THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

WAND
University of Waikato
Network Research Group

openLI

Running a Static IP Intercept

OpenLI Training: Chapter Fourteen

Shane Alcock
University of Waikato
New Zealand
shane.alcock@waikato.ac.nz

Replaying IP Traffic

- Last lesson, we configured a static IP intercept
  - Target address was 10.1.18.217

- OpenLI will now intercept all traffic to and from that address
  - We just need to generate some matching traffic in the lab

Replaying IP Traffic

- On the collector container, run:

```
tracereplay /home/openli-coll/pcaps/staticip.pcap ring:eth2
```

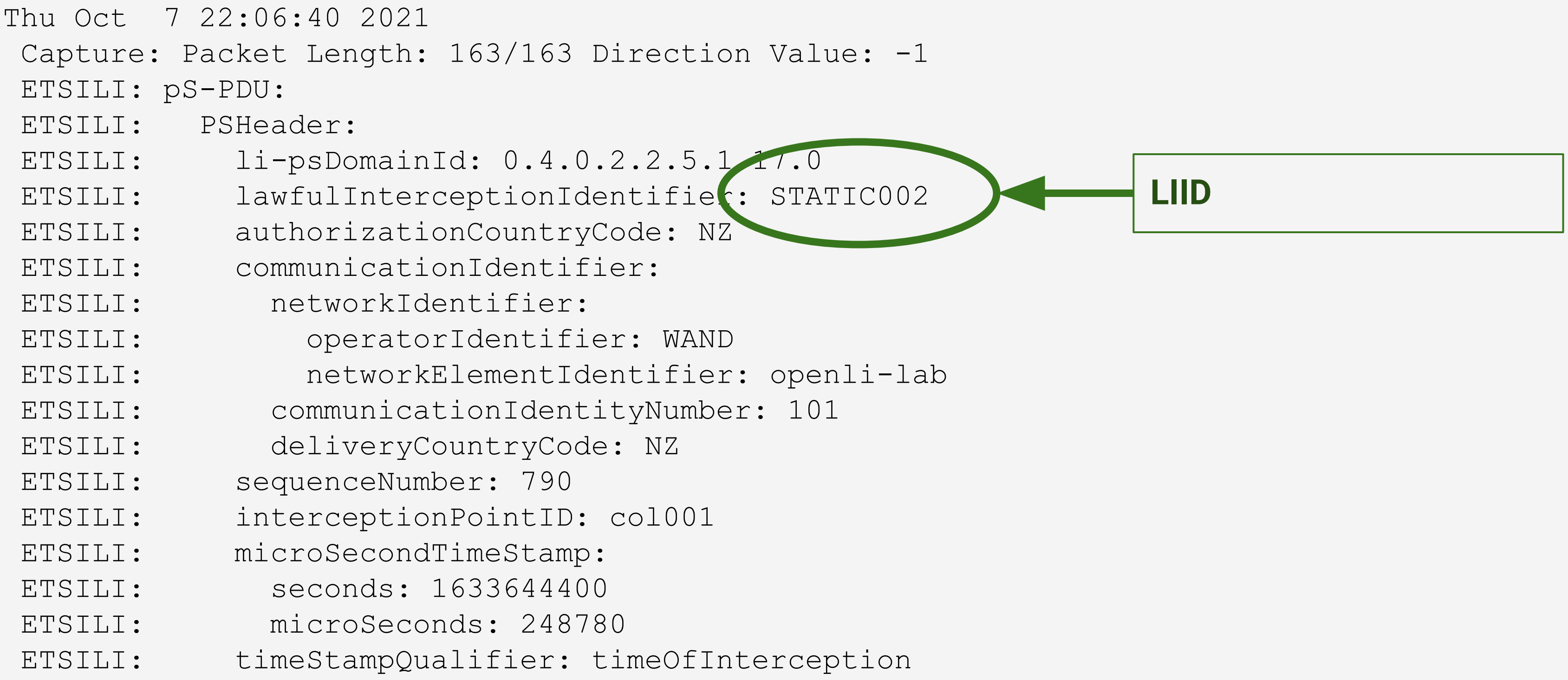
Examining HI3 Output

- Let’s take a look at the tracepktdump output for HI3
  - Remember this will be on the openli-agency container
  - Focus again on the **last** displayed packet
  - Starting with the PS Header

