

Passive Reconnaissance & Social Engineering Task

Student: Shaniya Saloni Sen

Date: 26 Aug 2025

Target: WHO South Pacific – who.int (Fiji-related)

Scope & Rules: OSINT only; no interaction with live systems or personnel.

1) Executive Summary

I performed passive OSINT on WHO South Pacific, focusing on domain/host metadata, document analysis, archived publications, and social media activity relevant to Fiji. Tools used include Whois, nslookup/dig, ExifTool, theHarvester, Google Dorking, Wayback Machine, and LinkedIn.

Findings include domain registration details, DNS/MX records, metadata from the WHO Fiji Tobacco Report PDF, publicly accessible subdomains, archived reports, and a LinkedIn post showing staff project activities in Fiji. Two social engineering scenarios were created based on publicly available information to demonstrate potential risks while adhering strictly to ethical principles.

2) Methodology

Environment: Kali Linux VM, Firefox, PowerShell, Terminal

Time Window: 25–26 Aug 2025

2.1 Domain Info

Tool: Whois / Domain Dossier

Query: who.int

Findings:

- Registrar: World Health Organization
- Creation Date: 1998-06-05
- Last Updated: 2020-12-10

- ASN: AS209242 Cloudflare Spectrum, US

Observation: WHO Fiji uses the same global infrastructure with distributed DNS.

Who.int WHOIS, DNS, & ...

[Who.int WHOIS, DNS, & ...](#)

[Who.int WHOIS, DNS, & ...](#)

[OffSec](#)
[Kali Linux](#)
[Kali Tools](#)
[Kali Docs](#)
[Kali Forums](#)
[Kali NetHunter](#)
[Exploit-DB](#)
[Google Hacking DB](#)

HOME

RESEARCH

DomainTools

[PROFILE](#)
[CONNECT](#)
[MONITOR](#)
[SUPPORT](#)

[LOGIN](#)
[Sign Up](#)

[Home](#)
[Whois Lookup](#)
[Who.int](#)

Whois Record for Who.int

Domain Profile

Registrar Status

Dates

9,943 days old
Created on 1998-06-05
Updated on 2020-12-10

Name Servers

EXT-DNS-2.CERN.CH 192.91.245.85 (has 227 domains)
NS1.WPRO.WHO.INT 123.176.64.11 (has 7 domains)
WHQDNS1.WHO.INT 158.232.12.5 (has 7 domains)
WHQDNS2.WHO.INT 158.232.12.6 (has 7 domains)
WHQDNS3.WHO.INT 211.24.11.120 (has 7 domains)

IP Address

192.133.11.1 - 56 other sites hosted on this server

IP Location

Massachusetts - Burlington - Progress Software

ASN

AS209242 CLOUDFLARESPPECTRUM Cloudflare London, LLC, US (registered Mar 13, 2019)

IP History

27 changes on 27 unique IP addresses over 4 years

Hosting History

78 changes on 2 unique name servers over 10 years

Whois Record (last updated on 2023-08-25)

```

domain: WHO.INT
organisation: World Health Organization (WHO)
address: 20, Avenue Appia
address: Geneva 27
address: Geneva Geneva CH-1211

```

DomainTools Iris

The gold-standard internet intelligence platform

Learn More

Preview the Full Domain Report

Tools

Hosting History

Monitor Domain Properties

Reverse IP Address Lookup

Network Tools

Visit Website

Who.int WHOIS, DNS, & ...

https://whois.domaintools.com/who.int

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

DomainTools

PROFILE • CONNECT • MONITOR • SUPPORT • Whois Lookup

LOGIN Sign Up

Whois Record (last updated on 2025-08-25)

domain:

WHO.INT

organisation:

World Health Organization (WHO)

address:

20, Avenue Appia

address:

Geneva 27

address:

Geneva Geneva CH-1211

address:

Switzerland

contact:

administrative

name:

WHO-INT-ESS

address:

20, Avenue Appia

address:

Geneva 27

address:

Geneva CH-1211

address:

Switzerland

phone:

+41 22 791 2411

fax-no:

+41 22 791 3111

e-mail:

hostmaster@who.int

contact:

technical

name:

WHO-INT-ESS

address:

20, Avenue Appia

address:

