572.5 - Encryption, Protocol Reversing, OPSEC and Intel

[Encoding, encryption & SSL 4-40](#_Toc156249929)

[Encoding 4-7](#_Toc156249930)

[Overview 4](#_Toc156249931)

[Base64 5-7](#_Toc156249932)

[Encryption 8-21](#_Toc156249933)

[Overview 8](#_Toc156249934)

[Strength 9-10](#_Toc156249935)

[Symmetric key encryption 11-13](#_Toc156249936)

[Overview 11](#_Toc156249937)

[Stream vs. block cipher modes 12-13](#_Toc156249938)

[Synchronous vs. self-synchronous 12-13](#_Toc156249939)

[Asymmetric key encryption 14-15](#_Toc156249940)

[Basic SSL/TLS process 16-17](#_Toc156249941)

[Perfect Forward Secrecy (PFS) 18](#_Toc156249942)

[Diffie-Hellman exchange 19-21](#_Toc156249943)

[SSL/TLS 22-33](#_Toc156249944)

[HTTPS 22](#_Toc156249945)

[TLS handshake details 23-30](#_Toc156249946)

[Client Hello 23](#_Toc156249947)

[JA3 fingerprint 24](#_Toc156249948)

[Server Hello 25](#_Toc156249949)

[JA3S fingerprint 26-27](#_Toc156249950)

[Certificate exchange 28-30](#_Toc156249951)

[HTTPS data transferred problem 31](#_Toc156249952)

[HTTP vs. HTTPS 32-33](#_Toc156249953)

[Analytic mitigation 34-40](#_Toc156249954)

[NetFlow & DNS correlation 34-35](#_Toc156249955)

[Certificate metadata 36](#_Toc156249956)

[Wireshark decryption 37-40](#_Toc156249957)

[Example 37-38](#_Toc156249958)

[Requirements 39](#_Toc156249959)

[PFS 40](#_Toc156249960)

[MITM 45-61](#_Toc156249961)

[Overview 45](#_Toc156249962)

[ARP Spoofing 46-47](#_Toc156249963)

[Port stealing (CAM table manipulation) 48](#_Toc156249964)

[UDP first response wins 49-51](#_Toc156249965)

[Common attack themes 52](#_Toc156249966)

[Other MITM attacks 52](#_Toc156249967)

[Open-source MITM tools 53-54](#_Toc156249968)

[Bettercap & dsniff 53](#_Toc156249969)

[Yersinia 54](#_Toc156249970)

[Investigative use 55-58](#_Toc156249971)

[Proxy, NSM, IDS/DLP 55-56](#_Toc156249972)

[Commercial solutions 57-58](#_Toc156249973)

[TLS inspection limitations 59-60](#_Toc156249974)

[Analytics on encrypted data 61](#_Toc156249975)

[Protocol Reversing 63-86](#_Toc156249976)

[Overview 63](#_Toc156249977)

[Protocol attributes 64](#_Toc156249978)

[How to approach 65](#_Toc156249979)

[Compromised websites 67-72](#_Toc156249980)

[Overview 67](#_Toc156249981)

[IPHONE8.5 example 68-72](#_Toc156249982)

[Request 68](#_Toc156249983)

[Response 69](#_Toc156249984)

[More responses 70](#_Toc156249985)

[Downloaded file 71](#_Toc156249986)

[Summary 72](#_Toc156249987)

[Common protocol backdoors 73-77](#_Toc156249988)

[Overview 73](#_Toc156249989)

[Cookie example 74-77](#_Toc156249990)

[Request 74-75](#_Toc156249991)

[Request (decoded) 76-77](#_Toc156249992)

[Mixed protocol analysis 78-81](#_Toc156249993)

[Overview 78](#_Toc156249994)

[No space example 79-81](#_Toc156249995)

[Request headers 79](#_Toc156249996)

[Request body (binary data) 80](#_Toc156249997)

[Decoded Windows shell 81](#_Toc156249998)

[Binary protocol analysis 82-86](#_Toc156249999)

[Overview 82](#_Toc156250000)

[GH0ST RAT example 83-68](#_Toc156250001)

[gh0st\_header 83](#_Toc156250002)

[Encoded message 84](#_Toc156250003)

[Decompressed payload 85](#_Toc156250004)

[Partially decoded 86](#_Toc156250005)

