572.2 - Core Protocols and Log Aggregation/Analysis

[HTTP Protocol](#_Toc156238873) 4-26

[Overview](#_Toc156238874) 4-6

[History & adaptation](#_Toc156238875) 4

[Forensic value](#_Toc156238876) 5

[HTTP version history](#_Toc156238877) 6

[Request/Response dissection](#_Toc156238878) 7-26

[Requests](#_Toc156238879) 8-14

[Methods, request string, idempotent](#_Toc156238880) 9-10

[Headers example](#_Toc156238881) 11

[Headers & data](#_Toc156238882) 12-14

[User\_agent](#_Toc156238883) 14

[Cookies](#_Toc156238884) 14

[X-Forwarded-For](#_Toc156238885) 14

[Proxy-Authorization](#_Toc156238886) 14

[Referer](#_Toc156238887) 14

[Responses](#_Toc156238888) 15-26

[Response codes](#_Toc156238889) 16-17

[Header example](#_Toc156238890) 18

[Headers & data](#_Toc156238891) 19-20

[Useful fields](#_Toc156238892) 21-22

[Analytic cookies](#_Toc156238893) 23-24

[Google Analytic Cookies (UTM)](#_Toc156238894) 23-24

[HubSpot targeting cookies](#_Toc156238895) 25-26

[HTTP/2](#_Toc156238896) 27-31

[Overview](#_Toc156238897) 27

[Debug decrypting TLS](#_Toc156238898) 28

[Example](#_Toc156238899) 29

[Browser developer tools](#_Toc156238900) 30-31

[Web server logs](#_Toc156238901) 36-47

[Relevance](#_Toc156238902) 36

[Log formats](#_Toc156238903) 37-43

[Overview](#_Toc156238904) 37

[NCSA Common format](#_Toc156238905) 38

[W3C Extended/Combined format](#_Toc156238906) 39

[Apache mod\_forensic format](#_Toc156238907) 40-41

[IIS log format](#_Toc156238908) 42-43

[Default](#_Toc156238909) 42

[ODBC, CBL](#_Toc156238910) 43

[Log file analysis methods](#_Toc156238911) 44-45

[Investigative value](#_Toc156238912) 46-47

[DNS](#_Toc156238913) 49-72

[DNS Basics](#_Toc156238914) 49-51

[Forward requests](#_Toc156238915) 49-50

[Stateless Protocol](#_Toc156238916) 51

[EDNS](#_Toc156238917) 51

[Compression pointers](#_Toc156238918) 52-53

[DNS hierarchy](#_Toc156238919) 54

[Canonical Name Records (CNAME)](#_Toc156238920) 56

[Forensic value](#_Toc156238921) 57

[DNS logging](#_Toc156238922) 58

[PassiveDNS](#_Toc156238923) 59~68

[Creating PassiveDNS evidence](#_Toc156238924) 59

[Use-cases](#_Toc156238925) 68

[Fast-Flux DNS](#_Toc156238926) 60-64

[Fast-Flux DNS (single)](#_Toc156238927) 60-61

[Fast-Flux DNS (double)](#_Toc156238928) 62-63

[Detecting Fast-Flux DNS](#_Toc156238929) 64

[Domain Name Generation Algorithms (DGAs)](#_Toc156238930) 65-66

[DGA CryptoLocker Example](#_Toc156238931) 67

[DNS-over-everything](#_Toc156238932) 69-71

[Overview](#_Toc156238933) 69

[Examples](#_Toc156238934) 70

[Mitigations](#_Toc156238935) 71

[Punycode](#_Toc156238936) 72

[Network Security Monitoring](#_Toc156238937) 74-91

[Origin](#_Toc156238938) 74

[Zeek NSM](#_Toc156238939) 75-91

[Overview](#_Toc156238940) 75

[Use-cases](#_Toc156238941) 76

[Usage](#_Toc156238942) 76

[Zeek log file types](#_Toc156238943) 77-78

[Zeek log content](#_Toc156238944) 79-80

[Parsing with ‘jq’](#_Toc156238945) 81-82

[How-to](#_Toc156238946) 81

[Example](#_Toc156238947) 82

[Pure ‘jq’ vs. ‘grep’ + ‘jq’](#_Toc156238948) 83

[‘jq’ resources](#_Toc156238949) 84

[Signature based detection & scripting](#_Toc156238950) 85

[Community ID](#_Toc156238951) 86-88

[Investigative relevance](#_Toc156238952) 89

[Customized FOR572 policies](#_Toc156238953) 90-91

[Logging Protocols & Aggregation](#_Toc156238954) 96-118

[Syslog](#_Toc156238955) 96-105

[Overview](#_Toc156238956) 96

[Syslog sources](#_Toc156238957) 97

[Syslog servers](#_Toc156238958) 98

[Log content](#_Toc156238959) 99

[Parameters](#_Toc156238960) 100-101

[Facility (source)](#_Toc156238961) 100-101

[Severity (importance)](#_Toc156238962) 100-101

[Priority (PRI)](#_Toc156238963) 100-101

[Syslog configuration](#_Toc156238964) 102-105

[rsyslog config sample](#_Toc156238965) 102-103

[rsyslog config visualized](#_Toc156238966) 104-105

[Windows Event Forwarding](#_Toc156238967) 106-109

