



GHOST
PROTOCOL

LD

THE FIELD LIBRARY

GROUND RULES

WHAT THE WORK MUST OBEY

The Law, Deeper

The law that governs the work,
authorisation as a legal instrument, data
protection, evidence and privilege, and
finding a crime. Informational, not legal
advice.



Ghost Protocol (Pvt) Ltd · Colombo · ghosts.lk

Security internship training · The Field Library · Edition 1 · 2026

THE GHOST PROTOCOL FIELD LIBRARY · GROUND RULES

The Law, Deeper

The law that governs the work, authorisation as a legal instrument, data protection, evidence and privilege, and finding a crime. Informational, not legal advice.

Ghost Protocol (Pvt) Ltd · Colombo

The Field Library, Edition 1 · 2026

Copyright 2026 Ghost Protocol (Private) Limited. All rights reserved.

Sold as a PDF for the buyer's own reading. Please do not share or resell the file.

The library

The Field Library is a whole shelf, not one book. The Core Path is the spine everyone reads. The rest is depth and breadth, taken on as the work calls for it. The shelf is complete now, and you are reading the one marked here.

A · THE CORE PATH

O The Oath BUILT

I Groundwork BUILT

II The Web BUILT

III The Wider Field BUILT

IV The Work BUILT

V The Craft BUILT

B · DEEP TRACKS

AI and Agents BUILT

Reading Code BUILT

Internal and Active Directory BUILT

The Web, Deeper BUILT

Cloud and Containers BUILT

Mobile and APIs BUILT

Reverse Engineering BUILT

Hardware and the Edges BUILT

C · THE OPERATIONS

Red and Purple Team BUILT

OSINT and Recon BUILT

Report Writing Mastery BUILT

The Consulting Craft BUILT

Bug Bounty BUILT

D · THE OTHER SIDE

Detection and Response BUILT

Threat Hunting and Forensics BUILT

Hardening and Architecture BUILT

E · THE GROUND RULES

The Law, Deeper YOU ARE HERE

Standards and Compliance BUILT

Ethics and Disclosure BUILT

F · COMPANIONS

The Reference Pack BUILT

The Lab Workbook BUILT

Case Files BUILT

The Bestiary BUILT

The Glossary and the Ledger BUILT

Contents

- Opening 5
- 1** The Law That Governs the Work 6
- 2** Authorisation as a Legal Instrument 11
- 3** Data Protection 16
- 4** Evidence, Disclosure and Privilege 19
- 5** Finding a Crime, and Disclosure 23
- Worked answers 28
- Sources and currency 30

The line has a statute



Blink had always treated the line as a feeling, a thing good people simply did not cross. Tonight a scope arrived with a signed authorisation stapled to it, and Blink finally asked why that one page carried so much weight.

BLINK "It is just a formality. We already know not to do harm."

SOL "It is not a formality, and the line is not only a feeling. It is written in law. Reaching into a system you were not permitted to reach is a crime with a statute and a number behind it, and that signed page is the exact thing that puts your work on the right side of it. A ghost who does not know where the line is written is one signature away from being the person answering for it."

Worm's eye was on the signature, on the date beside it and the scope above it.

WYRM "the paper is the law."

So the book is the ground the work stands on. It is informational, not legal advice, but every ghost needs it: the statutes that govern the work, what an authorisation really is, how to handle data and evidence, and what to do when a test turns up a genuine crime.

CHAPTER ONE

The Law That Governs the Work

Volume 0 gave you the one rule and the one offence. This chapter opens the statute and reads it properly, so you can see for yourself why the rule is not just house policy, and so you recognise the same shape in the law of any client's country.

You do not need to be a lawyer to do this work, but you do need to be able to read the one law that touches what you do every day and not flinch at it. Volume 0, The Oath, taught the rule: you test only what you are authorised, in writing, to test. This volume is that rule taken down to the statute it comes from. We read the Sri Lankan law first, because Ghost Protocol is a Sri Lankan company and the ground under the work is Sri Lankan, and then we look at the three other systems you will meet when a client is abroad. The point is not to turn you into counsel. It is to make the paperwork stop feeling like a formality and start reading as the thing standing between a day's work and a criminal charge.