Examining HI3 Output

```
Thu Oct  7 22:06:40 2021
 Capture: Packet Length: 163/163 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: STATIC002
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 101
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 790
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633644400
 ETSILI:       microSeconds: 248780
 ETSILI:     timeStampQualifier: timeOfInterception
```

Examining HI3 Output



```
Thu Oct  7 22:06:40 2021
 Capture: Packet Length: 163/163 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: STATIC002
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 101
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 790
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633644400
 ETSILI:       microSeconds: 248780
 ETSILI:     timeStampQualifier: timeOfInterception
```

LIID

Examining HI3 Output

```
Thu Oct  7 22:06:40 2021
 Capture: Packet Length: 163/163 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: STATIC002
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 101
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 790
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633644400
 ETSILI:       microSeconds: 248780
 ETSILI:     timeStampQualifier: timeOfInterception
```

CIN -- session ID

Examining HI3 Output

- Now let's look at the CC Payload

Examining HI3 Output

```
ETSILI:   Payload:
ETSILI:     cCPayloadSequence:
ETSILI:       CCPayload:
ETSILI:       payloadDirection: toTarget
ETSILI:       cCContents:
ETSILI:         iPCC:
ETSILI:           iPCCObjId: .5.3.10.2
ETSILI:           iPCCContents:
ETSILI:             iPPackets: ...
```

DIRECTION

Examining HI3 Output

- Finally, the captured IP payload itself

Examining HI3 Output

```
 IP: Header Len 20 Ver 4 DSCP 04 ECN 0 Total Length 52
 IP: Id 15749 Fragoff 0 DONT_FRAG
 IP: TTL 64 Proto 6 Checksum 7473
 IP: Source 80.180.114.112 Destination 10.1.18.217
 TCP: Source 50388 Dest 22
 TCP: Seq 3164057130
 TCP: Ack 149079413
 TCP: DOFF 8 Flags: ACK Window 65534
 TCP: Checksum 39408 Urgent 0
 TCP: NOP
 TCP: NOP
 TCP: Timestamp 756097133 106932973
unknown protocol tcp/22
 Unknown Protocol: 22
```

Examining HI3 Output

```
 IP: Header Len 20 Ver 4 DSCP 04 ECN 0 Total Length 52
 IP: Id 15749 Fragoff 0 DONT_FRAG
 IP: TTL 64 Proto 6 Checksum 7473
 IP: Source 80.180.114.112 Destination 10.1.18.217
 TCP: Source 50388 Dest 22
 TCP: Seq 3164057130
 TCP: Ack 149079413
 TCP: DOFF 8 Flags: ACK Window 65534
 TCP: Checksum 39408 Urgent 0
 TCP: NOP
 TCP: NOP
 TCP: Timestamp 756097133 106932973
unknown protocol tcp/22
 Unknown Protocol: 22
```