[OPSEC & Intel 91-111](#_Toc156250006)

[Overview 91-92](#_Toc156250007)

[Research OPSEC 93-98](#_Toc156250008)

[DNS lookup on bad domains 93](#_Toc156250009)

[OSINT 94-95](#_Toc156250010)

[IR: The attacker is watching 96](#_Toc156250011)

[IR: Premature blocking 97-98](#_Toc156250012)

[LAN Scope 99-102](#_Toc156250013)

[DHCP/DNS traffic 99-101](#_Toc156250014)

[MDNS/UPNP/Bonjour 99-101](#_Toc156250015)

[Other traffic 102](#_Toc156250016)

[Research risk mitigations 103-105](#_Toc156250017)

[Third party lookups 103](#_Toc156250018)

[VPN/TOR 103](#_Toc156250019)

[Air gapped 103-104](#_Toc156250020)

[Separate IR network 105](#_Toc156250021)

[Separate platforms 105](#_Toc156250022)

[Guarding intel from attackers 106-107](#_Toc156250023)

[Responsible sharing (ISACs & ISAOs) 106-107](#_Toc156250024)

[Traffic Light Protocol (TLP) 110](#_Toc156250025)

[Community resources 111](#_Toc156250026)

# Encoding, encryption & SSL 4-40

## Encoding 4-7

### Overview 4

### Base64 5-7

## Encryption 8-21

### Overview 8

### Strength 9-10

### Symmetric key encryption 11-13

#### Overview 11

#### Stream vs. block cipher modes 12-13

#### Synchronous vs. self-synchronous 12-13

### Asymmetric key encryption 14-15

### Basic SSL/TLS process 16-17

### Perfect Forward Secrecy (PFS) 18

### Diffie-Hellman exchange 19-21

## SSL/TLS 22-33

### HTTPS 22

### TLS handshake details 23-30

#### Client Hello 23

#### JA3 fingerprint 24

#### Server Hello 25

#### JA3S fingerprint 26-27

#### Certificate exchange 28-30

### HTTPS data transferred problem 31

### HTTP vs. HTTPS 32-33

## Analytic mitigation 34-40

### NetFlow & DNS correlation 34-35

### Certificate metadata 36

### Wireshark decryption 37-40

#### Example 37-38

#### Requirements 39

#### PFS 40

# MITM 45-61

## Overview 45

## ARP Spoofing 46-47

## Port stealing (CAM table manipulation) 48

## UDP first response wins 49-51

## Common attack themes 52

## Other MITM attacks 52

## Open-source MITM tools 53-54

### Bettercap & dsniff 53

### Yersinia 54

## Investigative use 55-58

### Proxy, NSM, IDS/DLP 55-56

### Commercial solutions 57-58

## TLS inspection limitations 59-60

## Analytics on encrypted data 61

# Protocol Reversing 63-86

## Overview 63

## Protocol attributes 64

## How to approach 65

## Compromised websites 67-

### Overview 67

### IPHONE8.5 example 68-72

#### Request 68

#### Response 69

#### More responses 70

#### Downloaded file 71

#### Summary 72

## Common protocol backdoors 73-77

### Overview 73

### Cookie example 74-77

#### Request 74-75

#### Request (decoded) 76-77

## Mixed protocol analysis 78-81

### Overview 78

### No space example 79-81

#### Request headers 79

#### Request body (binary data) 80

#### Decoded Windows shell 81

## Binary protocol analysis 82-86

### Overview 82

### GH0ST RAT example 83-68

#### gh0st\_header 83

#### Encoded message 84

#### Decompressed payload 85

#### Partially decoded 86

# OPSEC & Intel 91-111

## Overview 91-92

## Research OPSEC 93-98

### DNS lookup on bad domains 93

### OSINT 94-95

### IR: The attacker is watching 96

### IR: Premature blocking 97-98

## LAN Scope 99-102

### DHCP/DNS traffic 99-101

### MDNS/UPNP/Bonjour 99-101

### Other traffic 102

## Research risk mitigations 103-105

### Third party lookups 103

### VPN/TOR 103

### Air gapped 103-104

### Separate IR network 105

### Separate platforms 105

## Guarding intel from attackers 106-107

## Responsible sharing (ISACs & ISAOs) 106-107

## Traffic Light Protocol (TLP) 110

## Community resources 111