■ HOW TO READ THIS VOLUME

This is Ghost Protocol's working understanding of the law, written so a tester can operate cleanly. It is informational and for training. It is not legal advice, it creates no lawyer-client relationship, and it is not a substitute for a licensed attorney in the relevant country. Statutes are amended, and a date, a section number, or a figure can move after this edition is set. Every citation here was checked against a primary or authoritative source while it was being written, and the few points left open are gathered in one note, Sources and currency, at the back of this volume. Even so, a real question about what the law permits goes to Ryan and to counsel, before the action, never resolved by you at the keyboard.

Sri Lanka: the Computer Crime Act, No. 24 of 2007

Sri Lanka's **Computer Crime Act, No. 24 of 2007** is the statute that matters most to a tester. Its long title says it plainly: an Act to provide for the identification of computer crime, and the procedure for investigating and preventing it. The offences sit in a short ladder near the front, and the first rung is the one to carry in your bones.

Section 3, securing unauthorised access. Any person who intentionally does any act in order to secure, for themselves or anyone else, access to a computer or to any information held in a computer, knowing or having reason to believe they have no lawful authority to do so, is guilty of an offence. On conviction it carries a fine of up to one hundred thousand rupees, or imprisonment for a term up to five years, or both. Read what is not in that sentence. You do not have to take anything, change anything, or cause any harm. The act of securing the access, knowing you were not allowed, is the whole offence. "I only looked" is a description of the crime, not a defence to it.



already an offence.

There is no quiet version of unauthorised access that the law lets through. The looking is the thing it names. Say it back to yourself before any "quick check" on a host no one signed for.

Section 4, access to commit a further offence. The same unauthorised access, done with the intention of committing an offence under the Act or under any other law, is treated more gravely: a fine of up to two hundred thousand rupees, or up to five years, or both. The ladder is deliberate. The law is harder on access that is a step towards something worse.

Section 5, causing a computer to perform a function. Intentionally and without lawful authority causing a computer to perform any function, knowing or having reason to believe the function will cause unauthorised modification, damage, or potential damage to a computer, system, or programme, is an offence carrying a fine of up to three hundred thousand rupees, or up to five years, or both. This is the provision that reaches the active, changing side of testing, not just the reading of data.

Section 6, offences against national security. Causing a computer to perform a function knowing it will cause danger, or imminent danger, to national security, the national economy, or public order, carries imprisonment for a term up to five years. The figure to hold here is the custodial one: this section states a prison term, not a fine.

What "unauthorised access" and "interception" actually mean

Two ideas in the Act are worth separating, because beginners blur them. **Unauthorised access** is reaching a computer or its stored information without lawful authority. It is about getting in, or getting at data at rest, and sections 3 and 4 are built around it; sections 5 and 6 go further, to what you make a computer do. **Interception** is different: it is capturing data while it is moving, in transit between machines or across a network, or capturing the electromagnetic emissions of a system. The Act carries its own provisions on this. Section 8 makes illegal interception of data an offence. Section 9 makes it an offence to produce, sell, procure for use, distribute or otherwise make available a device, a program, or a password or access code, without lawful authority and with the intent that it be used to commit an offence under the Act. Section 7 reaches anyone who buys, receives, retains, sells, copies or otherwise deals with information they know, or have reason to believe, someone else obtained from a computer without lawful authority. Each carries a fine of not less than one hundred thousand and not more than three hundred thousand rupees, or imprisonment for not less than six months and not more than three years, or both. What you carry is the shape: capturing live traffic you were not authorised to capture, and supplying or procuring tools or passwords meant for an offence, are their own offences on top of access itself.

The Act Follows you across the border

Section 2 is the part testers forget, and it is the one that catches them. It sets out when the Act applies, and the reach is wide. In its own words, the Act applies where a person commits an offence under it "while being present in Sri Lanka or outside Sri Lanka", where the computer or information affected "was at the material time in Sri Lanka or outside Sri Lanka", where the facility or service used

was situated in or outside Sri Lanka, or where the loss or damage is caused within or outside Sri Lanka to the State or to a person resident in or outside Sri Lanka. In plain terms: testing a foreign system from a desk in Colombo can engage this Act, and so can testing a Sri Lankan system from abroad. Geography is not a loophole. The authorisation is.

The same shape, in three other systems

When a client is abroad, their own country's computer-crime law applies to their systems, and most countries, including the three here, treat it the same way: access without authority is the offence, and intent to help is not a defence. A few countries have narrow, conditional good-faith regimes for people who find and report flaws; Ghost Protocol never relies on them. Keep this at an awareness level. Do not advise a foreign client on their own law; flag it to Ryan and to counsel there. But recognise the family.