THE TARGET IP

Examining HI2 Output

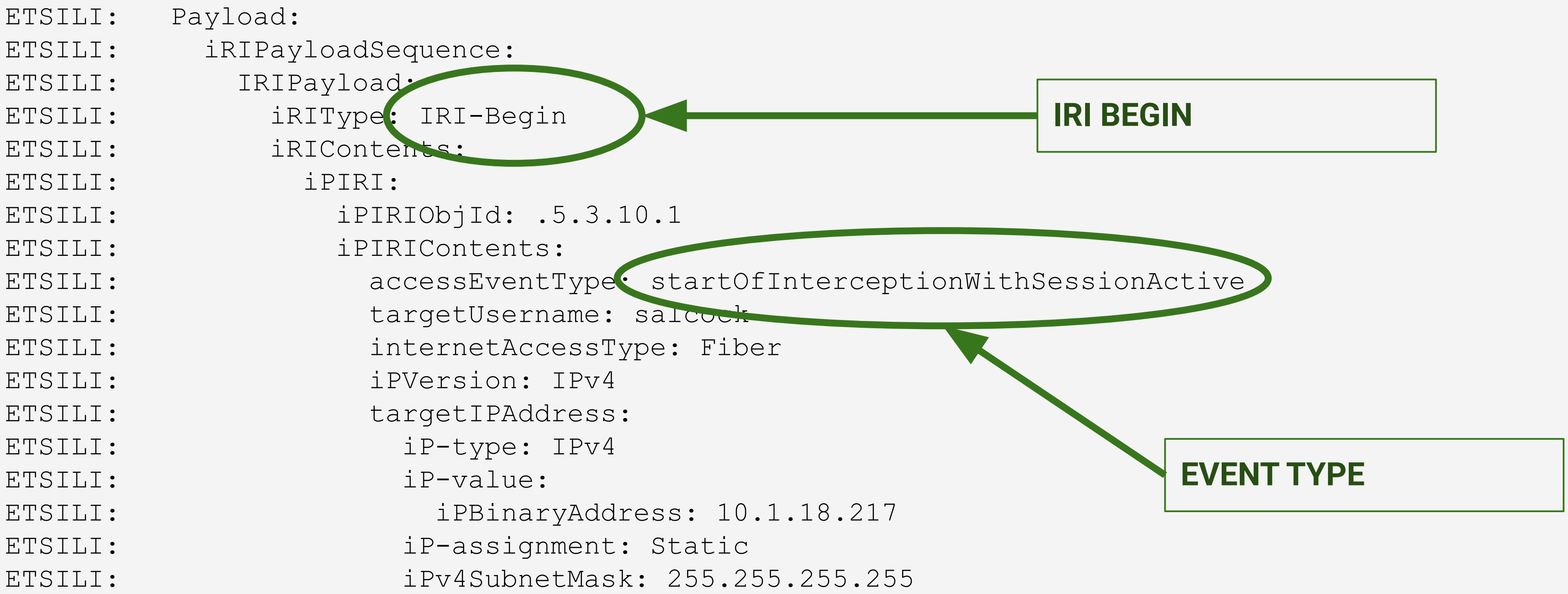
- HI2 records are sparse for a static IP intercept
  - Session is continuous, so no state changes to report
  - No accounting protocol

- ETSI defines IRIs for sessions that are already active
  - Let’s look at one (skipping the PS Header which is unchanged)

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:         iRIType: IRI-Begin
ETSILI:         iRIContents:
ETSILI:           iPIRI:
ETSILI:             iPIRIObjId: .5.3.10.1
ETSILI:             iPIRIContents:
ETSILI:               accessEventType: startOfInterceptionWithSessionActive
ETSILI:               targetUsername: salcock
ETSILI:               internetAccessType: Fiber
ETSILI:               iPVersion: IPv4
ETSILI:               targetIPAddress:
ETSILI:                 iP-type: IPv4
ETSILI:                 iP-value:
ETSILI:                   iPBinaryAddress: 10.1.18.217
ETSILI:                 iP-assignment: Static
ETSILI:                 iPv4SubnetMask: 255.255.255.255
```

Examining HI2 Output



