

Digital Security Field Manual (DSFM)

Christopher Quinn



Published by Purple Team Security

ISBN: 979-8-9988306-5-5

10 9 8 7 6 5 4 3 2

Digital Security Field Manual (DSFM)
Copyright © 2025 by Purple Team Security
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means electronic, mechanical, photocopying, recording, or otherwise without prior written permission of the publisher, except for brief quotations used in reviews or scholarly works as permitted by law.

ISBN: 979-8-9988306-5-5

Second Edition
Published by Purple Team Security
Printed in the United States of America

10 9 8 7 6 5 4 3 2

LEGAL DISCLAIMER

This manual, this arsenal of defense, this blueprint for personal sovereignty is a work of education, not sedition. It does not deputize you as a digital Robin Hood, nor does it grant you license to dance gleefully on the wrong side of the law. If you've come here looking for a hall pass to commit crimes, let me assure you: you are wrong.

What you now hold or perhaps, what now glares at you in digital form is not a weapon. It is not a blueprint for criminal conquest. It is, rather, a compendium of defensive knowledge, a tactical field guide for those wishing to survive the predatory chaos of the digital world.

By continuing beyond this page, you accept that you are solely accountable for your actions, choices, and consequences. The author, publisher, and anyone remotely involved disclaim all liability for your inevitable rendezvous with law enforcement should you ignore this warning.

This book is for defense, not destruction. For protection, not exploitation. It is for those who walk the line between freedom and surveillance, privacy and exposure, right and ruin.

By proceeding, you acknowledge that you are of sound mind, or at the very least, that you can convincingly fake it in a court of law. You accept that this is a toolbox, not a ticket. A lesson, not a loophole. What you build with it is entirely, irrevocably, and may the odds be ever in your favor your burden alone.

Table of Contents

1	The Story Behind This Manual	15
2	About the Digital Security Field Manual	17
3	Introduction to Digital Security	19
4	OSINT & Threat Intelligence	24
4.1	Understanding OSINT and Its Dangers	24
4.2	How Attackers Gather Information (OSINT Techniques)	25
4.3	Defensive OSINT: Reducing Your Digital Exposure .	27
4.4	Countering AI-Powered OSINT Tracking	28
4.5	Final Thoughts: The Future of OSINT & Privacy Defense	28
5	Building an Ultra-Secure Smartphone	30
5.1	Your Mission:	30
5.2	Choosing the Right Phone	31
5.3	Installing GrapheneOS	31
5.4	Other OS Options (When GrapheneOS Isn't an Option)	33
5.5	Post-Installation Hardening	33
5.6	Privacy-Respecting Apps You Should Consider . . .	34

5.7 Long-Term OPSEC Practices	34
6 Hardware Security	35
6.1 BIOS & Firmware Backdoors	35
6.2 The TPM Dilemma: Trusted, But Dangerous	36
6.3 Advanced Firmware Attestation and Tamper Detection	37
6.4 Supply Chain Verification: Trust No Box	39
6.5 Chipset Isolation: Outsmarting Silicon Spies	41
6.6 External Hardware Security Modules (HSMs)	43
6.7 RF Isolation and Electromagnetic Threats	45
6.8 Anti-Interdiction & Tamper-Proofing Techniques	47
7 Building an Air-Gapped System	50
7.1 Going Beyond Isolation: Real-World Air-Gap Threats	55
7.2 Building a Real-World Air-Gapped Workstation	58
7.3 Closing Thoughts on Hardware Security	61
7.4 Final Reality Check: Is Air-Gapping Right for You?	61
8 Secure Web Browsing & Anonymous Internet Use	63
8.1 Why Browsers Are Built to Betray You	63
8.2 Choosing a Browser That Works For You (Not Against You)	64
8.3 Psychological Manipulation: Defeating Dark Patterns	64
8.4 Why Fingerprinting Matters More Than Cookies	68
8.5 Silencing Trackers and Ad Networks	69
8.6 Mobile Browsing: Your Pocket Is Leaking Too	70
8.7 DNS Leaks: Your ISP's Favorite Snack	71
8.8 Operational Discipline: The Human Firewall	72