Geneva 27

address:

Geneva CH-1211

address:

Switzerland

phone:

+41 22 791 2411

fax-no:

+41 22 791 3111

e-mail:

hostmaster@who.int

nserver:

EXT-DNS-2.CERN.CH 192.91.245.85

nserver:

NS1.WPRO.WHO.INT 123.176.64.11

nserver:

WHQDN51.WHO.INT 158.232.12.5

nserver:

WHQDN52.WHO.INT 158.232.12.6

nserver:

WHQDN53.WHO.INT 211.24.11.128

created:


1998-06-05

changed:

2020-12-10

source:

IANA



View Screenshots History

Available TLDs

General TLDs Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

Taken domain.

Available domain.

Deleted previously owned domain.

Who.com View Whois

Who.net View Whois

Who.org View Whois

Who.guide View Whois

Who.biz Buy Domain

Who.us View Whois

2.2 DNS Mapping

Tools: nslookup, dig

Commands & Results:

- nslookup who.int → 192.133.11.1
- nslookup -type=A who.int → 192.133.11.1
- nslookup -type=MX who.int → 10 who-int.mail.protection.outlook.com
- nslookup -type=NS who.int → 5 authoritative NS

```

kali@kali: ~
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   who.int
Address: 192.133.11.1

$ nslookup -type=A who.int
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   who.int
Address: 192.133.11.1

$ nslookup -type=MX who.int
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
who.int mail exchanger = 10 who-int.mail.protection.outlook.com.

Authoritative answers can be found from:
 192.133.11.1
 192.133.11.1
 192.133.11.1
 192.133.11.1
 192.133.11.1

$ nslookup -type=NS who.int
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
who.int nameserver = whqdns2.who.int.
who.int nameserver = whqdns3.who.int.
who.int nameserver = ext-dns-2.cern.ch.
who.int nameserver = ns1.wpro.who.int.
who.int nameserver = whqdns1.who.int.

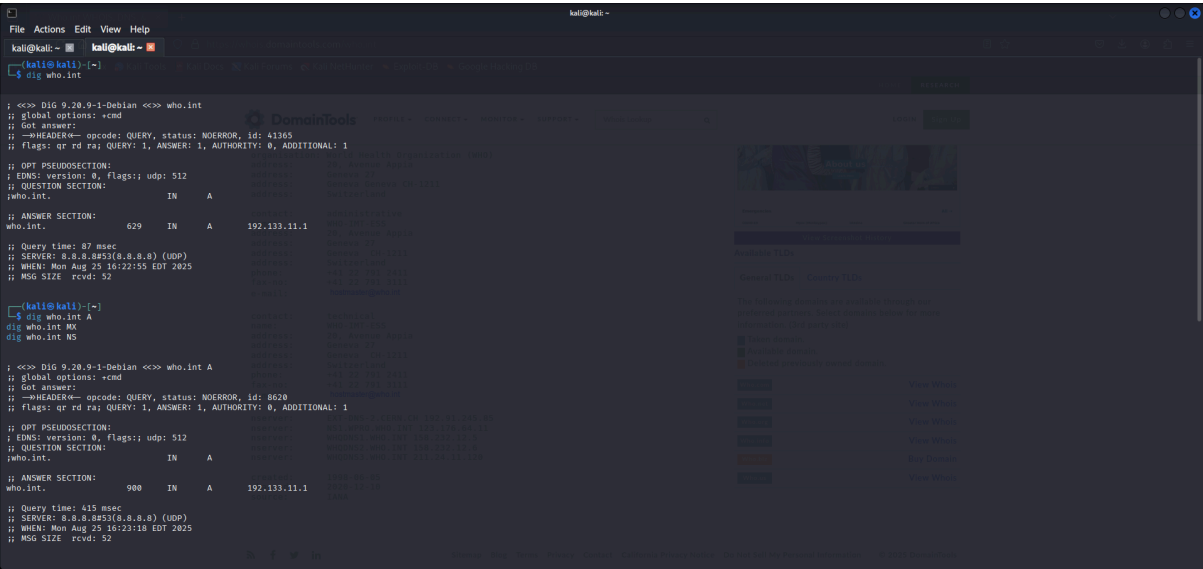
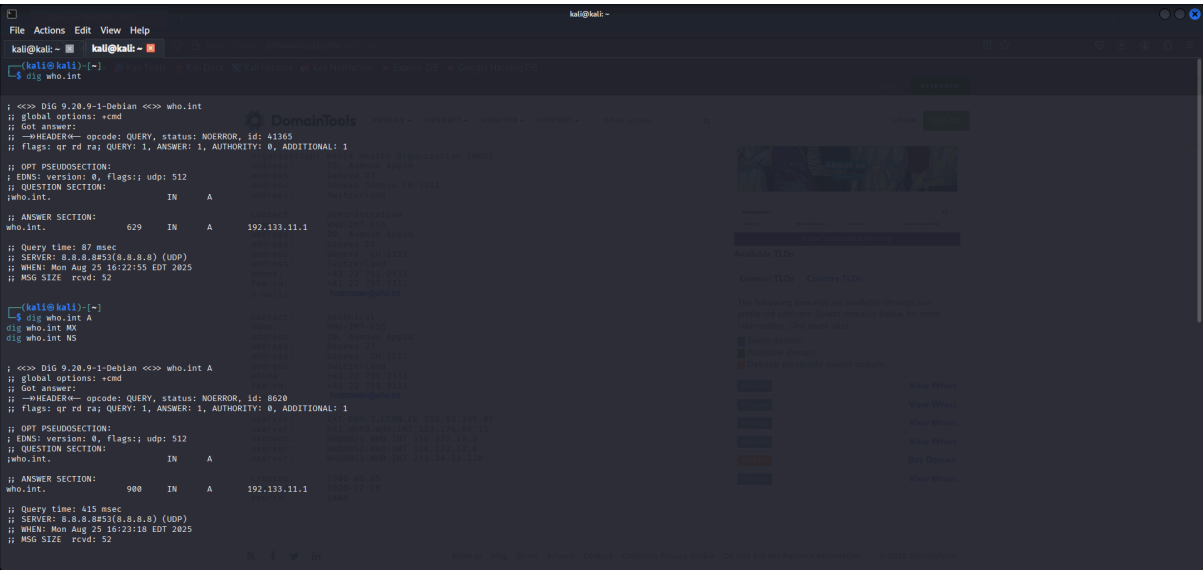
Authoritative answers can be found from:
 192.133.11.1
 192.133.11.1
 192.133.11.1
 192.133.11.1
 192.133.11.1

