

572.2- Core Protocols and Log Aggregation/Analysis

HTTP Protocol.....4-26

Overview 4-6

History & adaptation4

Forensic value5

HTTP version history6

Request/Response dissection 7-26

Requests.....8-14

Methods, request string, idempotent 9-10

Headers example11

Headers & data 12-14

User_agent14

Cookies14

X-Forwarded-For.....14

Proxy-Authorization.....14

Referer.....14

Responses15-26

Response codes..... 16-17

Header example18

Headers & data 19-20

Useful fields..... 21-22

Analytic cookies..... 23-24

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

HubSpot targeting cookies25-26

HTTP/227-31

Overview27

Debug decrypting TLS.....28

Example29

Browser developer tools 30-31

Web server logs.....36-47

Relevance36

Log formats 37-43

Overview37

NCSA Common format38

W3C Extended/Combined format 39

Apache mod_forensic format40-41

IIS log format42-43

Default42

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 logging58

PassiveDNS59~68

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

Punycode72

Network Security Monitoring..... 74-91

Origin74

Zeek NSM 75-91

Overview	75	ELK Stack	120-141
Use-cases	76	Overview	120
Usage.....	76	Pros & cons.....	121-123
Zeek log file types.....	77-78	Kibana.....	124-127
Zeek log content.....	79-80	SOF-ELK.....	128-141
Parsing with 'jq'	81-82	Overview	128
How-to	81	Supported log inputs	129-131
Example.....	82	Dashboards	132-141
Pure 'jq' vs. 'grep' + 'jq'	83	Summary dashboard.....	132-133
'jq' resources.....	84	Syslog dashboard	134-138
Signature based detection & scripting	85	HTTPD log dashboard	139-141
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		