Forensic Log Analysis Report:

The corrupt.vlog is corrupted and so it cannot be analyzed

Analyzed File: session\_1.vlog

Field Occurrence Frequency:

timestamp: 50

event\_type: 50

action\_type: 50

user: 50

target: 44

Sample Parsed Logs:

{'timestamp': '7716948', 'event\_type': 'XR-EXEC', 'action\_type': 'RUN\_usr', 'user': 'tara4', 'target': '/us

{'timestamp': '7716950', 'event\_type': 'XR-LOG', 'action\_type': 'OPN\_usr', 'user': 'odinX', 'target': '/op

{'timestamp': '7716952', 'event\_type': 'XR-CONN', 'action\_type': 'IP', 'user': '224', 'target': '.43.154.13

{'timestamp': '7716954', 'event\_type': 'XR-DEL', 'action\_type': 'DEL\_usr', 'user': 'tara4', 'target': '/tmp

{'timestamp': '7716956', 'event\_type': 'XR-DEL', 'action\_type': 'DEL\_usr', 'user': 'odinX', 'target': '/bin

Analyzed File: session\_2.vlog

Field Occurrence Frequency:

timestamp: 50

event\_type: 50

action\_type: 50

user: 50

target: 46

Sample Parsed Logs:

{'timestamp': '7664148', 'event\_type': 'XR-CONN', 'action\_type': 'IP', 'user': '39', 'target': '.62.133.75'}

{'timestamp': '7664150', 'event\_type': 'XR-EXEC', 'action\_type': 'RUN\_usr', 'user': 'odinX', 'target':'/tm

{'timestamp': '7664152', 'event\_type': 'XR-FILE', 'action\_type': 'MOD\_usr', 'user': 'mira01', 'target': '/e

{'timestamp': '7664154', 'event\_type': 'XR-DEL', 'action\_type': 'DEL\_usr', 'user': 'neo99', 'target': '/usr

{'timestamp': '7664156', 'event\_type': 'XR-FILE', 'action\_type': 'MOD\_usr', 'user': 'odinX', 'target':'/tm

Analyzed File: session\_3.vlog

Field Occurrence Frequency:

timestamp: 50

event\_type: 50

action\_type: 50

user: 50

target: 43

Sample Parsed Logs:

{'timestamp': '7622003', 'event\_type': 'XR-LOG', 'action\_type': 'OPN\_usr', 'user': 'mira01', 'target': '/o

{'timestamp': '7622005', 'event\_type': 'XR-SHDW', 'action\_type': 'KILL\_proc', 'user': 'pid5139', 'target

{'timestamp': '7622007', 'event\_type': 'XR-DEL', 'action\_type': 'DEL\_usr', 'user': 'tara4', 'target': '/opt/

{'timestamp': '7622009', 'event\_type': 'XR-CONN', 'action\_type': 'IP', 'user': '118', 'target': '.13.190.31

{'timestamp': '7622011', 'event\_type': 'XR-EXEC', 'action\_type': 'RUN\_usr', 'user': 'mira01', 'target': '/

Analyzed File: session\_4.vlog

Field Occurrence Frequency:

timestamp: 50

event\_type: 50

action\_type: 50

user: 50

target: 40

Sample Parsed Logs:

{'timestamp': '7875734', 'event\_type': 'XR-FILE', 'action\_type': 'MOD\_usr', 'user': 'tara4', 'target':'/bin

{'timestamp': '7875736', 'event\_type': 'XR-SHDW', 'action\_type': 'KILL\_proc', 'user': 'pid9271', 'target

{'timestamp': '7875738', 'event\_type': 'XR-SHDW', 'action\_type': 'KILL\_proc', 'user': 'pid3118', 'target

{'timestamp': '7875740', 'event\_type': 'XR-EXEC', 'action\_type': 'RUN\_usr', 'user': 'neo99', 'target': '/t

{'timestamp': '7875742', 'event\_type': 'XR-LOG', 'action\_type': 'OPN\_usr', 'user': 'neo99', 'target': '/et

Analyzed File: session\_5.vlog

Field Occurrence Frequency:

timestamp: 50

event\_type: 50

action\_type: 50

user: 50

target: 45

Sample Parsed Logs:

{'timestamp': '7928936', 'event\_type': 'XR-DEL', 'action\_type': 'DEL\_usr', 'user': 'neo99', 'target': '/tm

{'timestamp': '7928938', 'event\_type': 'XR-FILE', 'action\_type': 'MOD\_usr', 'user': 'tara4', 'target': '/us

{'timestamp': '7928940', 'event\_type': 'XR-SHDW', 'action\_type': 'KILL\_proc', 'user': 'pid5834', 'target

{'timestamp': '7928942', 'event\_type': 'XR-CONN', 'action\_type': 'IP', 'user': '172', 'target': '.70.145.19

{'timestamp': '7928944', 'event\_type': 'XR-DEL', 'action\_type': 'DEL\_usr', 'user': 'mira01', 'target': '/et