9	Secure File Storage & Encryption	76
9.1	Choosing the Right Encryption Strategy for the Right Data	76
9.2	Defending Against Coercion: Hidden Volumes	77
9.3	RAM Data Exposure & Cold Boot Attacks	78
9.4	The Metadata Problem: What Encryption Doesn't Hide	78
9.5	Secure Deletion: Shredding Unencrypted Data . . .	79
9.6	Secure Memory Erasure	79
9.7	The Truth About "Hardware Encrypted" USB Drives .	80
9.8	Cloud Disk Snapshot Exploits	85
9.9	The Real Takeaway	86
10	Hardware Attacks & Physical Threats	87
10.0.1	USB-Based Attacks	87
10.0.2	Keyloggers & Hardware Spy Devices	89
10.0.3	Evil Maid Attacks & BIOS/UEFI Exploits . .	90
10.0.4	Malicious Peripherals: HID Spoofing & Firmware Attacks	91
10.0.5	Side-Channel & Supply Chain Attacks	92
10.0.6	Final Hardware Security Recommendations . .	92
11	Secure Communication	94
11.0.1	Threats to Private Communication	94
11.0.2	Choosing a Secure Messaging App	95
11.0.3	Using PGP for Secure Email Encryption . . .	96
11.1	Out-of-Band Key Verification	97
11.1.1	Self-Hosting Private Email Servers	97
11.1.2	Decentralized Social Media and Communication	98
11.1.3	Secure Multi-Party Communication Protocols	98

11.2 The Endpoint Problem: Device Compromise Risks . .	99
11.2.1 Traffic Analysis Resistance in Voice and Video Communication	99
11.2.2 Final Security Recommendations for Private Communication	100
12 Physical Security & Anti-Forensics	101
12.0.1 Physical Security Threats	102
12.0.2 Decentralized Identity (DID) & Verifiable Credentials	102
12.0.3 Securing Your Devices Against Physical At- tacks	102
12.0.4 Detecting Network Taps and Implants	105
12.0.5 Secure Data Destruction	107
12.0.6 Forensic Anti-Analysis Techniques	108
12.0.7 Final Physical Security Recommendations . .	108
13 Advanced Anti-Forensics & Secure Data Destruction	110
13.1 Why Advanced Anti-Forensics Matters	110
13.2 Secure Deletion: Erasing vs. Destroying	111
13.3 Forensic Evasion Tradecraft	112
13.4 Deniable Encryption & Steganography	113
13.5 Air-Gapped Storage and Dead Drops	114
13.6 Advanced Data Safeguards the Feds Hate	114
13.7 Final Operational Reality Check	114
14 Hardened Operating Systems (Linux)	115
14.0.1 Best Linux Distributions for Security . . .	115
14.0.2 Application Sandboxing: Firejail, Bub- blewrap, Flatpak	116

14.0.3	Hardening Linux for Security and Privacy	116
14.1	Hardening Linux: From Hobbyist to Hardened Operator	118
14.1.1	Full Disk Encryption with LUKS	118
14.2	Why This Matters More Than Ever	119
15	Windows Hardening	120
15.1	Windows Hardening	120
15.1.1	Disable Microsoft Telemetry and Tracking	120
15.1.2	Firewall and Network Hardening	122
15.1.3	Application and Software Security	122
15.1.4	Secure Web Browsing and Communication	123
15.1.5	Enable Exploit Protection	123
15.1.6	Enable Credential Guard & LSA Protection	123
15.1.7	Disable Legacy SMBv1 Protocol	124
15.1.8	Block LSASS Memory Credential Dumping	124
15.1.9	Lock Down App Execution with WDAC	125
15.1.10	Tighten SmartScreen or Disable Script Hosts	125
15.1.11	Harden Microsoft Defender	125
16	iOS Hardening	126
16.1	Disable Apple Telemetry and Tracking	126
16.2	Hardening Safari and Web Browsing	126
16.3	Locking Down iCloud and Apple Services	127
16.4	iPhone Security and Network Protection	127
16.5	Jailbreaking: Security Risks vs. Privacy Benefits	128
16.5.1	Risks of Jailbreaking	128
16.5.2	Safe Jailbreak Hardening (For Advanced Users)	128
16.6	Detecting AirTags and Bluetooth Trackers	129