```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:         iRIType: IRI-Begin
ETSILI:         iRIContents:
ETSILI:           iPIRI:
ETSILI:             iPIRIObjId: .5.3.10.1
ETSILI:             iPIRIContents:
ETSILI:               accessEventType: startOfInterceptionWithSessionActive
ETSILI:               targetUsername: salcock
ETSILI:               internetAccessType: Fiber
ETSILI:               iPVersion: IPv4
ETSILI:               targetIPAddress:
ETSILI:                 iP-type: IPv4
ETSILI:                 iP-value:
ETSILI:                   iPBinaryAddress: 10.1.18.217
ETSILI:                 iP-assignment: Static
ETSILI:                 iPv4SubnetMask: 255.255.255.255
```

IRI BEGIN

EVENT TYPE

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:         iRIType: IRI-Begin
ETSILI:         iRIContents:
ETSILI:           iPIRI:
ETSILI:             iPIRIObjId: .5.3.10.1
ETSILI:             iPIRIContents:
ETSILI:               accessEventType: startOfInterceptionWithSessionActive
ETSILI:               targetUsername: salcock
ETSILI:               internetAccessType: Fiber
ETSILI:               iPVersion: IPv4
ETSILI:               targetIPAddress:
ETSILI:                 iP-type: IPv4
ETSILI:                 iP-value:
ETSILI:                   iPBinaryAddress: 10.1.18.217
ETSILI:                 iP-assignment: Static
ETSILI:                 iPv4SubnetMask: 255.255.255.255
```

USERNAME

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:         iRIType: IRI-Begin
ETSILI:         iRIContents:
ETSILI:           iPIRI:
ETSILI:             iPIRIObjId: .5.3.10.1
ETSILI:             iPIRIContents:
ETSILI:               accessEventType: startOfInterceptionWithSessionActive
ETSILI:               targetUsername: salcock
ETSILI:               internetAccessType: Fiber
ETSILI:               iPVersion: IPv4
ETSILI:               targetIPAddress:
ETSILI:                 iP-type: IPv4
ETSILI:                 iP-value:
ETSILI:                   iPBinaryAddress: 10.1.18.217
ETSILI:                 iP-assignment: Static
ETSILI:                 iPv4SubnetMask: 255.255.255.255
```

ACCESS TYPE

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:         iRIType: IRI-Begin
ETSILI:         iRIContents:
ETSILI:           iPIRI:
ETSILI:             iPIRIObjId: .5.3.10.1
ETSILI:             iPIRIContents:
ETSILI:               accessEventType: startOfInterceptionWithSessionActive
ETSILI:               targetUsername: salcock
ETSILI:               internetAccessType: Fiber
ETSILI:               iPVersion: IPv4
ETSILI:               targetIPAddress:
ETSILI:                 iP-type: IPv4
ETSILI:                 iP-value:
ETSILI:                   iPBinaryAddress: 10.1.18.217
ETSILI:                 iP-assignment: Static
ETSILI:                 iPv4SubnetMask: 255.255.255.255
```

IP ADDRESS

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:         iRIType: IRI-Begin
ETSILI:         iRIContents:
ETSILI:           iPIRI:
ETSILI:             iPIRIObjId: .5.3.10.1
ETSILI:             iPIRIContents:
ETSILI:               accessEventType: startOfInterceptionWithSessionActive
ETSILI:               targetUsername: salcock
ETSILI:               internetAccessType: Fiber
ETSILI:               iPVersion: IPv4
ETSILI:               targetIPAddress:
ETSILI:                 iP-type: IPv4
ETSILI:                 iP-value:
ETSILI:                   iPBinaryAddress: 10.1.18.217
ETSILI:                 iP-assignment: Static
ETSILI:                 iPv4SubnetMask: 255.255.255.255
```

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:         iRIType: IRI-Begin
ETSILI:         iRIContents:
ETSILI:           iPIRI:
ETSILI:             iPIRIObjId: .5.3.10.1
ETSILI:             iPIRIContents:
ETSILI:               accessEventType: startOfInterceptionWithSessionActive
ETSILI:               targetUsername: salcock
ETSILI:               internetAccessType: Fiber
ETSILI:               iPVersion: IPv4
ETSILI:               targetIPAddress:
ETSILI:                 iP-type: IPv4
ETSILI:                 iP-value:
ETSILI:                   iPBinaryAddress: 10.1.18.217
ETSILI:                 iP-assignment: Static
ETSILI:                 iPv4SubnetMask: 255.255.255.255
```

MASK

Examining HI2 Output

- Withdrawing the intercept will produce a similar IRI
    - IRI Type: IRI-End
    - Access Event Type: endOfInterceptionWithSessionActive

Next Time

- IP intercepts when using RADIUS to assign IPs