United Kingdom. The **Computer Misuse Act 1990** sets out, in section 1, "Unauthorised access to computer material"; in section 2, "Unauthorised access with intent to commit or facilitate commission of further offences"; and in section 3, "Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.". The ladder is the same as Sri Lanka's: bare access, access with worse intent, and acts that damage.

United States. The **Computer Fraud and Abuse Act**, codified at 18 U.S.C. section 1030 and titled "Fraud and related activity in connection with computers", turns on accessing a computer "without authorization" or in a way that "exceeds authorized access". That second phrase was read narrowly by the Supreme Court in **Van Buren v. United States**, 593 U.S. 374 (2021): a person exceeds authorised access when they reach areas of a computer that are off-limits to them, such as files or databases they may not touch, and not merely by using access they do have for an improper purpose. The lesson for a tester is simple: "I had a login" is not the same as "I was authorised to go there".

European context. EU member states criminalise unauthorised access and interception through national law shaped by EU instruments, and the bloc also runs a separate regime for personal data, which is Chapter Three's subject, not this one. At this level, hold one fact: in the EU, as almost everywhere, probing a system without the owner's authority is an offence, and meaning well does not make it lawful outside the narrow, conditional exceptions a few countries have written, which Ghost Protocol never relies on.

Sri Lanka's Act was drafted in the era of the Council of Europe's Convention on Cybercrime, often called the Budapest Convention, which many states use as the template for this family of offences. Sri Lanka acceded to it in 2015, the accession taking effect on 1 September 2015, the first state in South Asia to join. You do not need the treaty to do the work. You need to know the domestic Act, and it is No. 24 of 2007.

**SOL SAYS**

Learn to read the one statute that governs you, and the fear drops away, because fear is mostly not knowing where the edge is. The edge is bright and close: access without authority, on its own, with no harm needed and no good heart to save you. Once you have seen that in the text, the authorisation stops being a hoop the client makes you jump through and becomes the exact thing that moves your keystrokes from section 3 to a day's honest work. The next chapter is about that document, because it is the most important legal instrument you will ever hold.

■ VERIFY IT

Do not take this chapter's section numbers or figures on its word, including for your own country if you work abroad. The primary texts are public. Open the Computer Crime Act, No. 24 of 2007 from an official Sri Lankan source, find section 3, and read the penalty with your own eyes. Then do the same for one foreign Act that would apply to a client you might one day serve. A law you have read in the primary source is one you can cite without flinching. A law you half-remember from a handbook is one that will fail you in the room where it matters.

■ THE LINE

If you are ever unsure whether an action is lawful or authorised, that uncertainty is itself the answer: you stop. A legal doubt is never resolved by proceeding to see what happens. It is resolved by asking, before the action, in writing, to Ryan and where needed to counsel. The cost of asking is a few minutes. The cost of guessing wrong is in section 3, and section 2 means the border does not save you.

■ ON YOUR FEET

A prospective client is a company registered in London, running its application on servers it rents in Germany, and you would be testing from your desk in Colombo. A teammate says, "Sri Lankan law is the only one that applies to us, we are in Sri Lanka." Based on this chapter, is that right, and which laws are actually in the picture before a single packet is sent?



WHAT WYRM KEEPS

In Sri Lanka, securing access to a computer you were not allowed into is a crime on its own, no harm required and no good-intentions defence. The Act reaches across the border. Most countries, including the three here, treat it the same way.

- Computer Crime Act, No. 24 of 2007: s.3 unauthorised access (fine up to Rs 100,000 or up to 5 years or both); s.4 access to commit a further offence (up to Rs 200,000 or 5 years or both); s.5 causing a function that modifies or damages (up to Rs 300,000 or 5 years or both); s.6 offences against national security (up to 5 years).
- Interception is a separate idea from access: it captures data in transit. The Act's sections 7, 8 and 9 (dealing with unlawfully obtained data, illegal interception, illegal devices) carry it, each a fine of Rs 100,000 to Rs 300,000, or six months to three years, or both.
- Section 2 gives the Act extraterritorial reach: offender, system, service, or loss in or outside Sri Lanka all count. Geography is not a loophole.
- Awareness abroad: UK Computer Misuse Act 1990 (ss.1 to 3); US CFAA, 18 U.S.C. 1030, narrowed on "exceeds authorized access" by *Van Buren v. United States* (2021). This is informational, not legal advice; a real question goes to Ryan and counsel.