16.6.1	How AirTag Stalking Works	129
16.6.2	How to Detect AirTags and Bluetooth Trackers	129
16.7	Covert Privacy Techniques for High-Risk Users . .	129
17	Automated Hardening Scripts	131
17.0.1	Linux Security Automation Script	131
17.0.2	Advanced SSH Security Script	132
17.0.3	Network Hardening Script	132
17.0.4	Final Hardening Recommendations	133
18	Self-Hosting & Private Cloud Storage	134
18.0.1	Best Private Cloud Storage Options	134
18.0.2	Choosing the Best Cloud Alternative	135
18.0.3	Setting Up a Private Nextcloud Server	135
18.0.4	Encrypted File Syncing with Syncthing	136
18.0.5	Advanced Self-Hosting Security Measures	137
18.0.6	Self-Hosting a Password Manager (Vaultwarden)	138
18.0.7	Final Recommendations	138
19	Self-Hosting Privacy Tools	139
19.0.1	Private Cloud Storage with Nextcloud	139
19.0.2	Self-Hosting a Private VPN	140
19.0.3	Running a Matrix Server for Secure Chat	141
19.0.4	Dead Drop Networks for Secure Data Exchange	141
19.0.5	Self-Hosting a Privacy-Focused Search Engine (SearXNG)	142
19.0.6	Setting Up a Private Email Server (Mail-in-a-Box)	142
19.0.7	Self-Hosting a Tor Hidden Service	142

19.0.8	Anonymous Hosting with Tor Hidden Services .	143
19.0.9	Choosing the Best Self-Hosting Setup . . .	144
19.0.10	Secure Remote Access with Tailscale (Zero Trust VPN)	144
19.0.11	Final Recommendations: Harden Your Self-Hosted Services	145
20	OPSEC for High-Risk Individuals	146
20.0.1	Maintaining Anonymity While Traveling . . .	146
20.0.2	Avoiding Digital & Physical Surveillance . .	148
20.0.3	Using Disposable Identities & Burner Accounts	149
20.0.4	Secure Financial Transactions for High-Risk Individuals	149
20.0.5	Digital Footprint Reduction Strategies . .	150
20.0.6	Final OPSEC Considerations for High-Risk Individuals	150
21	Case Study: Ross Ulbricht OPSEC Failures	152
21.0.1	What He Did Right	152
21.0.2	How His OPSEC Mistakes Got Him Caught . . .	153
21.0.3	How Law Enforcement Exploited His OPSEC Failures	155
21.0.4	Key OPSEC Lessons from Ross Ulbricht . . .	156
22	Defending Against Nation-State Surveillance	157
22.0.1	Avoiding IMSI Catchers & Stingray Devices .	157
22.0.2	AI-Assisted Surveillance & Metadata Exploitation	158
22.0.3	Defending Against Advanced Spyware (Pegasus, FinSpy, etc.)	159

22.0.4	Countering Supply Chain and Hardware-Level Surveillance	160
22.0.5	Secure Offline Communications	161
22.0.6	Avoiding Facial Recognition & Biometric Tracking	161
23	Vehicle & GPS Tracking Evasion	164
23.1	Understanding Modern Vehicle Tracking Threats . .	164
23.1.1	Common Tracking Technologies	164
23.2	Detecting and Removing Tracking Devices	165
23.2.1	How to Sweep for Trackers	165
23.2.2	Detecting Passive Loggers	165
23.3	Disrupting Digital Vehicle Telemetry	166
23.4	Counter-Surveillance Driving Techniques	166
23.4.1	Tactical Driving Methods	166
23.4.2	Environmental Awareness	167
23.5	Defeating AI-Based Vehicle Recognition	167
23.5.1	Vehicle Signature Obfuscation	167
23.5.2	Acoustic Signature Masking	167
23.6	Advanced Defensive Measures	167
23.7	Advanced Counter-Tracking Enhancements	168
24	AI-Based Cyber Threats	170
24.1	Deepfake Attacks: AI-Powered Social Engineering .	170
24.2	AI-Assisted Surveillance & Tracking	172
24.3	AI-Powered Physical Security Breaches	173
24.4	AI-Augmented Supply Chain Attacks	174
24.5	AI-Assisted Social Engineering at Scale	176
24.6	AI-Powered Hacking & Autonomous Exploits	177

