

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

- Name Servers: EXT-DNS-2.CERN.CH, NS1.WPRO.WHO.INT, WHQDNS1-3.WHO.INT
- IP Address: 192.133.11.1
- ASN: AS209242 Cloudflare Spectrum, US

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

The image contains two side-by-side screenshots of the DomainTools Whois Lookup interface. Both screenshots show the results for the domain WHO.int and WHO.INT respectively, with identical information. The results include:

- Registrar Status:** WHO.int is 9,943 days old, created on 1998-06-05, updated on 2020-12-10.
- Name Servers:** EXT-DNS-2.CERN.CH, NS1.WPRO.WHO.INT, WHQDNS1.WHO.INT, WHQDNS2.WHO.INT, WHQDNS3.WHO.INT.
- IP Address:** 192.133.11.1 - 56 other sites hosted on this server.
- IP Location:** Massachusetts - Burlington - Progress Software
- ASN:** AS209242 CLOUDFLARESPECTRUM 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 2025-08-25. Shows the WHO.int WHOIS record with the following details:

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 (has 227 domains)
nserver:	NS1.WPRO.WHO.INT 123.176.64.11 (has 7 domains)
nserver:	WHQDNS1.WHO.INT 158.232.12.5 (has 7 domains)
nserver:	WHQDNS2.WHO.INT 158.232.12.6 (has 7 domains)
nserver:	WHQDNS3.WHO.INT 211.24.11.120 (has 7 domains)

The right side of both screenshots displays a sidebar with various DomainTools services and a thumbnail image of medical professionals in scrubs.

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

The screenshot shows the DomainTools web application interface. The left pane displays a terminal window with the following command history:

```

kali㉿kali: ~ [kali@kali: ~] nslookup who.int
Server: 8.8.8.8 Address: 8.8.8.853
Non-authoritative answer:
Name: who.int
Address: 192.133.11.1

(kali㉿kali: ~) $ nslookup -type=A who.int
Server: 8.8.8.8 Address: 8.8.8.853
Non-authoritative answer:
Name: who.int
Address: 192.133.11.1

(kali㉿kali: ~) $ nslookup -type=MX who.int
Server: 8.8.8.8 Address: 8.8.8.853
Non-authoritative answer:
Name: who.int
Address: 192.133.11.1

(kali㉿kali: ~) $ nslookup -type=NS who.int
Server: 8.8.8.8 Address: 8.8.8.853
Non-authoritative answer:
Name: who.int
Address: 192.133.11.1

```

The right pane shows a search results page for "who.int" with various WHOIS and domain information listed.

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.

Detailed description: This screenshot shows the DomainTools web interface. In the top navigation bar, 'WHOIS' is selected. The main content area displays the WHOIS record for the domain 'who.int'. The record includes fields such as 'Name Server', 'Address', 'Phone', 'Email', and 'MX Record'. Below the WHOIS data, there's a sidebar titled 'Available TLDs' and 'General TLDs - Country TLDs' with several buttons like 'View Whois', 'Buy Domain', etc.

```

; <>> Dig 9.20.9-1-Debian <>> who.int
; Global options: +cmd
; Got answer:
; =HEDER=  opcode: QUERY, status: NOERROR, id: 43365
; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; QUESTION SECTION:
; who.int.           IN  A
;
; ANSWER SECTION:
; who.int.       629  IN  A    192.133.11.1
;
; Query time: 87 msec
; SERVER: 8.8.8.8#53(8.8.8.8) UDP
; WHEN: Mon Aug 25 16:22:55 EDT 2025
; MSG SIZE rcvd: 52

;(kali㉿kali)-[~]
$ dig who.int

; <>> Dig 9.20.9-1-Debian <>> who.int A
; Global options: +cmd
; Got answer:
; =HEDER=  opcode: QUERY, status: NOERROR, id: 8620
; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; QUESTION SECTION:
; who.int.           IN  A
;
; ANSWER SECTION:
; who.int.       900  IN  A    192.133.11.1
;
; Query time: 415 msec
; SERVER: 8.8.8.8#53(8.8.8.8) UDP
; WHEN: Mon Aug 25 16:23:18 EDT 2025
; MSG SIZE rcvd: 52

```

Detailed description: This screenshot shows the DomainTools web interface, identical to the one above but with a different session ID. It displays the WHOIS record for 'who.int' with the same fields and layout. The sidebar on the right also shows 'Available TLDs' and 'General TLDs - Country TLDs' buttons.

```

; <>> Dig 9.20.9-1-Debian <>> who.int
; Global options: +cmd
; Got answer:
; =HEDER=  opcode: QUERY, status: NOERROR, id: 43365
; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; QUESTION SECTION:
; who.int.           IN  A
;
; ANSWER SECTION:
; who.int.       629  IN  A    192.133.11.1
;
; Query time: 87 msec
; SERVER: 8.8.8.8#53(8.8.8.8) UDP
; WHEN: Mon Aug 25 16:22:55 EDT 2025
; MSG SIZE rcvd: 52

;(kali㉿kali)-[~]
$ dig who.int

; <>> Dig 9.20.9-1-Debian <>> who.int A
; Global options: +cmd
; Got answer:
; =HEDER=  opcode: QUERY, status: NOERROR, id: 8620
; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; QUESTION SECTION:
; who.int.           IN  A
;
; ANSWER SECTION:
; who.int.       900  IN  A    192.133.11.1
;
; Query time: 415 msec
; SERVER: 8.8.8.8#53(8.8.8.8) UDP
; WHEN: Mon Aug 25 16:23:18 EDT 2025
; MSG SIZE rcvd: 52

```

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.

The terminal window shows the following command and its output:

```
$ pshw
PowerShell 7.5.1
$ exiftool /home/kali/who_fiji_tobacco_report.pdf
File Name           : who_fiji_tobacco_report.pdf
ExifTool Version Number : 13.25
Directory          : /home/kali
File Size          : 5.5 MB
File Modification Date/Time : 2025:08:25 15:47:02-04:00
File Access Date/Time : 2025:08:25 15:47:22-04:00
File Inode Change Date/Time : 2025:08:25 15:50:05-04:00
File Permissions   : -rw-rw-r-
File Type          : PDF
File Type Extension: pdf
MIME Type          : application/pdf
PDF Version        : 1.4
Linearized         : Yes
Language           : en-US
Tagged PDF         : Yes
XMP Toolkit        : Adobe XMP Core 9.1-c001 79.675d0f7, 2023/06/11-19:21:16
Create Date        : 2024:04:17 14:10:27+07:00
Metadata Date     : 2024:04:17 17:05:31-07:00
Modify Date        : 2024:04:17 17:05:31-07:00
Creator Tool       : Adobe InDesign 19.3 (Windows)
Instance ID        : uuid:768b3aaa-e806-4216-a3cc-bffee501b67a
Original Document ID : xmp.did:a93bea0a-568b-6e4d-a5b7-af23d035e482
Document ID       : xmp.id:bdec6b1d-81a9-0047-a3bc-6e3dd0801633
Rendition Class   : proof/pdf
Derived From Instance ID : xmp.iid:c08c47f4-e95c-63ad-b5b8-371bf28ab96
Derived From Document ID : xmp.did:5988caac-0893-a24f-92e9-28335ec81c56
Derived From Original Document ID : xmp.did:a93bea0a-568b-6e4d-a5b7-af23d035e482
Derived From Rendition Class : default
History Action    : converted
History Parameters : from application/x-indesign to application/pdf
History Software Agent : Adobe InDesign 19.3 (Windows)
History Changed   :
History When      : 2024:04:17 14:10:27+07:00
Format             : application/pdf
Producer           : Adobe PDF Library 17.0
Trapped            : False
Page Count         : 68
Creator            : Adobe InDesign 19.3 (Windows)

(kali㉿kali)-[~/home/kali]
└─$ mv /home/kali/9789240091733-eng.pdf /home/kali/who_fiji_tobacco_report.pdf

(kali㉿kali)-[~/home/kali]
└─$ xdg-open /home/kali/who_fiji_tobacco_report.pdf

(kali㉿kali)-[~/home/kali]
└─$ ``
```

The background shows a presentation slide titled "Investment Case for Tobacco Control in FIJI" with logos for the Ministry of Health & Medical Services, FCTC, and World Health Organization.

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.

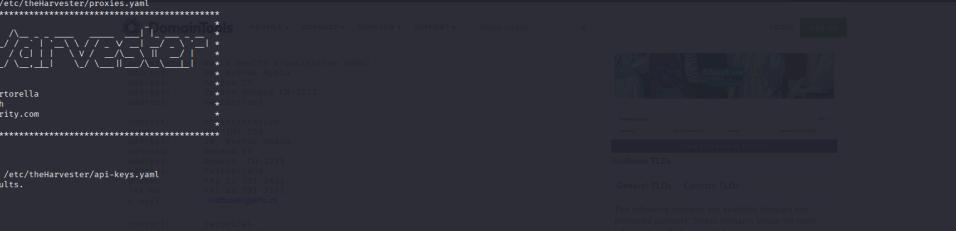
```
[*] Target: who.int
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
    Searching 0 results.

[*] Searching Bing.
[*] No IPs found.
[*] No emails found.
[*] No people found.
[*] Hosts found: 4
data.who.int
zen.who.int
iris.who.int
trialssearch.who.int

[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.

[+] Created: 1998-05-05
[+] Changed: 2020-12-10
[+] Country: ZA

(kali㉿kali)-[~]
```

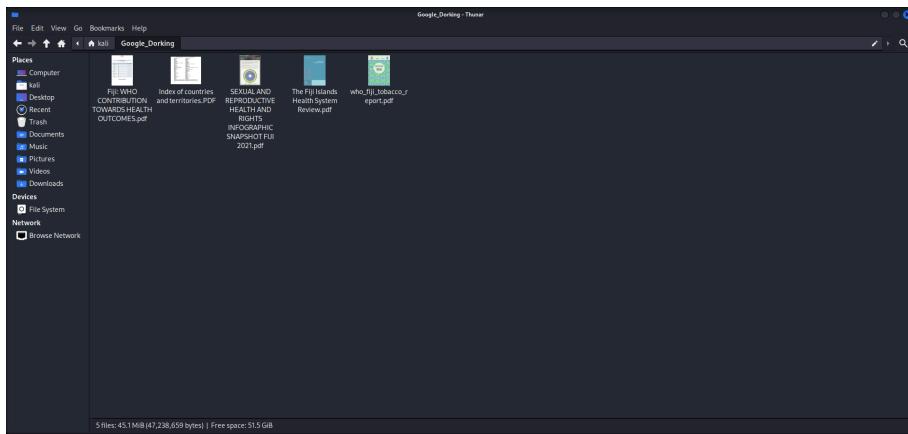


2.5 Google Dorking

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

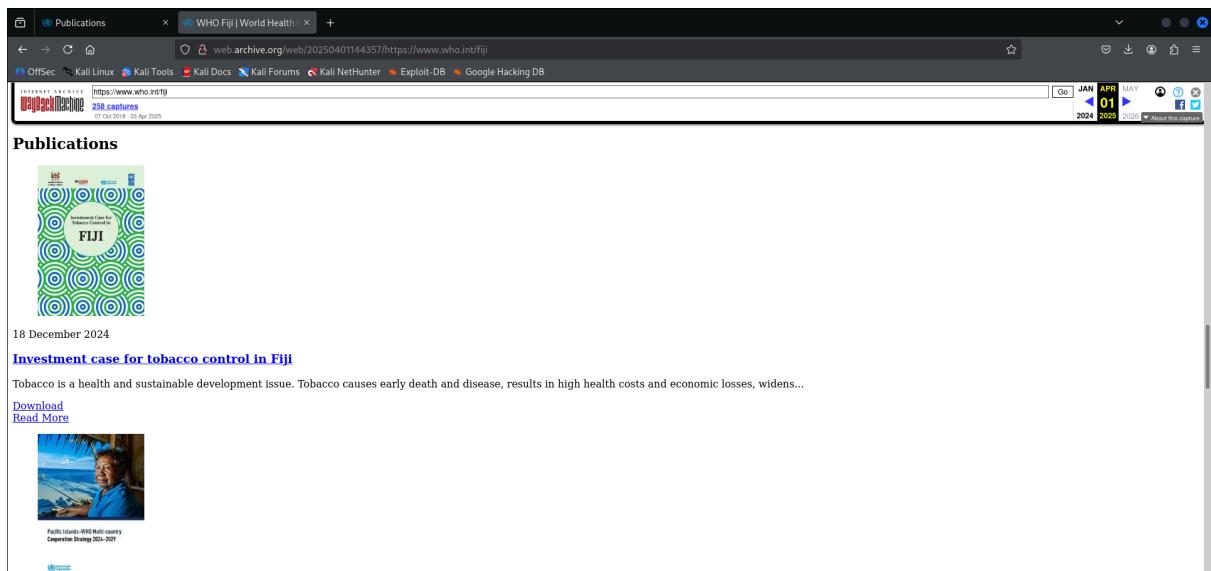
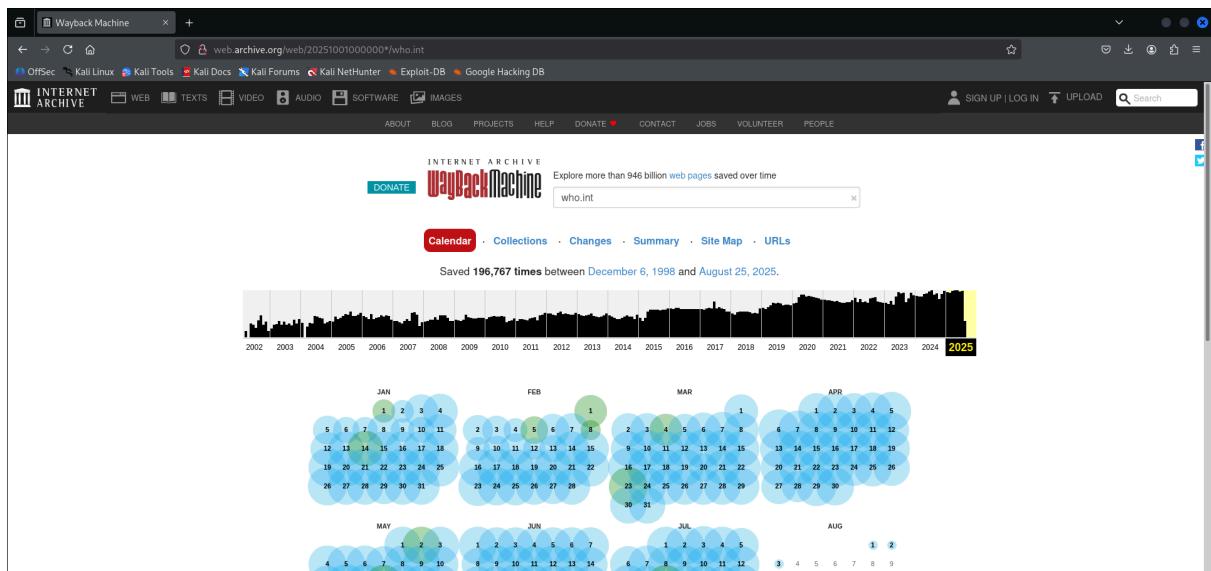
Tool: <https://archive.org/web/>

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.



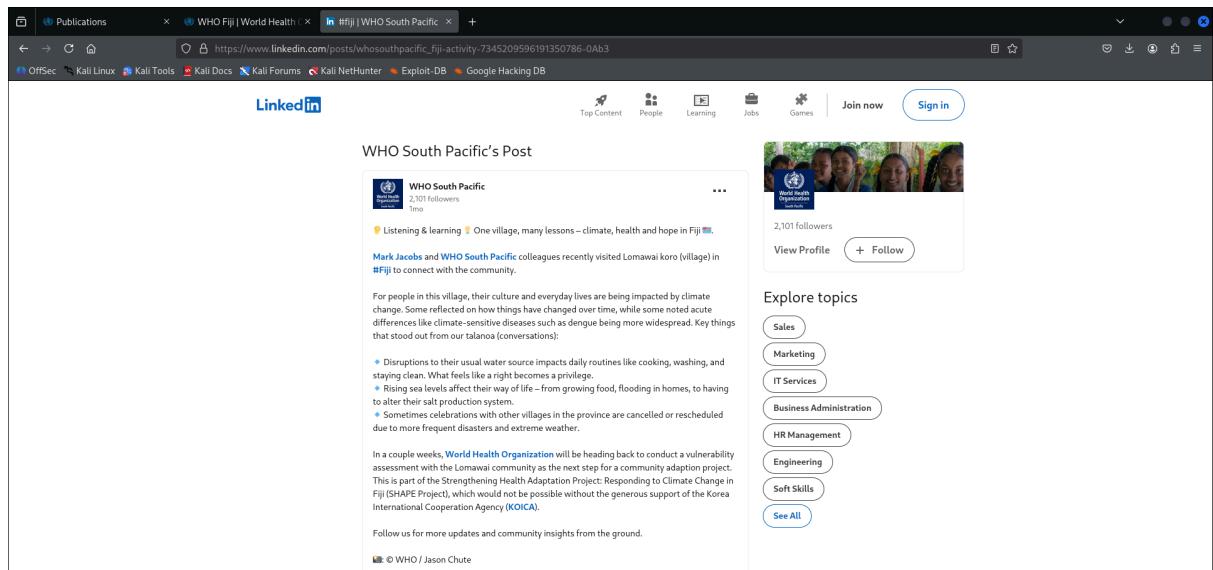
2.7 Social Media

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



The screenshot shows a LinkedIn post from the WHO South Pacific page. The post is titled "WHO South Pacific's Post" and features a profile picture of the WHO South Pacific team. It has 2,101 followers. The post content discusses a visit to Lomawai koro in Fiji, mentioning climate change impacts such as flooding and salt production issues. It also mentions the SHAPE Project and the support of KOICA. The post includes a photo of several people and ends with a note to follow for more updates.

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.