[Overview & history](#_Toc156238968) 106-107

[Enterprise scale](#_Toc156238969) 108-109

[Mixed environment](#_Toc156238970) 110-111

[Logging shortfalls](#_Toc156238971) 112

[Real-time centralized logging](#_Toc156238972) 113-114

[Logging innovations](#_Toc156238973) 115-116

[rsyslog](#_Toc156238974) 115-116

[New protocols](#_Toc156238975) 115-116

[Enterprise solutions](#_Toc156238976) 117-118

[ELK Stack](#_Toc156238977) 120-141

[Overview](#_Toc156238978) 120

[Pros & cons](#_Toc156238979) 121-123

[Kibana](#_Toc156238980) 124-127

[SOF-ELK](#_Toc156238981) 128-141

[Overview](#_Toc156238982) 128

[Supported log inputs](#_Toc156238983) 129-131

[Dashboards](#_Toc156238984) 132-141

[Summary dashboard](#_Toc156238985) 132-133

[Syslog dashboard](#_Toc156238986) 134-138

[HTTPD log dashboard](#_Toc156238987) 139-141

# HTTP Protocol 4-

## Overview 4-6

### History & adaptation 4

### Forensic value 5

### HTTP version history 6

## Request/Response dissection 7-26

### Requests 8-14

#### Methods, request string, idempotent 9-10

#### Headers example 11

#### Headers & data 12-14

##### User\_agent

##### Cookies

##### X-Forwarded-For

##### Proxy-Authorization

##### Referer

### Responses 15-26

#### Response codes 16-17

#### Header example 18

#### Headers & data 19-20

## Useful fields 21-22

## Analytic cookies 23-24

### Google Analytic Cookies (UTM) 23-24

### HubSpot targeting cookies 25-26

# HTTP/2 27-31

## Overview 27

## Debug decrypting TLS 28

## Example 29

## Browser developer tools 30-31

# Web server logs 36-47

## Relevance 36

## Log formats 37-43

### Overview 37

### NCSA Common format 38

### W3C Extended/Combined format 39

### Apache mod\_forensic format 40-41

### IIS log format 42-43

#### Default 42

#### ODBC, CBL 43

## Log file analysis methods 44-45

## Investigative value 46-47

# DNS 49-72

## DNS Basics 49-51

### Forward requests 49-50

### Stateless Protocol 51

### EDNS 51

## Compression pointers 52-53

## DNS hierarchy 54

## Canonical Name Records (CNAME) 56

## Forensic value 57

## DNS logging 58

## PassiveDNS 59~68

### Creating PassiveDNS evidence 59

### Use-cases 68

## Fast-Flux DNS 60-64

### Fast-Flux DNS (single) 60-61

### Fast-Flux DNS (double) 62-63

### Detecting Fast-Flux DNS 64

## Domain Name Generation Algorithms (DGAs) 65-66

## DGA CryptoLocker Example 67

## DNS-over-everything 69-71

### Overview 69

### Examples 70

### Mitigations 71

## Punycode 72

# Network Security Monitoring 74-

## Origin 74

## Zeek NSM 75-91

### Overview 75

### Use-cases 76

### Usage 76

### Zeek log file types 77-78

### Zeek log content 79-80

### Parsing with ‘jq’ 81-82

#### How-to 81

#### Example 82

#### Pure ‘jq’ vs. ‘grep’ + ‘jq’ 83

#### ‘jq’ resources 84

### Signature based detection & scripting 85

### Community ID 86-88

### Investigative relevance 89

### Customized FOR572 policies 90-91

# Logging Protocols & Aggregation 96-118

## Syslog 96-105

### Overview 96

### Syslog sources 97

### Syslog servers 98

### Log content 99

### Parameters 100-101

#### Facility (source) 100-101

#### Severity (importance) 100-101

#### Priority (PRI) 100-101

## Syslog configuration 102-105

### rsyslog config sample 102-103

### rsyslog config visualized 104-105

## Windows Event Forwarding 106-109

### Overview & history 106-107

### Enterprise scale 108-109

## Mixed environment 110-111

## Logging shortfalls 112

## Real-time centralized logging 113-114

## Logging innovations 115-116

### rsyslog 115-116

### New protocols 115-116

## Enterprise solutions 117-118

# ELK Stack 120-141

## Overview 120

## Pros & cons 121-123

## Kibana 124-127

## SOF-ELK 128-141

### Overview 128

### Supported log inputs 129-131

### Dashboards 132-141

#### Summary dashboard 132-133

#### Syslog dashboard 134-138

#### HTTPD log dashboard 139-141