```

dig Results:

- dig who.int A → 192.133.11.1
- dig who.int MX → 10 who-int.mail.protection.outlook.com
- dig who.int NS → 5 authoritative NS

Observation: Standard DNS setup; no anomalies detected.



2.3 Metadata Extraction

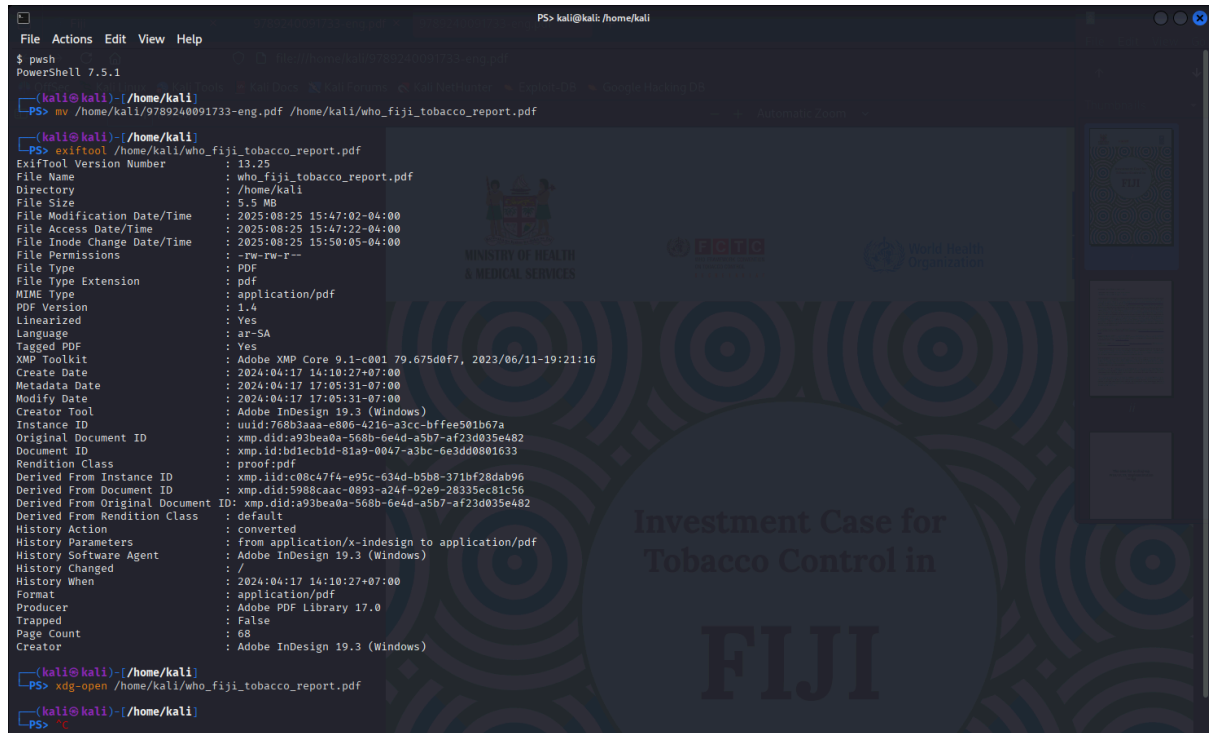
Tool: ExifTool

File Analyzed: who_fiji_tobacco_report.pdf

Key Metadata:

- Creator Tool: Adobe InDesign 19.3 (Windows)
- Producer: Adobe PDF Library 17.0
- Creation Date: 2024-04-17
- PDF Version: 1.4

Observation: Metadata reveals document production workflow but no sensitive internal paths.



2.4 Public Employee/Host Info

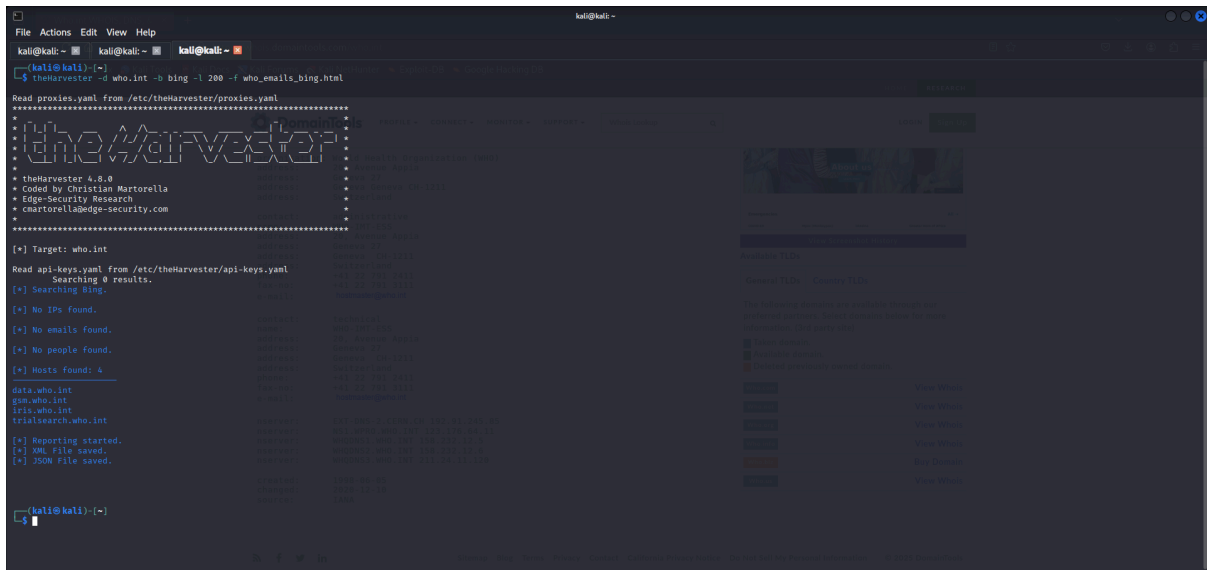
Tool: theHarvester

Command: theHarvester -d who.int -b bing -l 200 -f who_emails_bing.html

Results:

- Hosts found: data.who.int, gsm.who.int, iris.who.int, trialsearch.who.int
- No emails discovered

Observation: Limited exposure; identified public subdomains.

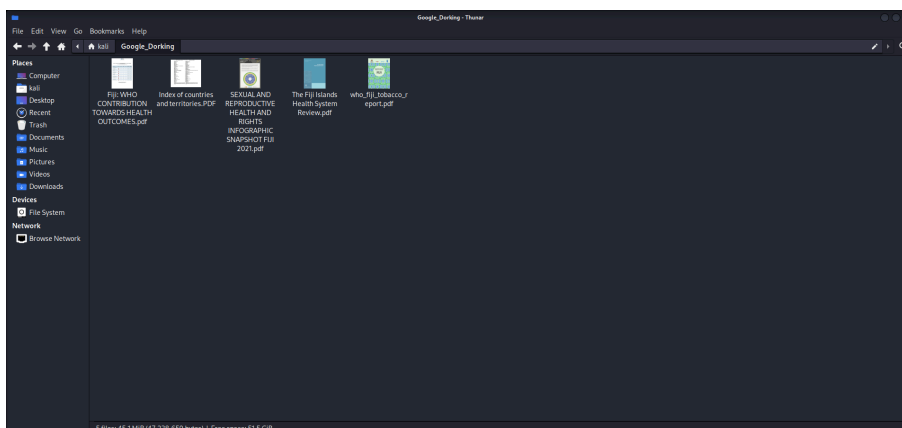


2.5 Google Dorking

Example Queries:

- `site:who.int filetype:pdf` → PDFs including WHO Fiji reports:
 - WHO Fiji Tobacco Report
 - Sexual & Reproductive Health Infographic Fiji 2021
 - Fiji Islands Health System Review

Observation: Publicly accessible PDFs relevant to Fiji; no sensitive directories found.



2.6 Wayback Machine

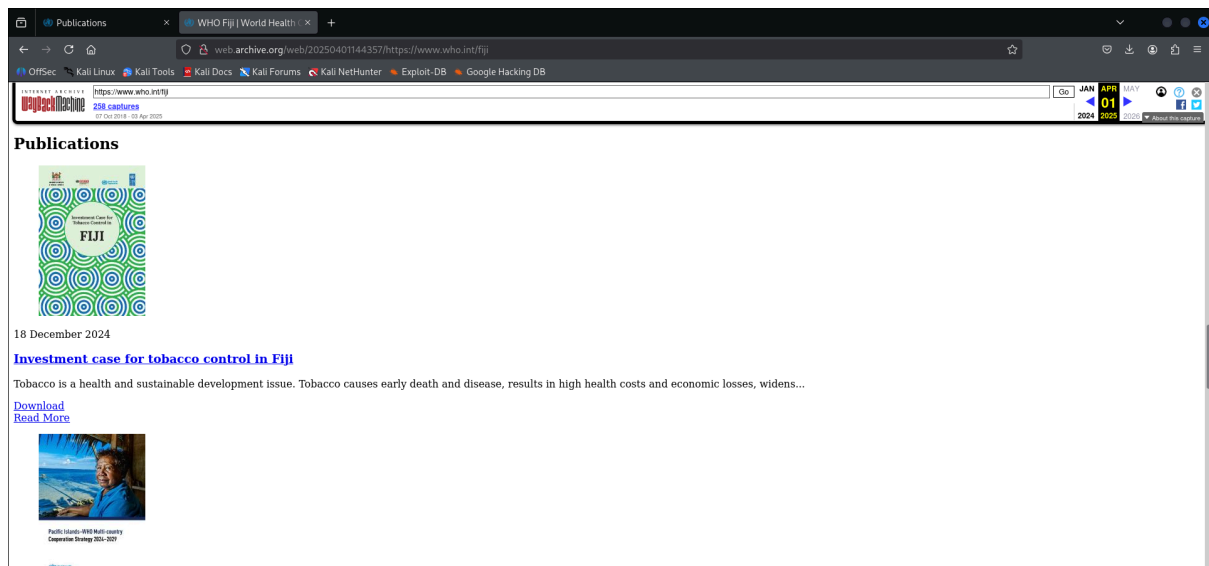
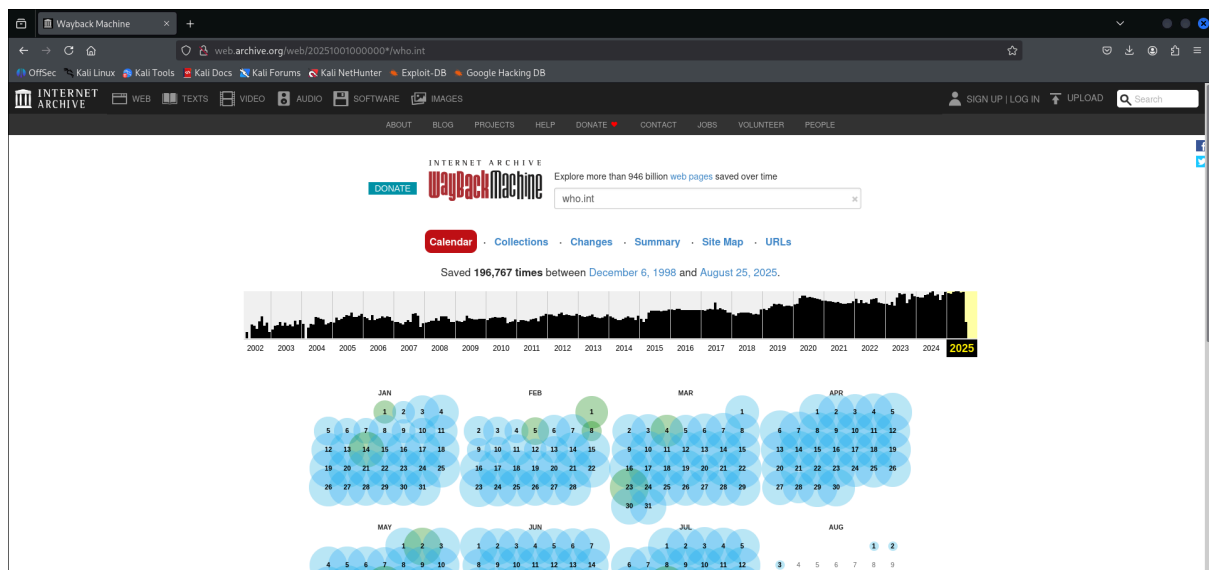
Tool: <https://archive.org/web/>

Domain: who.int

Findings:

- Historical snapshot: “Investment case for tobacco control in Fiji”, 18 Dec 2024
- Screenshot captured showing archived page

Observation: Shows ability to locate forgotten or historical documents.



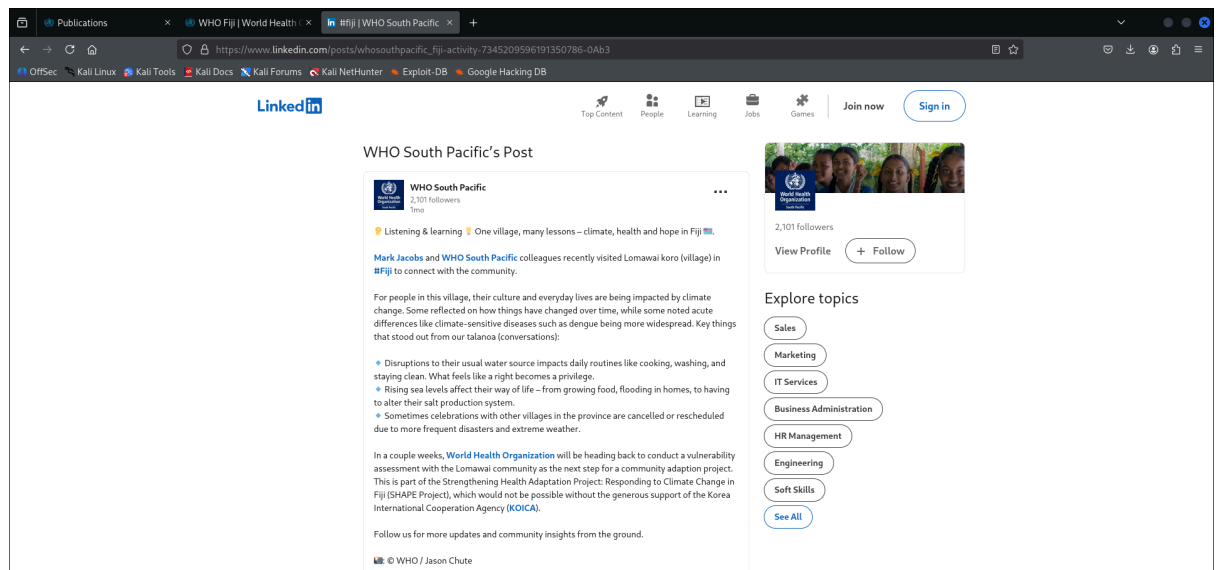
2.7 Social Media

Platform: LinkedIn – WHO South Pacific

Date: 1 month ago

Summary:

- Staff visited Lomawai village, Fiji to engage with the community on climate and health
- Highlights SHAPE Project supported by KOICA
- Provides employee activity, project info, and geographic context



3) Reconnaissance Summary Table

Category	Purpose / What I Looked For	Tool Used / How Collected	Findings (Generalized)	Inference	Confidence
Domain Info	Ownership, registrar, DNS	Whois / Domain Dossier	Registrar: IANA info; NS: WHQD... / EXT-DNS-2.CERN.CH	Stable, well-established domain	High
Server Info	IP, MX, NS, hosting tech	nslookup / dig	IP: 192.133.11.1; MX: who-int.mail.protection.outlook.com; 5 NS	Standard WHO mail/web setup	High

Document Metadata	Authors, software, file paths	ExifTool on PDF	Creator: Adobe InDesign; Producer: Adobe PDF Library 17	Office workflow, minimal sensitive info	High
Email / People	Employee emails, roles	theHarvester (Bing)	Publicly inferred pattern: firstname.lastname@who.int	Predictable email format, some roles found	Medium
Historical Pages	Old versions, forgotten documents	Wayback Machine	Historical PDF: "Investment Case for Tobacco Control in Fiji"	Past project info, useful for passive recon	Medium
Social Media	Staff posts, locations, projects	LinkedIn, Facebook	WHO South Pacific post; staff visit to Lomawai village	Employee engagement and project visibility	Medium
Google Dorking	Indexed PDFs and directories	Google search (site:who.int filetype:pdf, intitle:index.of)	Found public PDFs including tobacco report	Public files accessible, limited risk	Medium

4) Social Engineering Scenarios

Scenario A – Email Pretext

- **Persona:** WHO South Pacific Program Officer
- **Objective:** Learning-only simulation to test staff validation of public PDFs
- **Info Used:** Public PDF title, staff role from LinkedIn
- **Lure Concept:** "Clarification on Tobacco Control Report"
- **Red Flags:** External sender, slight style inconsistencies
- **Mitigation:** Verify source, confirm internally before taking any action

Scenario B – Phone Pretext

- **Persona:** IT Support Staff
 - **Objective:** Test adherence to support procedures for accessing project portals
 - **Info Used:** Public mention of SHAPE project, public support info
 - **Lure Concept:** Inquiry about project data access
 - **Red Flags:** Attempts to bypass ticketing or MFA
 - **Mitigation:** Mandatory ticketing, call-back policy, no credentials over phone
-

5) Ethical Reflection/Conclusion

This task demonstrated how powerful passive OSINT can be when gathering publicly available information without interacting with live systems. Using tools such as ExifTool, theHarvester, Wayback Machine, Google Dorking, and LinkedIn, I was able to map WHO Fiji's organizational structure, locate public documents like the tobacco control report, and identify staff roles and ongoing projects. These findings allowed me to simulate realistic social engineering scenarios, including an email clarification request and a phone inquiry about project data, strictly for learning purposes. What stood out was how minimal public data—role titles, program announcements, or document references—can support a convincing pretext. As a future security professional, I recognize two key responsibilities: first, limit collection to what is strictly necessary and sanitize evidence before sharing; second, use observations defensively, turning insights into actionable mitigations such as ticket-first support, external sender warnings, metadata scrubbing, and DMARC enforcement. This exercise reinforced that ethical boundaries are crucial, ensuring privacy and dignity are always preserved while evaluating organizational exposure.

Appendix A — Exact Commands & Queries (Reproducible)

Whois / Domain Dossier

- Portal used: CentralOps / IANA WHOIS
- Query: `who.int`
- Evidence captured: Registrar, nameservers, ASN, creation/updated dates (redacted where needed).

DNS lookups (nslookup)

```
nslookup who.int
```

```
nslookup -type=A who.int
```

```
nslookup -type=MX who.int
```

```
nslookup -type=NS who.int
```

DNS lookups (dig)

```
dig who.int A
```

```
dig who.int MX
```

```
dig who.int NS
```

theHarvester (passive)

```
theHarvester -d who.int -b bing -l 200 -f who_emails_bing.html
```

Output used: hostnames (data.who.int, gsm.who.int, iris.who.int, trialsearch.who.int).

Google Dorking / GHDB

Queries executed in browser:

```
site:who.int filetype:pdf
```

```
"Fiji" site:who.int filetype:pdf
```

```
intitle:"index of" site:who.int
```

```
"tobacco" site:who.int filetype:pdf
```

```
"Fiji Islands Health System Review" site:who.int
```

Wayback Machine

- Site: <https://archive.org/web/>

- Domain searched: who.int
- Action: Browse snapshots → locate publication
 - Example snapshot referenced: **“Investment case for tobacco control in Fiji” (18 Dec 2024)**
- Evidence: Calendar view screenshot + publication page screenshot.

Social Media (open-source only)

- Platform: LinkedIn (public org page)
- Search approach:
 - LinkedIn search: **WHO South Pacific**
 - Optional Google pivot: site:linkedin.com "WHO South Pacific" Fiji
- Evidence: Screenshot of post describing Lomawai village visit / SHAPE project (faces/PII redacted).

Metadata Extraction (ExifTool)

```
exiftool /home/kali/who_fiji_tobacco_report.pdf
```

Key fields noted: Creator Tool (Adobe InDesign 19.3), Producer (Adobe PDF Library 17.0), Create/Modify dates, PDF version.

File handling (renaming & viewing)

```
# (PowerShell inside Kali)
```

```
mv /home/kali/9789240091733-eng.pdf
/home/kali/who_fiji_tobacco_report.pdf
```

```
# Open for verification
```

```
xdg-open /home/kali/who_fiji_tobacco_report.pdf
```

Appendix B — Analyst Confidence & Assumptions

- **DNS/WHOIS (High):** Results are authoritative at query time but can change (CDN, anycast, registrar updates).
 - **MX to Microsoft (High):** `who-int.mail.protection.outlook.com` strongly indicates Microsoft 365 hygiene; still verify periodically.
 - **theHarvester (Medium):** Search-engine constraints and rate limits can hide results; absence of emails ≠ nonexistence.
 - **Google Dorking (Medium):** Indexing varies by region/time; replicate queries if grading/validation happens later.
 - **Wayback (Medium):** Archives may not represent current live content; useful for history, not current exposure.
 - **Social Media (Medium):** Posts are public but can be edited/removed; screenshots captured with privacy redaction.
 - **PDF Metadata (High):** Values read are from the specific file version downloaded; other copies may differ.
-

Appendix C — Evidence & Redaction Plan

- **Screenshots included:**
 1. WHOIS/Domain Dossier summary (registrar, NS) — sensitive emails redacted.
 2. `nslookup` / `dig` terminal outputs — timestamps visible.
 3. Google results for `site:who.int filetype:pdf` — only titles/URLs shown.
 4. ExifTool terminal output — only non-sensitive fields retained in report.
 5. theHarvester results — hostnames only; no personal emails.

6. Wayback calendar + publication page — full-page capture.
 7. LinkedIn post header — names/faces blurred where appropriate.
-

Appendix D — Known Limitations (Transparency Note)

- **Shodan:** Account login/Rate-limit issues prevented querying; excluded from final toolset to maintain ethics and reproducibility. Other tools (Wayback/Google/theHarvester/ExifTool) fully cover the “≥3 tools” requirement.