24.7 Polymorphic Malware and Autonomous Exploitation .	178
24.8 Code Signing Abuse to Evade Detection	179
24.9 Adversarial AI Attacks: Hacking AI Itself	180
25 Facial Recognition & Gait Analysis Evasion	182
25.0.1 Understanding Facial Recognition Threats .	182
25.0.2 Techniques for Evasion	182
25.0.3 Gait Recognition & Motion Analysis	183
25.0.4 Evasion Through Environmental Exploitation	183
25.0.5 Active Anti-Surveillance Wearables	184
25.0.6 Adversarial Object Carrying	184
25.0.7 Psychological Warfare: Poisoning the Dataset Before They Find You	184
25.0.8 Environmental and Optical Disruption Tactics	185
25.0.9 Behavioral Misdirection & Social Engineer- ing Evasion	185
26 Cryptocurrency Privacy & Financial Anonymity	187
26.1 Bitcoin Privacy: Avoiding Blockchain Analysis . .	187
26.2 Privacy Coins vs. Bitcoin Mixers: Which is Safer?	189
26.3 Avoiding Common Mistakes in Crypto Privacy	190
26.4 Advanced Financial Privacy Techniques	190
26.5 Avoiding Blockchain Dust & Metadata Leaks	192
26.6 Legal and Regulatory Caution	193
27 OSINT Awareness & Digital Footprint Reduction	194
27.1 How Attackers Gather Information (OSINT Techniques)	194
27.2 Removing Personal Data from the Internet	196
27.3 Preventing Cross-Platform Stylometric Profiling .	198

27.4 Controlling Search Engine Caching and Archives . .	199
27.5 Using Honeytokens to Detect OSINT Abuse	199
27.6 Monitoring Leaks With Dark Web Search Tools . . .	200
27.7 Social Graph Poisoning to Break Profiling Engines	201
27.8 Preventing Device Fingerprinting	203
27.9 Building an Anonymous Online Presence	204
28 Final OPSEC Measures	205
28.1 Protecting Against Nation-State Attacks	205
28.2 Advanced Attack Techniques and Countermeasures . .	206
28.3 Physical Security for Devices	206
28.4 Mitigating Insider Threats and Betrayal Vectors .	207
28.5 Securing the Hardware Supply Chain	208
28.6 Countering Behavioral Exploitation	208
28.7 Secure Computing Environments	211
28.8 Anonymity Workflow for High-Security Operations .	212
29 OPSEC Checklist	214
30 Additional Resources	217
30.0.1 Privacy-Focused Operating Systems	217
30.0.2 Recommended Books on OPSEC and Digital Privacy	218
30.0.3 Cryptocurrency Privacy Tools	218
31 Privacy Security Checklists	220
31.1 General Privacy User Checklist	220
31.2 Journalist / Activist in a Hostile Country	221
31.3 Whistleblower / Leaker Checklist	222
31.4 Ex (Stalking/Abuse Prevention)	222

31.5 High-Profile / Politician Privacy Checklist . . .	223
31.6 Cryptocurrency & Financial Privacy Checklist . . .	224

1.

The Story Behind This Manual

Every book starts somewhere. Some begin as research papers; others, as corporate whitepapers dressed up to look like something they're not. This one? It started as something far simpler: a checklist.

It was February 2025. I was preparing for a trip to Europe over spring break nothing unusual, just a visit to Germany to watch my two favorite soccer clubs, Schalke 04 and 1. FC Nürnberg, take the pitch. But I wasn't about to leave my operational mindset at home. As an InfoSec professional, I knew bringing my laptop was the smart move. I understood the threat landscape here in the U.S., but I assumed Europe was similar. And as we all know, "assuming" isn't how you stay secure.

So, I started writing a list.

Privacy screen? Check.

Software firewall? Installed and configured.

Unnecessary services? Disabled.

LUKS full-disk encryption? Verified.

Nuke password for LUKS? Tested. Metaphorically, just verified setup, for obvious reasons.

USB kill switch rigged to shut down my machine if snatched in a café? Ready to go.

Somewhere between line item thirty and forty, I paused and said aloud half-joking, half-frustrated:

“Why isn’t there a field manual for this?”

And that was it. The spark. The Digital Security Field Manual was born not as a book deal, not as a thought leadership stunt but as a tool I wished already existed. Something real. Something usable. Something you could actually apply the moment you closed the page.

