A. de C.V.
  + Location: Monterrey, Nuevo Leon, Mexico

Administrative Contact:

* + Name: Network Information Center, S.A. de C.V.
  + Location: Monterrey, Nuevo Leon, Mexico

Technical Contact:

* + Name: Network Information Center, S.A. de C.V.
  + Location: Monterrey, Nuevo Leon, Mexico​(tccd.edu - Domain Dossi…).

tccd.edu:

IP Address: 64.28.255.100

Name Servers:

* + pdns82.ultradns.net
  + pdns82.ultradns.com
  + pdns82.ultradns.org
  + pdns82.ultradns.biz
* Administrative Contact:
  + Name: Richard Sullivan
  + Email: richard.sullivan@tccd.edu
  + Phone: +1.817.515.1821
  + Address: 1500 Houston, Fort Worth, TX 76102, USA
* Technical Contact:
  + Name: Suresh Venugopal
  + Email: suresh.venugopal@tccd.edu
  + Phone: +1.817.515.5800
  + Address: 300 Trinity Campus Circle, Fort Worth, TX 76102, USA​

tarrantcountytx.gov:

* IP Address: 192.84.52.206
* Name Servers:
  + cbru.br.ns.els-gms.att.net
  + cmtu.mt.ns.els-gms.att.net
  + ns3.tarrantcountytx.gov
  + ns4.tarrantcountytx.gov​(tarrantcountytx.gov - D…).

fbi.gov:

* IP Addresses:
  + 104.16.148.244
  + 104.16.149.244
  + 2606:4700::6810:94f4 (IPv6)
  + 2606:4700::6810:95f4 (IPv6)
* Name Servers:
  + ns-cloud-e1.googledomains.com
  + ns-cloud-e2.googledomains.com
  + ns-cloud-e3.googledomains.com
  + ns-cloud-e4.googledomains.com

How can the information from domain records be used?

Hackers:

Spearphishing: If personal names and emails are visible in domain records, attackers can send fake emails to steal information. Domains that hide personal details reduce this risk.

Reconnaissance: Exposed IP addresses and name servers help attackers map networks and find weak spots. Even without an IP, name servers can reveal vulnerabilities.

DDoS Attacks: If the IP is available, it can be targeted in DDoS attacks, overwhelming the server and causing disruption.

Ethical Hackers:

Vulnerability Testing: They use IPs and name servers to find and fix security flaws before attackers exploit them.

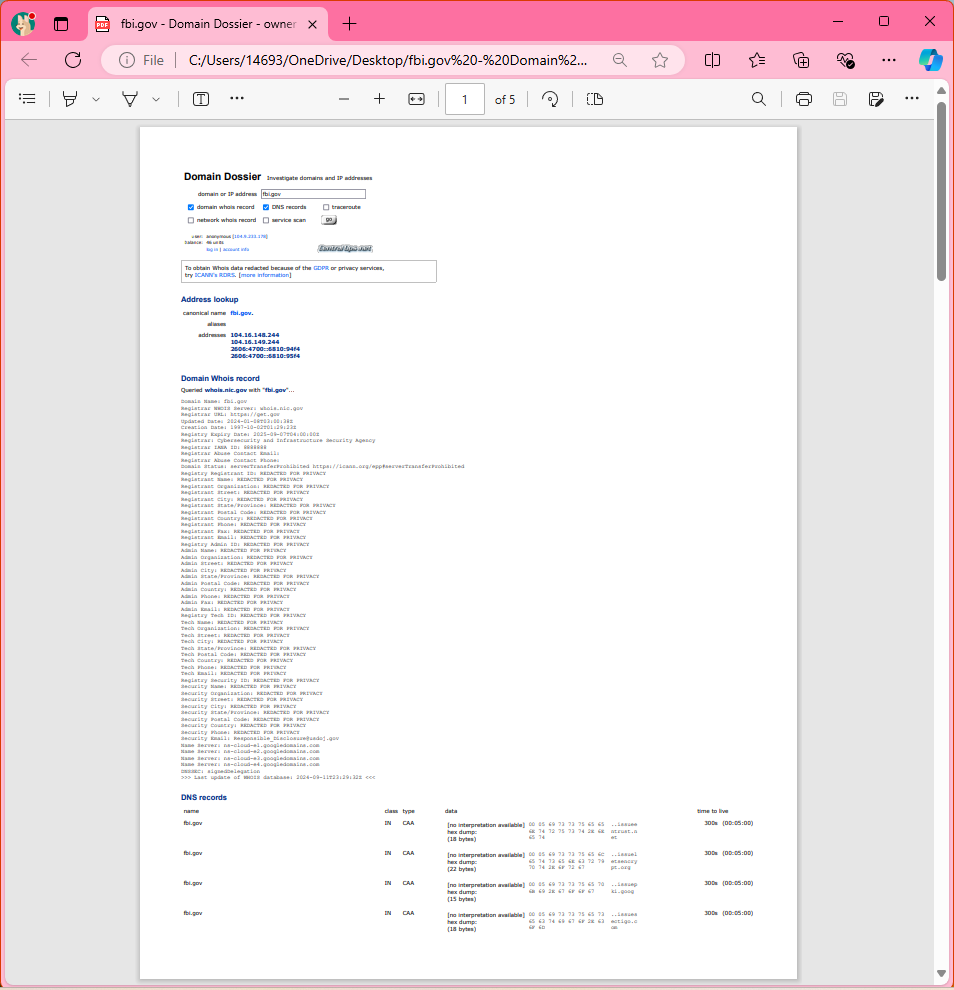
Network Monitoring: By tracking IP traffic, ethical hackers can spot suspicious activity and stop attacks early.

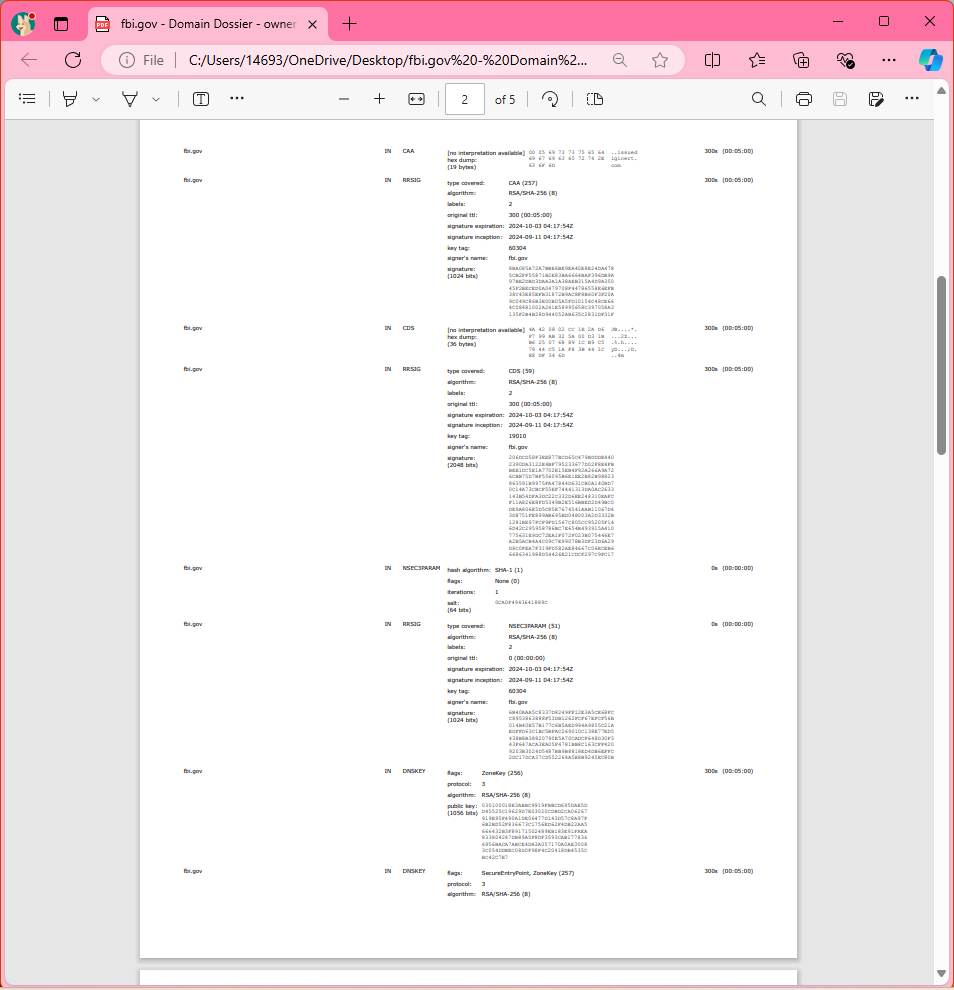
Incident Response: Access to network details allows quick action during cyberattacks to reduce damage.

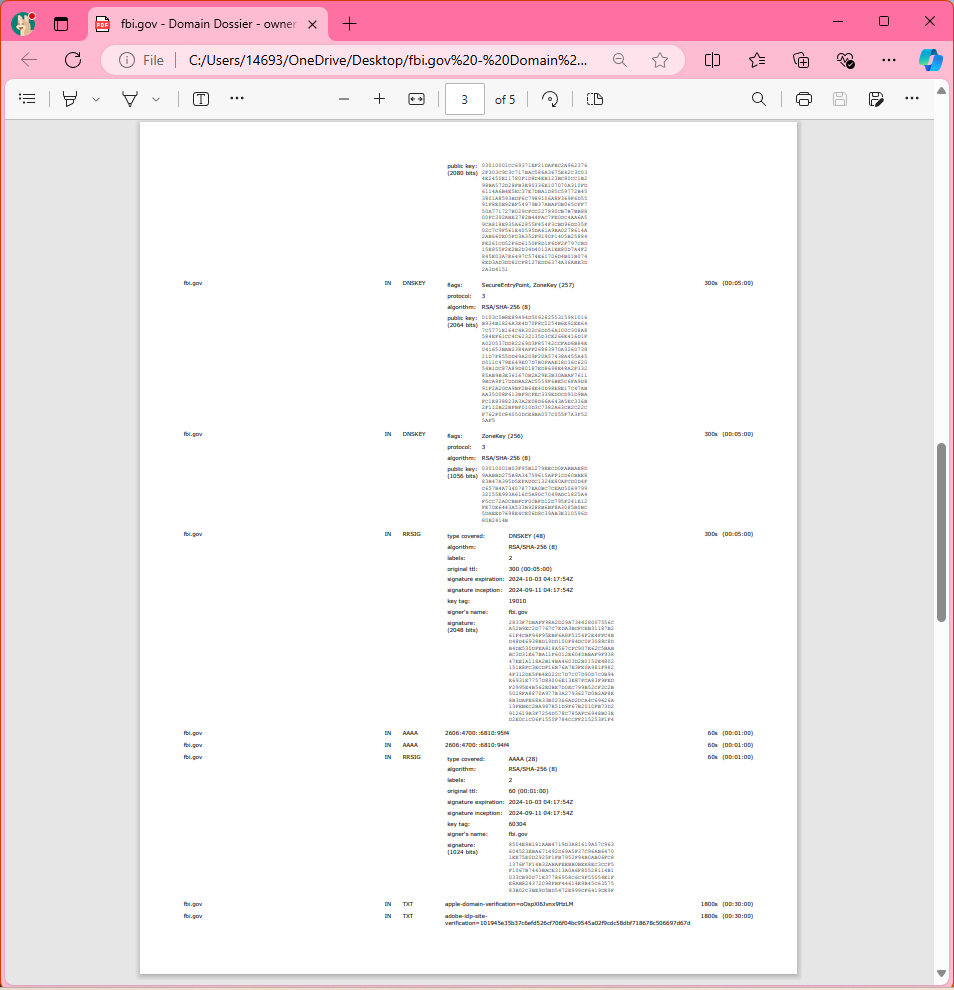
* TCCD.edu is most exposed, with detailed employee and network information, making it highly vulnerable to spearphishing and network attacks.
* Gob.mx shares network data but not personal details, offering some protection but still posing a risk for network-based attacks.
* Tarrantcountytx.gov is similar to gob.mx, sharing technical data but keeping personal details private, reducing phishing risk but still susceptible to network attacks.
* FBI.gov is the most secure, offering minimal exploitable information, protecting it from most common attacks.

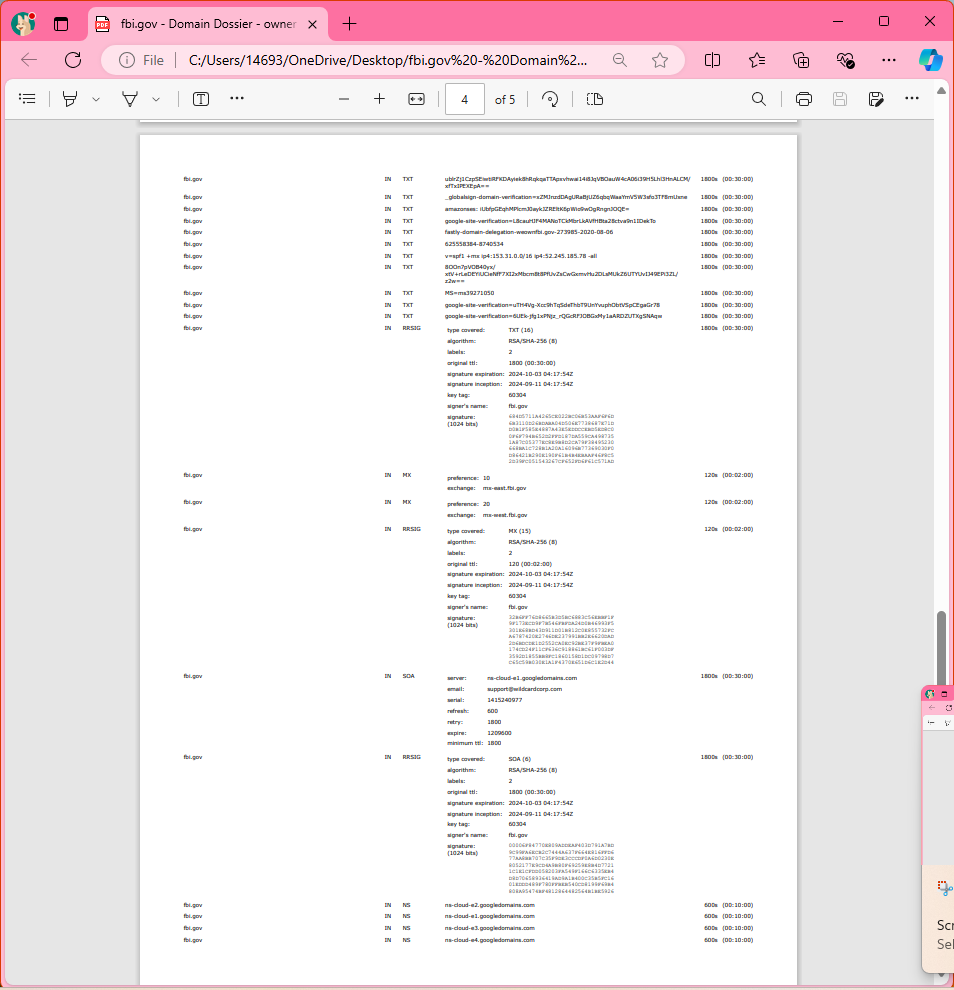
Screenshots:

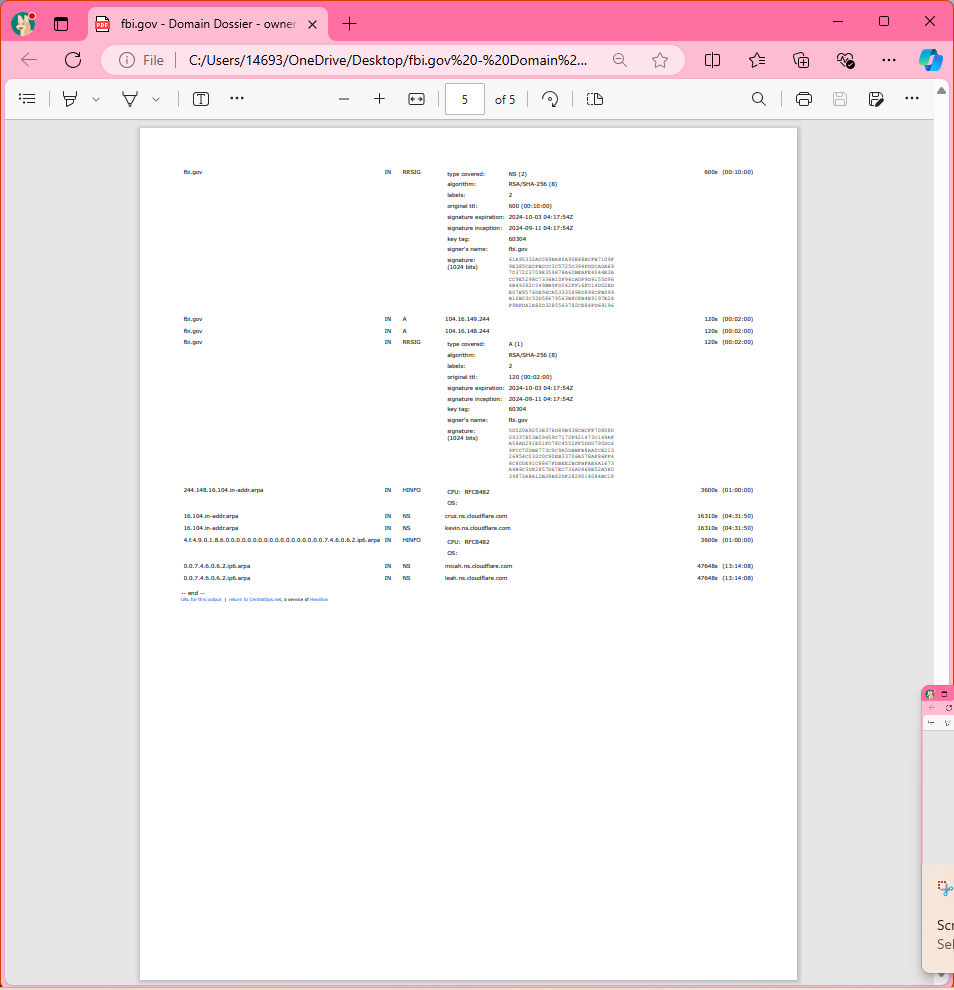
* FBI.gov:



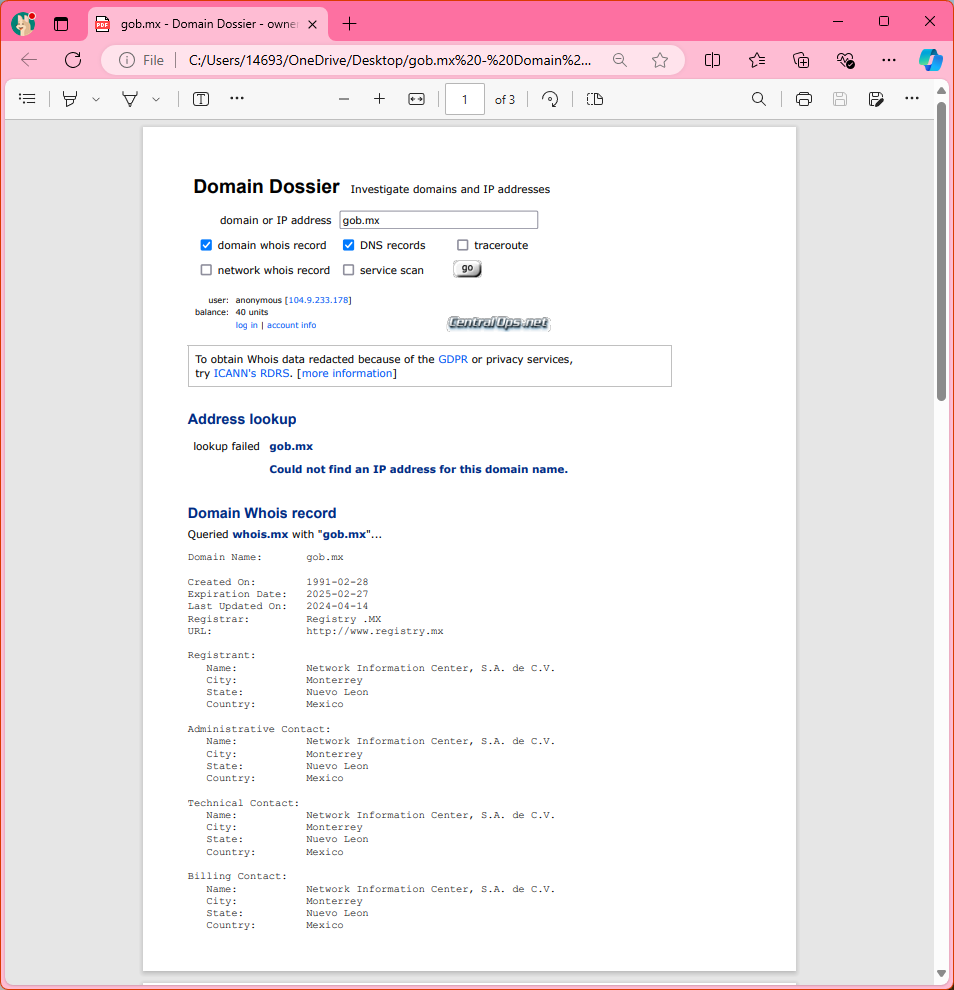


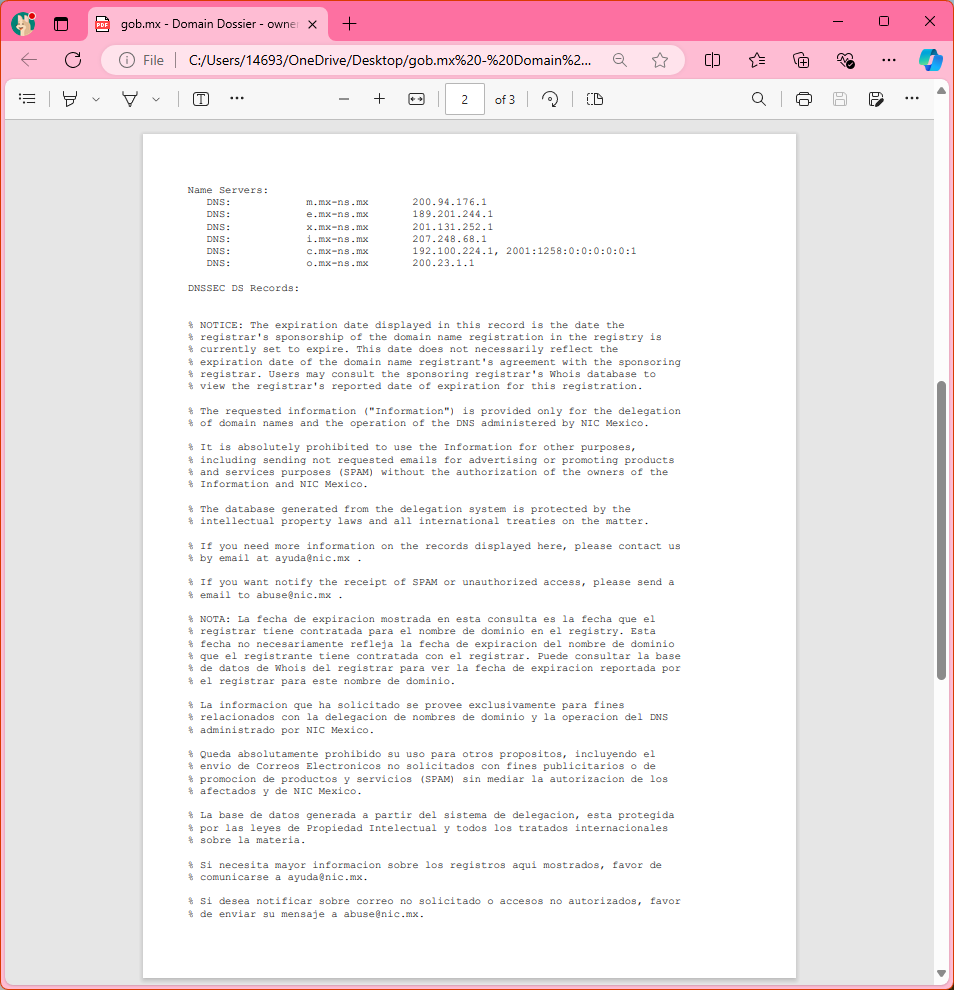


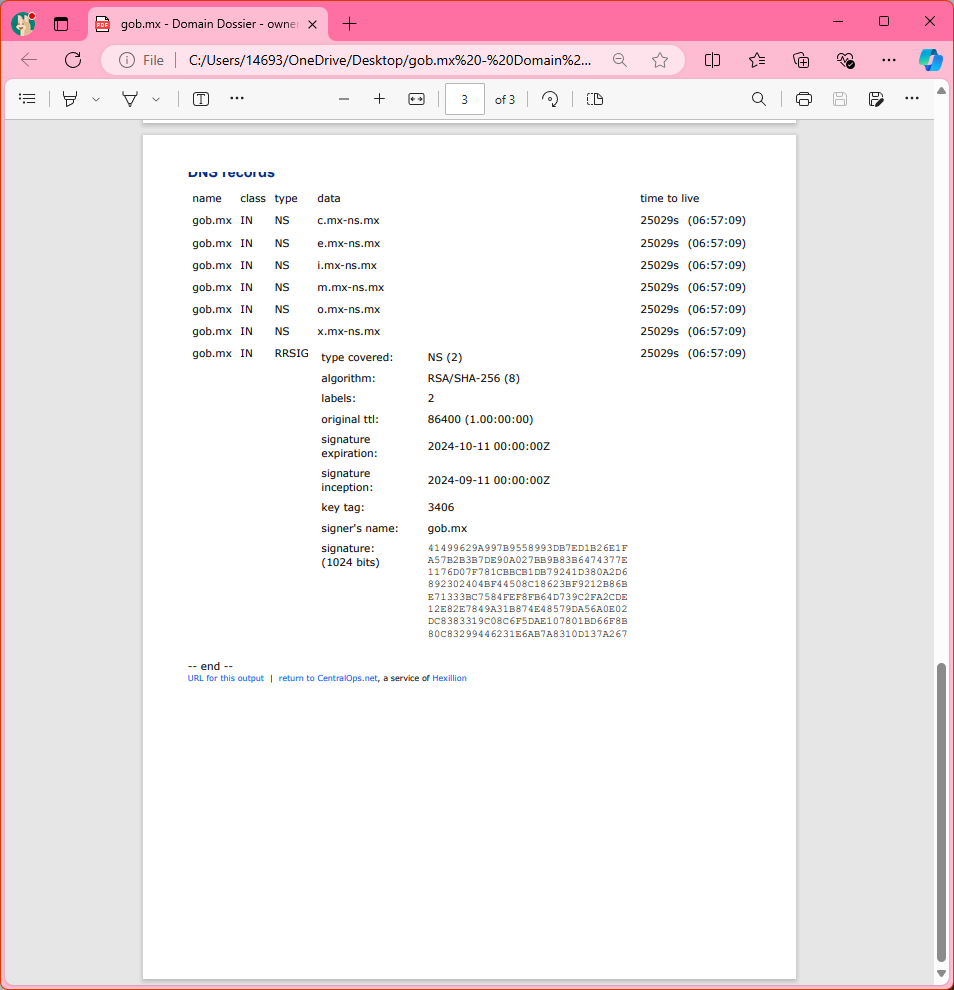




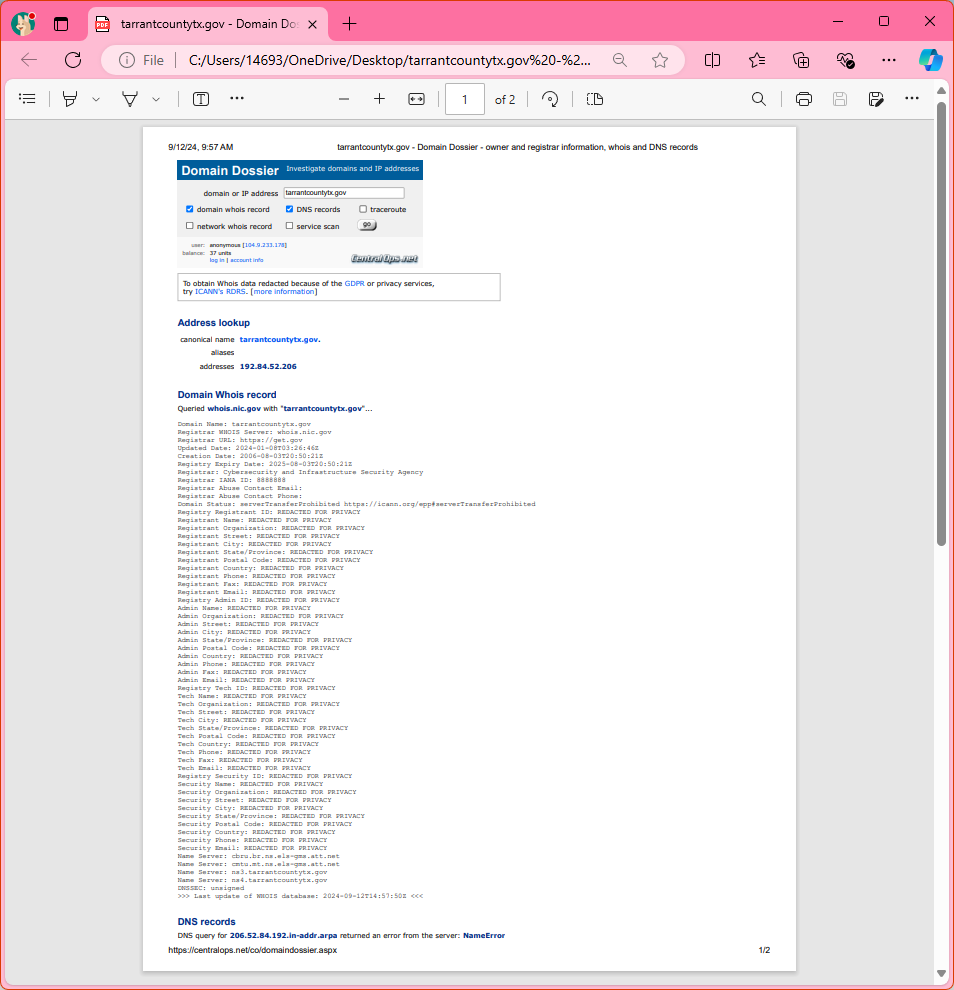
gob.mx:

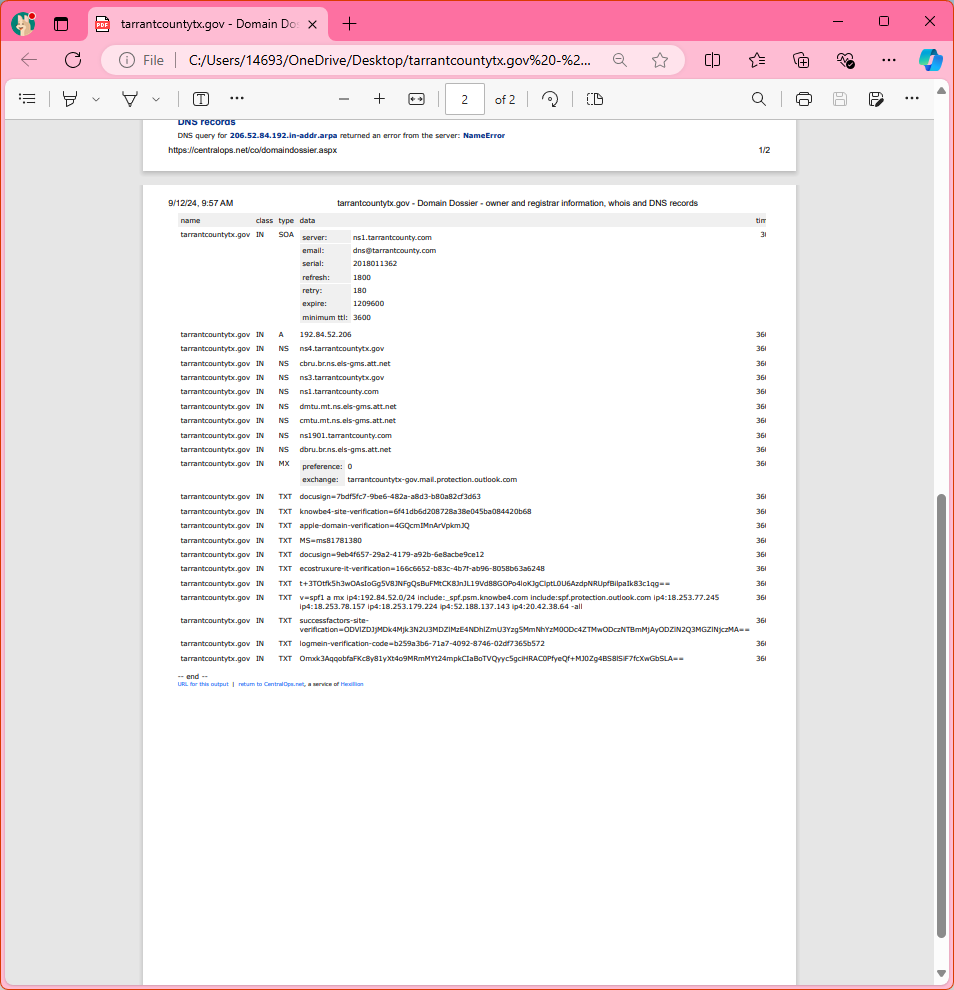






tarrantcountytx.gov:





tccd.edu:

