**PASSIVE RECONNAISSANCE**

**REPORT**

**INTRODUCTION :**

This report presents the results of passive reconnaissance performed on the target domain **ford.com**. The objective was to gather publicly available information without actively interacting with the target’s infrastructure.

**OBJECTIVE :**

* To demonstrate the process of passive footprinting and reconnaissance.
* To identify publicly available data that could aid an attacker.

**SCOPE :**

* **Target:** ford.com
* **Tools Used:** whois, dig/nslookup, subfinder, assetfinder, amass, theHarvester, exiftool, metagoofil, Maltego CE, SpiderFoot, Google Dorking, gau, katana, linkfinder, JSleak.
* **Approach:** Passive only, no active exploitation or scanning performed.

**METHODOLOGY :**

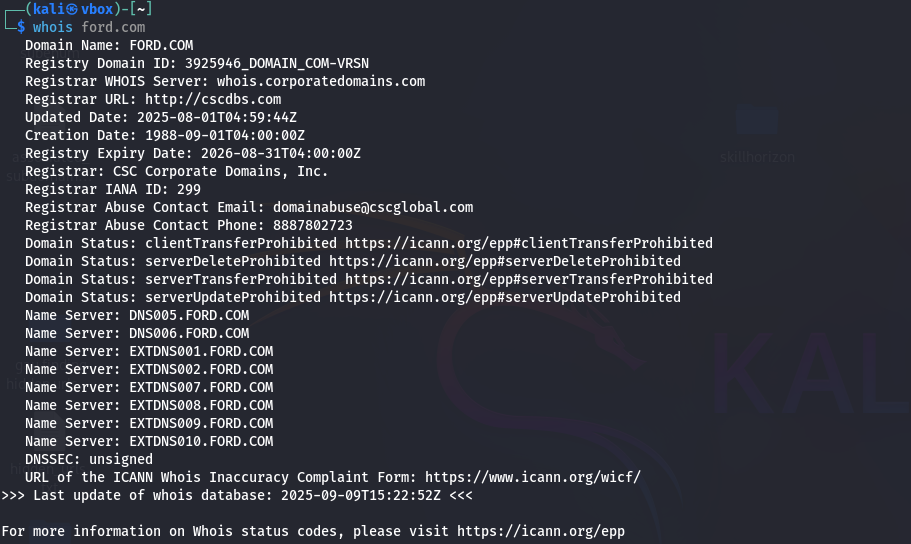
The reconnaissance was carried out in step-wise fashion:

1. WHOIS & DNS enumeration
2. Subdomain discovery
3. Email/employee data gathering
4. Metadata extraction from public documents
5. Google Dorking
6. Social media and OSINT analysis
7. URL & JavaScript file collection
8. Secret leak detection in JS

**FINDINGS :**

* **WHOIS & DNS RECORDS:**
* **WHOIS Summary:**

|  |  |
| --- | --- |
| Domain Name | FORD.COM |
| Registry Domain ID | 3925946\_DOMAIN\_COM-VRSN |
| Registrar WHOIS Server | whois.corporatedomains.com |
| Registrar URL | <http://cscdbs.com> |
| Updated Date | 2025-08-01T04:59:44Z |
| Creation Date | 1988-09-01T04:00:00Z |
| Registry Expiry Date | 2026-08-31T04:00:00Z |
| Registrar | CSC Corporate Domains, Inc. |
| Registrar IANA ID | 299 |
| Registrar Abuse Contact Email | [domainabuse@cscglobal.com](mailto:domainabuse@cscglobal.com) |
| Registrar Abuse Contact Phone | 8887802723 |
| Domain Status | clientTransferProhibited <https://icann.org/epp#clientTransferProhibited> |
| Domain Status | serverDeleteProhibited <https://icann.org/epp#serverDeleteProhibited> |
| Domain Status | serverTransferProhibited <https://icann.org/epp#serverTransferProhibited> |
| Domain Status | serverUpdateProhibited <https://icann.org/epp#serverUpdateProhibited> |
| Name Server | DNS005.FORD.COM |
| Name Server | DNS006.FORD.COM |
| Name Server | EXTDNS001.FORD.COM |
| Name Server | EXTDNS002.FORD.COM |
| Name Server | EXTDNS007.FORD.COM |
| Name Server | EXTDNS008.FORD.COM |
| Name Server | EXTDNS009.FORD.COM |
| Name Server | EXTDNS010.FORD.COM |
| DNSSEC | unsigned |

****

* **DNS Records Identified:**

|  |  |
| --- | --- |
| **Field** | **Details** |
| Command | dig ford.com |
| Query Type | A (IPv4 Address) |
| Status | NOERROR |
| Query ID | 19499 |
| Flags | qr, rd, ra |
| Question Section | ford.com IN A |
| Answer Section | ford.com → 19.12.113.37ford.com → 19.12.97.37 |
| Authority Section | None |
| Additional Section | OPT PSEUDOSECTION: EDNS version: 0, flags:; udp: 1232 |
| Query Time | 40 msec |
| DNS Server Used | 10.0.2.3 (UDP) |
| Date & Time of Query | Tue Sep 09 20:28:55 IST 2025 |
| Message Size | 1. ytes |

**A computer screen shot of a computer

AI-generated content may be incorrect.**

* **SUBDOMAIN ENUMERATION:**
* **Tools Used:** subfinder, assetfinder, amass (passive mode)
* **Subdomains Identified:** 
  + Using subfinder: (click on the file to open)



* + Using Assetfinder:



* + Using Amass: *“No assets were discovered”*

****

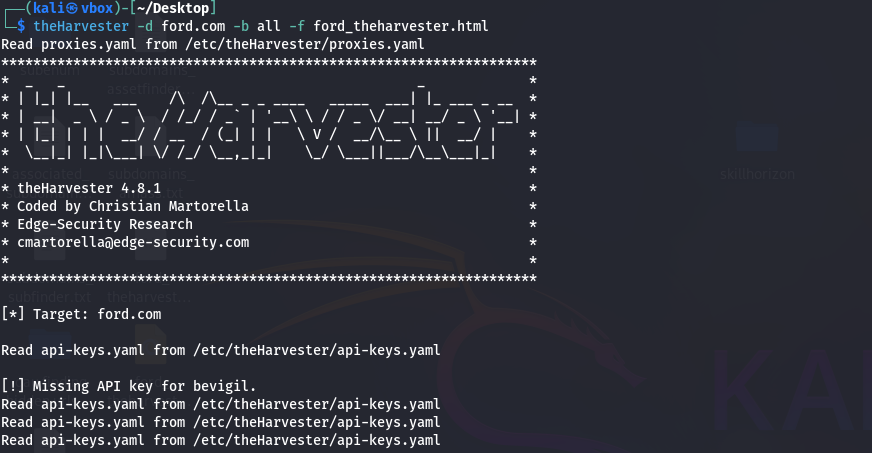
****

****

* **EMAIL & EMPLOYEE INFO:**
* **Tool Used: theHarvester**
* **Results:**
  + Emails Found: 1
  + Host Found: 2600
  + Linkedin Links Found: 0
  + Ips Found: 220
  + ASNS Found: 10

Click on the file to view:

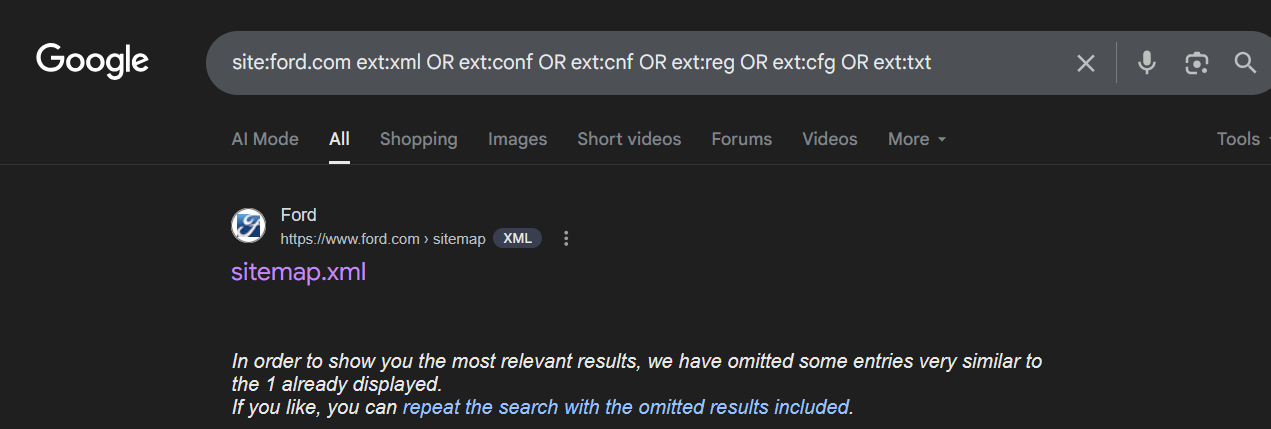


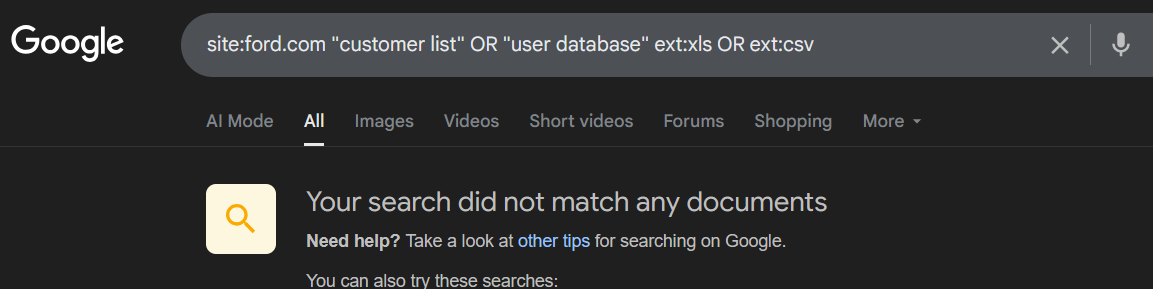


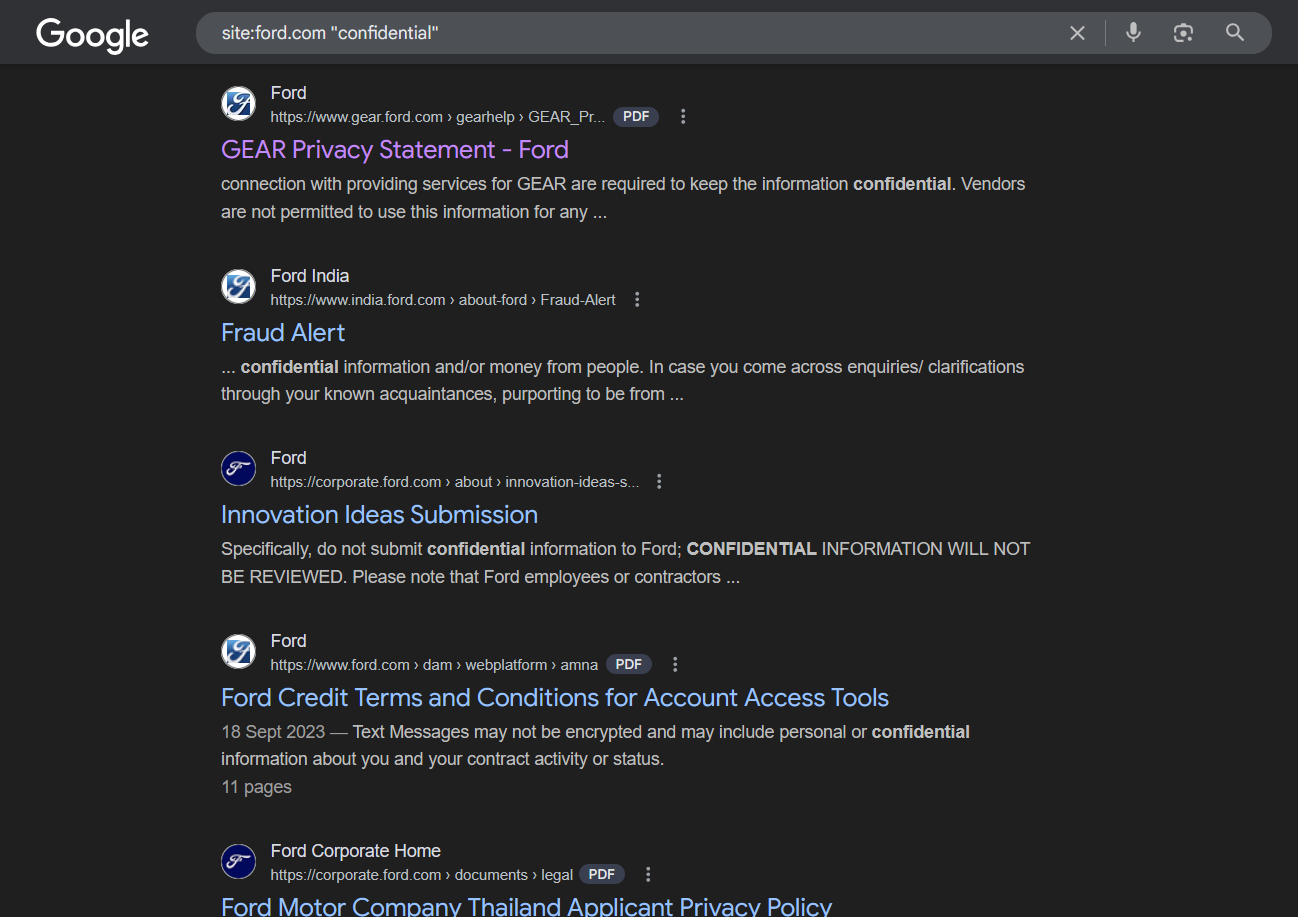
* **METADATA EXTRACTION:**
* **Tools Used:** exiftool, strings, metagoofil
* **Document Analyzed:** \*.pdf, \*.pptx, \*.docx
* **Extracted Metadata:**
* Most of the document URLs obtained (via tool like gau ) were not accessible or returned errors.
* Since no active or downloadable files were available, it was **not possible to perform metadata extraction** using exiftool, strings, or metagoofil.
* **Google Dorking:**
* **Queries Used:**
  + site:ford.com ext:xml OR ext:conf OR ext:cnf OR ext:reg OR ext:cfg OR ext:txt
  + site:ford.com "confidential"
  + site:s3.amazonaws.com ford.com
  + site:ford.com "customer list" OR "user database" ext:xls OR ext:csv
* **Interesting Results:**

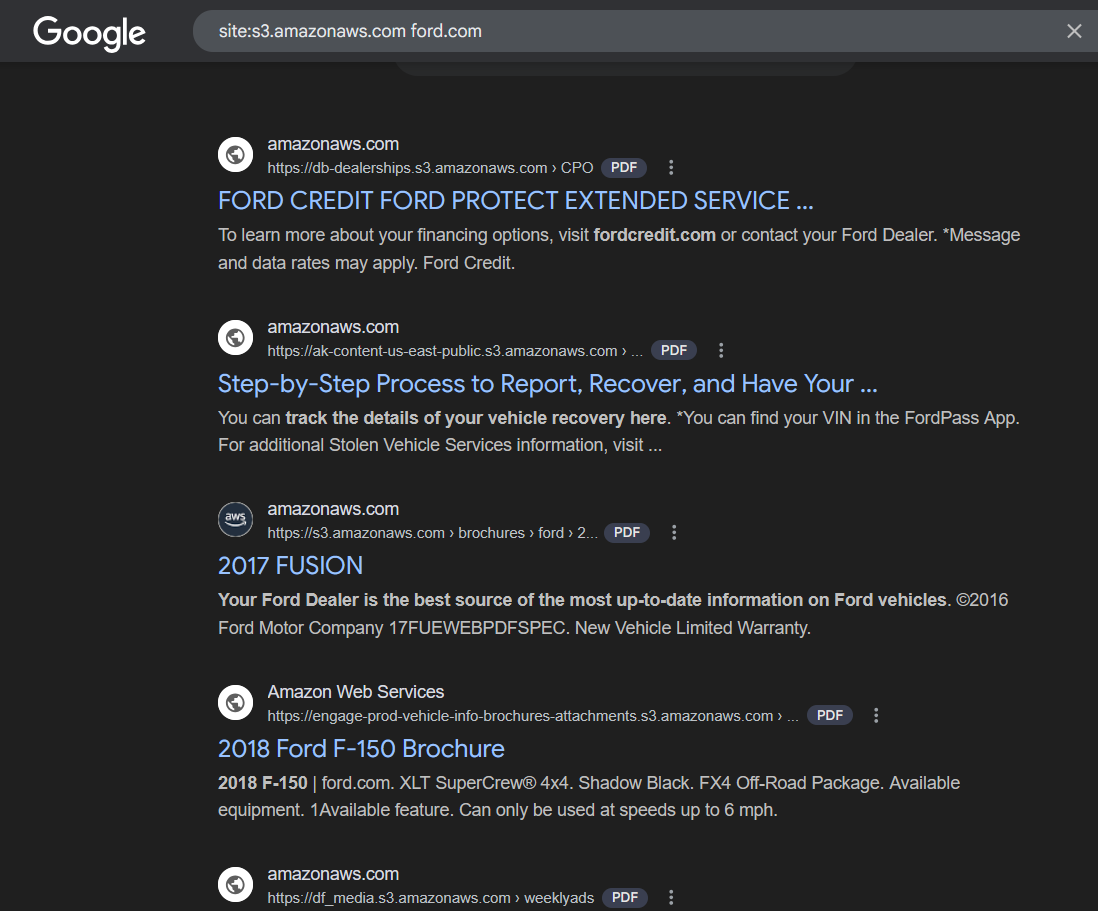










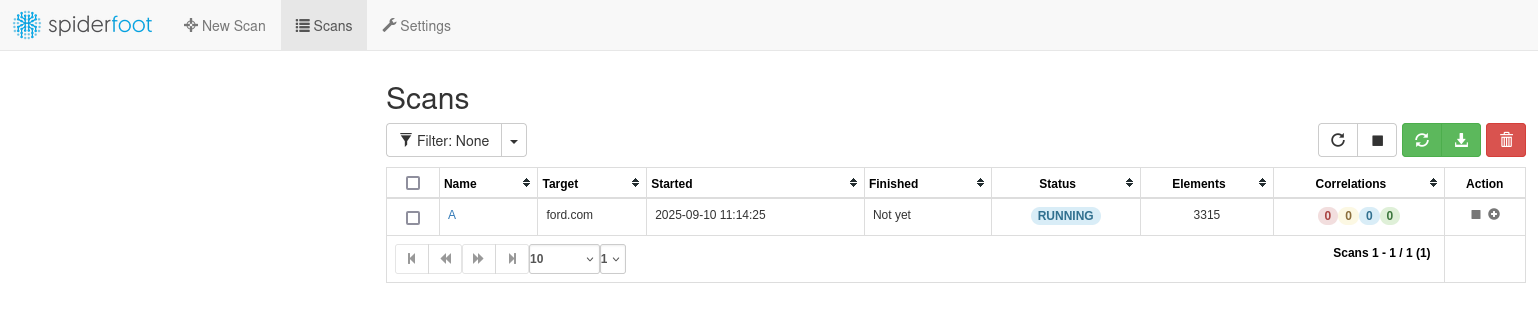


* **SOCIAL MEDIA PRESENCE & OSINT:**
* **Tools Used:** Spiderfoot, Maltego
* **Results:**
* Spiderfoot:



Maltego :

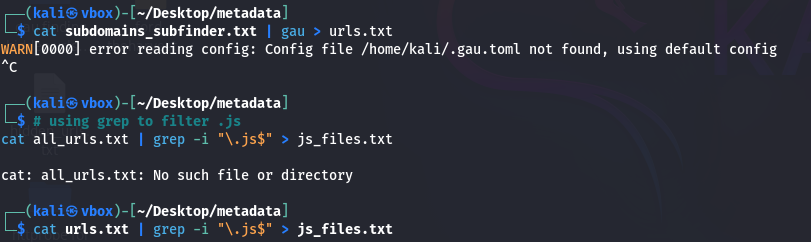
(not have a valid activation key)

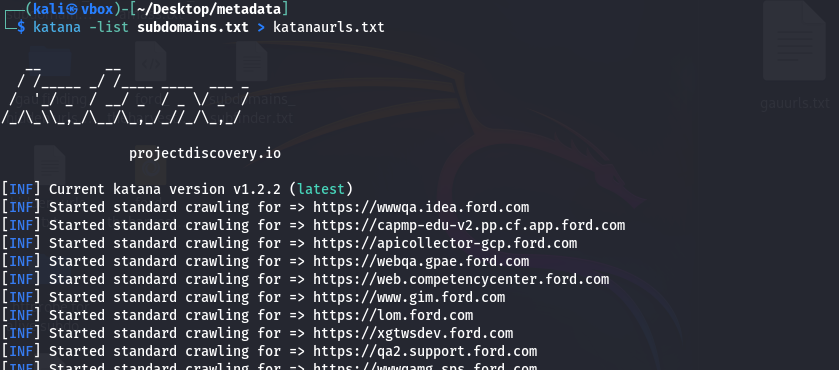


* **FILTERED JAVASCRIPT URLS:**
* **Tools Used:** GAU, KATANA
* **Results:**

****

****







* **SECRETS IN JS FILES:**
* **Tool Used:** JSleak
* **Results:**