The first draft was done in five hours. It wasn’t pretty. It wasn’t polished. But it worked. What you’re holding now is the refined second edition built from that original skeleton, expanded with everything I’ve learned since, and shaped by the realities faced not just by cybersecurity professionals, but by everyday people, journalists, activists, executives, and privacy-conscious individuals worldwide. You should be able to surf the web and not feel like a victim afterward. You should be able to do your job without worrying about being compromised. This book, while a great start, will help you get there. However, this is only the first step.

This isn’t theory. It’s practice. It’s what I do, and it’s what I hope this book helps you do.

Stay safe. Stay sharp. Stay sovereign.

2.

About the Digital Security Field Manual

There was a time when privacy meant four walls and a locked door. Today, those walls are glass, the lock is an illusion, and someone's watching through the peephole with a high-powered telescope... or worse, a data broker's API.

Your personal data is under siege.

Governments spy in the name of national security. Corporations harvest your clicks, keystrokes, and even your silences all in the name of "personalized experiences." Meanwhile, cybercriminals lurk in the shadows, sipping stale coffee while auctioning off your stolen data on forums you'll never visit.

Make no mistake: your life, your habits, your digital soul they are commodities. Bought, sold, and weaponized. Not in some far-flung dystopian future, but here. Now. While you read these very words.

This manual this humble little field guide is your countermeasure. Not a silver bullet, but a loaded magazine.

Inside, you'll find tactics designed to:

- De-Google your smartphone, stripping it of corporate surveillance tentacles.

- Build air-gapped systems so isolated, even nation-states would blush.
- Deploy military-grade encryption because, frankly, “good enough” is not.
- Communicate like a ghost in the machine present, but untraceable.
- Fortify your operating systems until even forensic analysts question their career choices.

You see, the internet is not a highway; it’s a warzone. And in this war, information is the prize. Your information.

While the security world overflows with shiny tools and whispered techniques, this manual focuses on what works tried, tested, and, most importantly, used by me. That said, don’t treat these pages as gospel. Treat them as your opening statement. Research, adapt, evolve. The arms race never ends.

Your Privacy Matters

Privacy is not a privilege it’s your birthright. Every move you make to lock down your digital life is a blow against profiling, exploitation, and control.

You are the guardian of your privacy the first, the last, the only.

Threat actors, governments, corporations they never sleep. Their tactics evolve daily. So, I ask you:

Will you be the product?

Or will you be the problem?

Let’s begin.

3.

Introduction to Digital Security

Ah, the digital age. A marvel of convenience, a miracle of connection, and, dare I say, a masterclass in manipulation. Every click, every swipe, every whispered search in the dead of night you're not alone. You're never alone.

Governments, corporations, cybercriminals they all sit at the same table, feasting on data. Your data. Your habits, your movements, your weaknesses. Tracked, logged, sold, and served back to you with a smile.

It doesn't matter if you're a cautious citizen, a whistleblower on the run, or someone who just doesn't like the idea of a faceless algorithm knowing when you sleep, when you wake, and when you order pizza at 2 AM.

If you're reading this, you've already taken the first step. Welcome.

This guide is your roadmap to digital resistance. You'll learn how to:

- Break free from the clutches of corporate surveillance with a de-Googled smartphone.

- Build a computer so isolated it could make a submarine blush.
- Encrypt your data until even quantum computers throw their hands up.
- Vanish into the digital ether with anonymous communications.
- Fortify your systems against even the most curious forensic analyst.

Surveillance is not a conspiracy it's an industry. And business, my friend, is booming.

Understanding Digital Security

Digital security, at its core, is an elegant cocktail of technology, behavior, and common sense. Three pillars hold it together:

- **Technical Security** Encryption, hardened systems, and hardware that doesn't rat you out.
- **Operational Security (OPSEC)** Your behavior. Your habits. Your discipline. The art of not being an easy mark.
- **Physical Security** Because what good is a fortress if someone can just walk in through the front door?

Every action you take leaves a trace. This manual? It teaches you how to clean up after yourself.

Threat Modeling: Who Are You Protecting Against?

Let's not get ahead of ourselves. You can't defend what you haven't defined.

Take a moment. Ask yourself:

- Who's coming for you? Hackers? Corporations? Governments? A jealous ex?
- What's at stake? Your identity? Your finances? Your reputation? Your freedom?
- What's the most likely attack? Phishing? Malware? Physical surveillance? Social engineering?

Depending on your answers, your defense strategy changes.

- Casual Privacy Seekers: Block trackers, use encrypted apps, limit what you share.
- Professionals & Activists: Harden your devices, compartmentalize identities, expect targeted attacks.
- High-Risk Operators: Go offline. Air-gap. Operate like your life depends on it because it might.

Common Digital Security Threats

Know your enemy. Here's the shortlist:

- Mass Surveillance: Metadata is the new gold. You are the mine.
- Device Exploits: Every unpatched vulnerability is an open door.
- Social Engineering: The easiest system to hack is the one between your ears.
- Metadata Collection: Encrypted or not, your patterns betray you.
- Compromised Networks: Free Wi-Fi? Free surveillance.

- Supply Chain Attacks: Sometimes, the trojan horse arrives shrink-wrapped and factory-sealed.

These threats aren't hypothetical they're operational.

Best Practices for Digital Security

Let's cut the fluff. Here's what works:

1. Reduce Your Attack Surface

- Run minimalist operating systems (GrapheneOS, Qubes OS, Tails).
- Uninstall what you don't need. Bloatware is surveillance by another name.
- Avoid cloud services without end-to-end encryption. No exceptions.

2. Encrypt Everything

- Full-disk encryption on every device. No excuses.
- Use Signal, Briar, or Session for messaging. If it's not end-to-end encrypted, it's public.
- Lock down your sensitive files with VeraCrypt or GPG.

3. Strengthen Your OPSEC

- Never reuse passwords. Ever. Use Bitwarden or KeePassXC.
- Burn your email addresses like a spy burns an identity.
- Social media is a buffet for attackers. Serve them nothing.

4. Use Anonymity Tools

- Tor Browser. Mullvad Browser. Become nobody.
- Route your traffic through VPNs or Tor Bridges.
- Ditch biometric unlocks. Your face and fingerprints belong to you not your phone.

What This Guide Covers

This manual is not a bedtime story. It's a blueprint for rebellion.

1. Ultra-Secure Smartphones: De-Google, harden, and control your communications.
2. Air-Gapped Systems: Build computers that know nothing of networks.
3. Encryption Mastery: Lock down your data, your emails, your life.
4. Anonymous Internet Use: Move through the digital world like a shadow.
5. Operational Security: Practice behaviors that leave attackers grasping at air.

By the end, you'll be armed with more than tools. You'll have a mindset.

Because privacy isn't just something you install. It's something you become.

4.

OSINT & Threat Intelligence

4.1 Understanding OSINT and Its Dangers

They say knowledge is power. Allow me to correct that.

Knowledge about you is power.

And every click, post, photo, or careless share contributes to a dossier you never agreed to build.

Open-Source Intelligence, or OSINT if you're feeling punchy, is the art of profiling people using nothing but what they themselves and their technologies carelessly leave behind. No hacking. No backdoors. Just breadcrumbs. Millions of them.

It's used by security professionals. Law enforcement. Corporate spies. Political operatives. Hackers in dark basements with nothing better to do. And yes, that kid you blocked on social media last week.

How OSINT Is Used Against You:

- **Doxxing** Your home, your phone number, your email packaged and posted for the world to see.
- **Social Engineering** Attackers don't need to guess your mother's maiden name when you posted it on Facebook in

2011.

- Targeted Cyber Attacks The more they know, the more precise their attacks become.
- Corporate Espionage Think LinkedIn is boring? It's a goldmine for your competitors.

With nothing but public data, an adversary can map your life your habits, your routines, your soft spots.

4.2 How Attackers Gather Information (OSINT Techniques)

OSINT isn't magic. It's methodical. It comes in two flavors:

- Passive Reconnaissance The art of watching silently.
- Active Reconnaissance The art of poking until something falls over.

1. Social Media Intelligence (SOCMINT):

- Username Tracking Your clever handle? You've reused it everywhere.
- Geotag Analysis Your photos tell them where you've been. Your timestamps tell them when.
- Hashtag Monitoring You thought that meme was funny. They thought it connected you to twenty others just like you.
- Metadata Extraction That picture you posted? It didn't just capture your smile. It captured your phone model, GPS coordinates, and the time you took it.

2. Domain & Infrastructure Reconnaissance: