slide1

slide2


BRITISH
COLUMBIA
Introduction
Lance Morgan
Lead Investigator
Office of the Chief Information Officer
Investigations and Forensics Unit
2

slide3


BRITISH
COLUMBIA
Investigator
Common Traits
• Unbiased
• Flexible
• Alert / Observant
• Organized
• Creative Thinker
• Tactful / Understanding
• And know when to not be
• Professional and Thorough
3

slide4

Investigation

What are the Key Elements?

- Issue / Complaint / Allegation
- Person(s) of interest
- A definitive resolution

- RESPONISIBILITY / AUTHORITY to investigate

slide5

Investigation

Process Terms

- Reasonable and Probable Grounds
- Mandate and Scope
- Investigative Interview
- Standard of Proof
- Continuity of Evidence
- Exhibit

slide6

Common Investigation Types

- Human Resource
  - Inappropriate Use
- Internal Threat
  - Compromised / Unsophisticated Employee
  - Malicious Employee
- External Threat
  - Nefarious Actors

slide7


BRITISH
COLUMBIA
Conducting an Investigation
Initiation
• Identify Issue
• Identify actors / key assets
• Plan the investigation
• Open Case - Documentation
• Identify Resources required to successfully review the situation
7

slide8

BRITISH COLUMBIA

Conducting an Investigation

Documentation

- Initial Report
- Ongoing Documentation
- Interim Reporting
- Concluding Report
  - Recommendations?

slide9


BRITISH
COLUMBIA
Conducting an Investigation
Documentation - Elements of a report
• Administrative
• Who's involved
• Narrative
• What I did
• Summary
• What I found
• Concluding Report
• Recommendations ?
9

slide10

Conducting an Investigation

Coordination

- Coordinate response
  - Who is part of the investigative team?
  - Who needs to be notified / kept apprised

- Each investigation is unique

slide11

Data Collection

'Evidence'

- Physical assets
  - Devices
- Documentary
  - Logs
- Testimonial
  - Statements

slide12


BRITISH
COLUMBIA
Standard Evidence Principles
• Standard of Proof
• Criminal
• Civil
• Entrapment
• Admissibility of Evidence
• Chain of Custody
• Non Repudiation of Data
12

slide13

BRITISH COLUMBIA

Interviewing

slide14


BRITISH
COLUMBIA
Interviewing
2 Key purposes
• Determine facts
• Detect Deception
14

slide15


BRITISH
COLUMBIA
Interviewing
Determine Facts
Key Questions to ask yourself
• What do I know
• How do I know it
• Why is it important
15

slide16


BRITISH
COLUMBIA
Interviewing
Actors
• Witnesses
• Suspects
• Corroborative persons
16

slide17


BRITISH
COLUMBIA
Interviewing
Traditional
• What Happened?
• Chronological in nature
• Isolates the event in the interviewee
17

slide18

Interviewing

Cognitive

- Re-establish environment, mood, setting & experiences
- Non linear
- Non specific – enjoy the journey …

slide19

slide20

http://www.ctvnews.ca/a-deeper-look-into-the-interrogation-of-russell-williams-1.565832

slide21

Forensic Interview

Used with Suspects

Part 1: Information Gathering

- Understand the circumstances
- Have suspect commit to their "story"

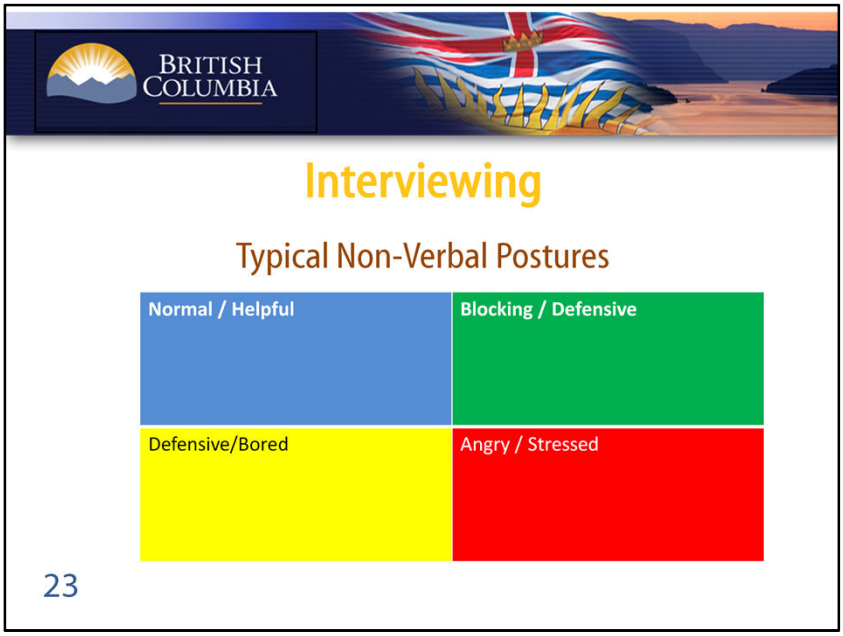
Part 2: Interrogation

- Break down their "story" by identifying inconsistencies, lies, etc.
- Have the suspect provide an admission and confession

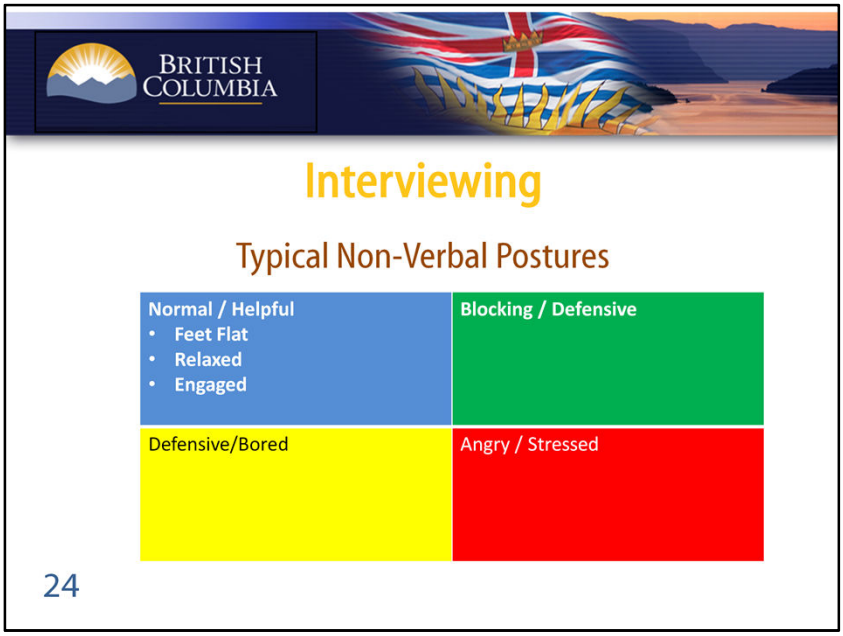
slide22


BRITISH
COLUMBIA
Interviewing
• Various Techniques:
• Open ended
• Goal:
• Develop as clear a picture as possible
22

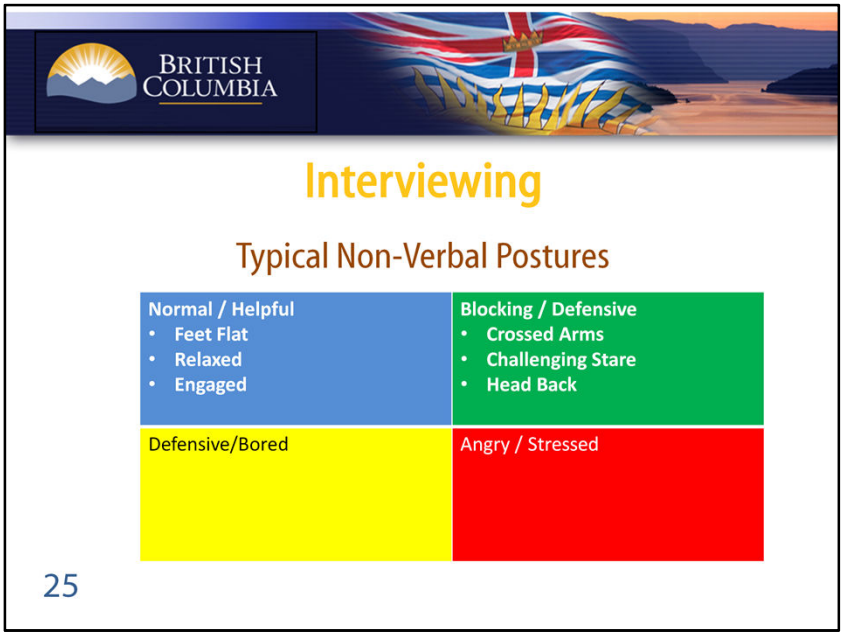
slide23


BRITISH COLUMBIA
Interviewing
Typical Non-Verbal Postures
Normal / Helpful
Blocking / Defensive
Defensive/Bored
Angry / Stressed
23

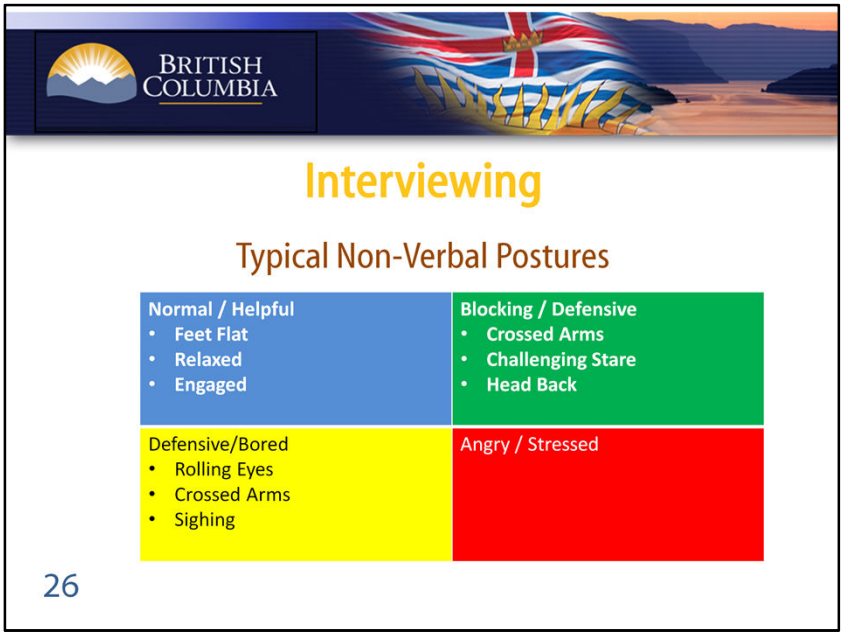
slide24


BRITISH COLUMBIA
Interviewing
Typical Non-Verbal Postures
Normal / Helpful
• Feet Flat
• Relaxed
• Engaged
Blocking / Defensive
Defensive/Bored
Angry / Stressed
24

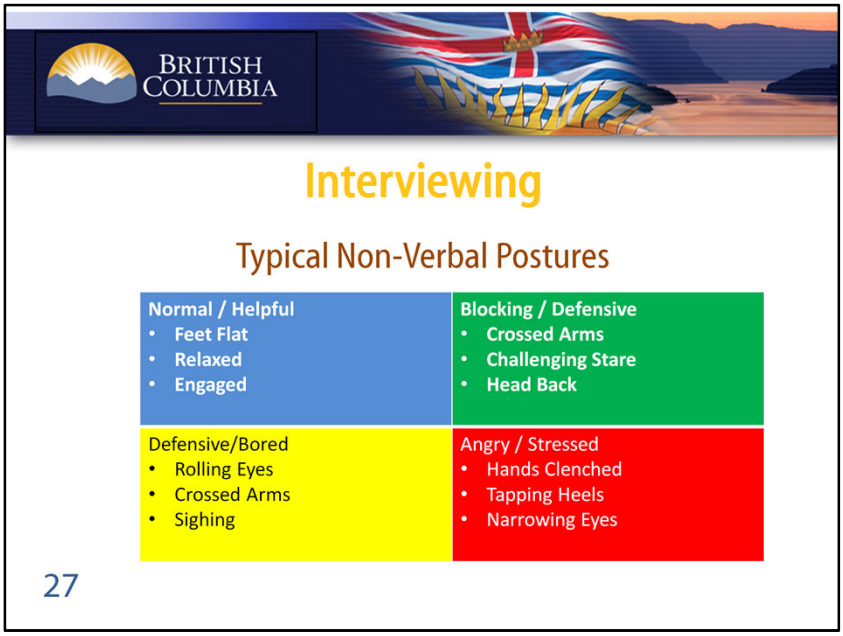
slide25


BRITISH COLUMBIA
Interviewing
Typical Non-Verbal Postures
Normal / Helpful
• Feet Flat
• Relaxed
• Engaged
Blocking / Defensive
• Crossed Arms
• Challenging Stare
• Head Back
Defensive/Bored
Angry / Stressed
25

slide26


BRITISH COLUMBIA
Interviewing
Typical Non-Verbal Postures
Normal / Helpful
• Feet Flat
• Relaxed
• Engaged
Blocking / Defensive
• Crossed Arms
• Challenging Stare
• Head Back
Defensive/Bored
• Rolling Eyes
• Crossed Arms
• Sighing
Angry / Stressed
26

slide27


BRITISH COLUMBIA
Interviewing
Typical Non-Verbal Postures
Normal / Helpful
• Feet Flat
• Relaxed
• Engaged
Blocking / Defensive
• Crossed Arms
• Challenging Stare
• Head Back
Defensive/Bored
• Rolling Eyes
• Crossed Arms
• Sighing
Angry / Stressed
• Hands Clenched
• Tapping Heels
• Narrowing Eyes
27

slide28


BRITISH
COLUMBIA
Common Investigation Types
• Human Resource
• Inappropriate Use
• Threatening Behaviour
• Misuse of Time
• Bringing employer into disrepute / exposure of data
• Copyright Infringement
28

slide29


BRITISH
COLUMBIA
Common Investigation Types
• Internal Threat
• Unsophisticated Employee
• Compromised Employee
• Malicious Employee
• Key loggers / introduction of malware
• Data Leak
• Hacking
• Social Engineering
• Hacktivists
29

slide30


BRITISH
COLUMBIA
Common Investigation Types
• External Threat
• Nefarious Actors
• Hackers, Phishers, Hacktivists
• Social Engineers (Mitnick)
30

slide31

http://www.azfamily.com/news/Tempted-to-vent-about-work-online-You-could-get-fired-188133881.html

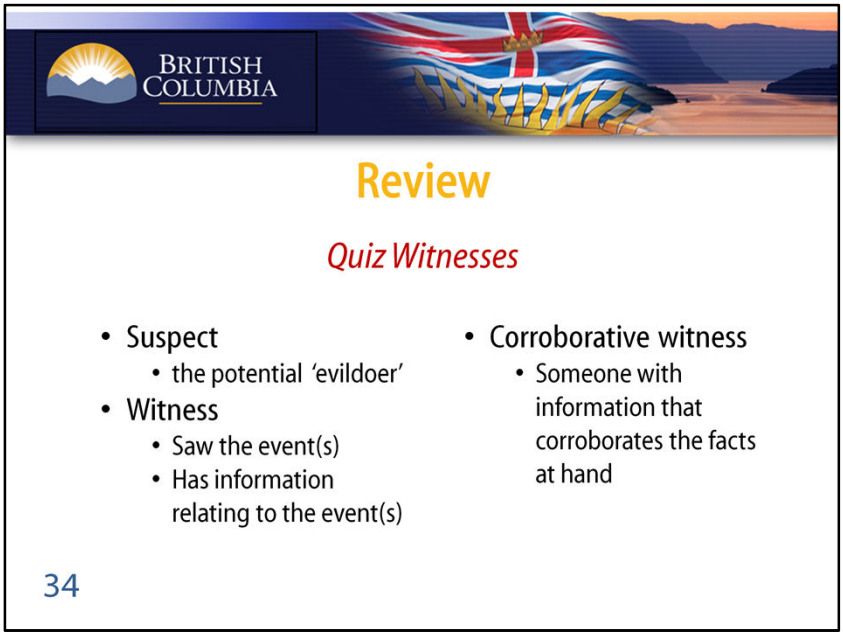
slide32

slide33

Review

- Types of Actors?
  - Suspects
  - Witnesses / Corroborative Witnesses
- Types of Data Sources (Evidence)
  - Logs
  - Devices
- Documentary Requirements
  - Reports / Communications Trail

slide34

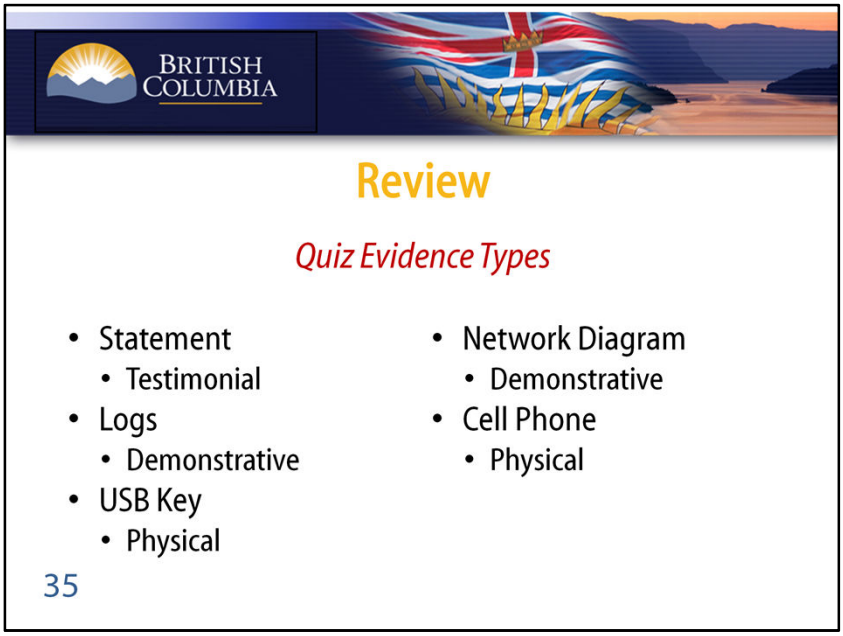


Review

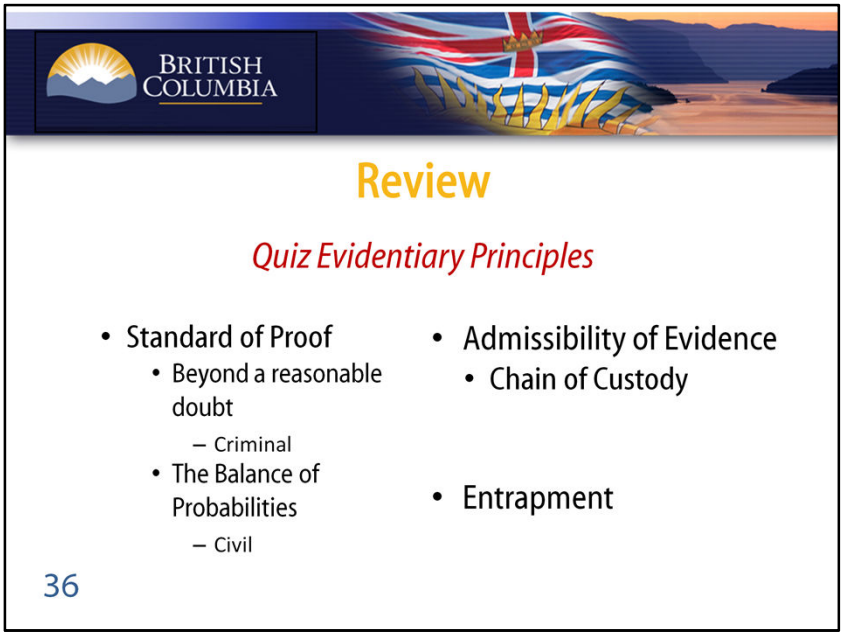
Quiz Witnesses

- Suspect
  - the potential 'evildoer'
- Witness
  - Saw the event(s)
  - Has information relating to the event(s)
- Corroborative witness
  - Someone with information that corroborates the facts at hand

slide35


BRITISH
COLUMBIA
Review
Quiz Evidence Types
• Statement
• Testimonial
• Logs
• Demonstrative
• USB Key
• Physical
• Network Diagram
• Demonstrative
• Cell Phone
• Physical
35

slide36



Review

Quiz Evidentiary Principles

- Standard of Proof
  - Beyond a reasonable doubt
    - Criminal
  - The Balance of Probabilities
    - Civil
- Admissibility of Evidence
  - Chain of Custody
- Entrapment

slide37

BRITISH COLUMBIA

Review

Documentation - Elements of a report

- Administrative
  - Who's involved
- Narrative
  - What I did
- Summary
  - What I found
- Concluding Report
  - Recommendations ?

slide38


BRITISH
COLUMBIA
Current Events
It's a wild wild world....
• Hacktivists
• Script Kiddies
• Useful idiots….
• Hackers
• Criminal Elements
• National Actors
• Co-opted elements.
38

slide39

Espionage / Exploits

Nothing New

- Social Engineering
- USB Techniques
- Flame

slide40


BRITISH
COLUMBIA
Espionage / Exploits
Nothing New
• Social Engineering
• Officers, Agents & Spies
• Covert agendas
• Not what it appears to be
• Prays on human nature to be 'helpful'
40

slide41

Espionage / Exploits

Nothing New

- USB Techniques
  - Stuxnet
  - Key loggers
  - Other viral implants
  - Data Extraction

slide42

Espionage / Exploits

Nothing New

- Flame
  - Data Extraction
  - Network exploitation
  - High degree of sophistication
- Mini-Flame
  - Follow on for precision strikes

slide43

http://www.youtube.com/watch?v=M4V3BwTlN0A
RU Television

http://www.youtube.com/watch?v=M4V3BwTlN0A
47 MInute
US Naval War College ILD 2012 Panel Discussion Cyber Attacks: The Law
Published on Oct 10, 2012
International Law Conference, U.S. Naval War College
June 25-27, 2012

http://www.youtube.com/watch?v=oz_NPGqNlqo
PBS Great Decisions 2012 Excerpts: How to Protect Against Cyber Attacks
Published on Jun 11, 2012
From Great Decisions 2012, Episode 4 "Cybersecurity: Defense in the Digital Age" - Originally aired on PBS
As cyber attacks continue to occur at a breakneck pace, is the U.S. at risk?
Category
News & Politics
License
Standard YouTube License
http://www.youtube.com/watch?v=3V8w5yDEY84

Published on Oct 1, 2012
Posted 9/22/2012

slide44

'Cyber War'

Future is Now

- Estonia 2007
  - Strictly non kinetic – Infowar
  - Used by 'non-national' forces against Estonian Government and Financial targets
  - Suspected involvement of Russian Authorities but no proof

slide45


BRITISH
COLUMBIA
'Cyber War'
Future is Now
• Georgia 2008
• Supported Kinetic activity
• Active DDOS against Georgian Government Sites
• Experts believe involvement of Russian Military Intelligence and Federal Security highly likely.
45

slide46


BRITISH
COLUMBIA
'Cyber War'
Future is Now
• South Korea 2011
• 10 Days of Rain
• Brilliant use of cultural knowledge in creating the exploit tool
• Major assault against S. Korean Government sites and US Forces Korea network
• Self destruct feature
• Very sophisticated for a 'simple' DDOS strike
– A test for something later????
46

slide47

'Cyber War'

Future is Now

- Iran Stuxnet / Duqu
  - The next level
    - Multi-nation effort – ***Operation Olympic Games***
    - Highly specific
    - Huge Effort
    - An example of asymmetric warfare
- Supply Chain issues

slide48

slide49

http://threatpost.com/en_us/blogs/malware-infects-two-power-plants-lacking-basic-security-controls-011413

http://www.theregister.co.uk/2008/01/11/tram_hack/

STUXNET
Cyber Defence Units Announced Recently:

India
Turkey
Brazil

Romania recently attacked through Red October vulnerability

slide50

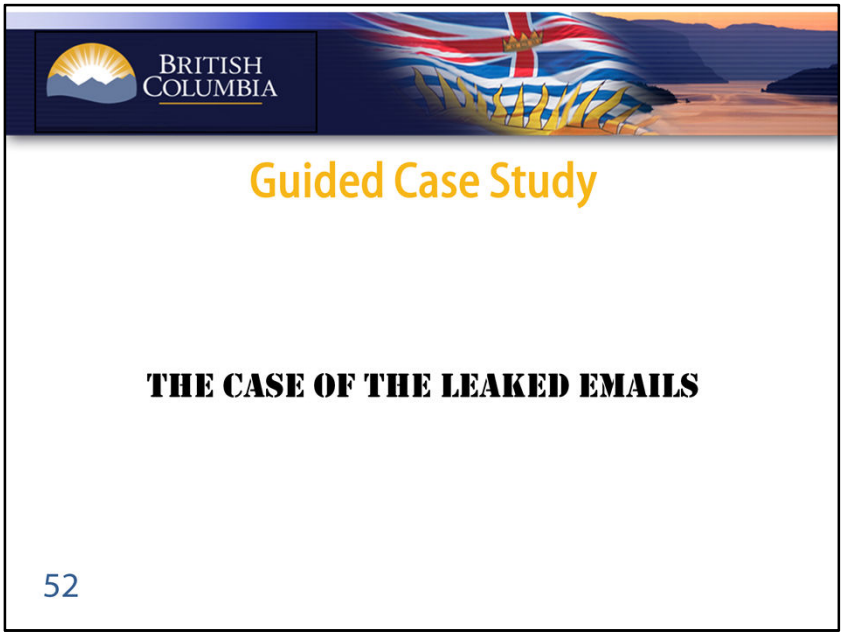
Privacy and Investigations

Regina v. Cole

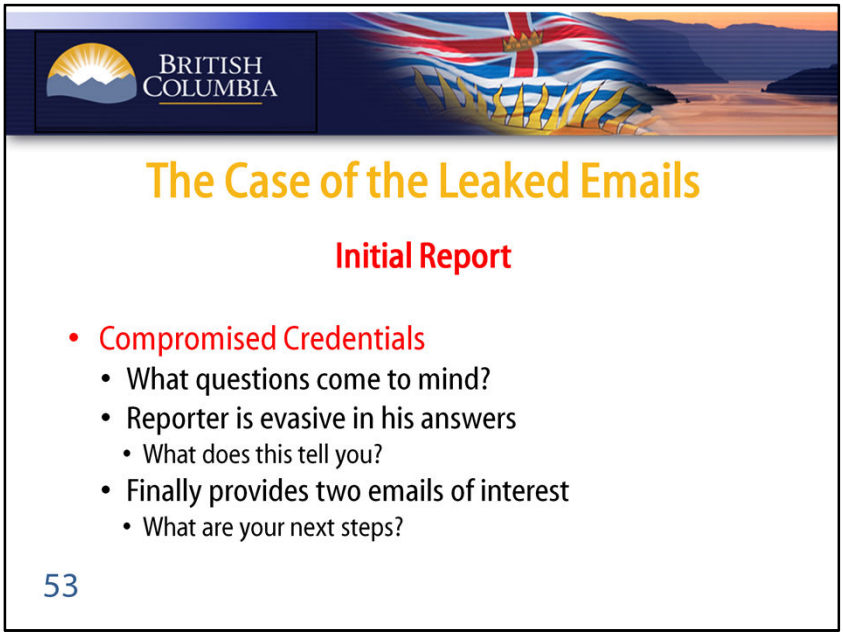
- Unreasonable Search and Seizure
  - Device was provided for personal use as well
  - Device transferred to Law Enforcement
- Employer Policies of Use must be clear
- Personal Use allowances invite risk and uncertainty

slide51

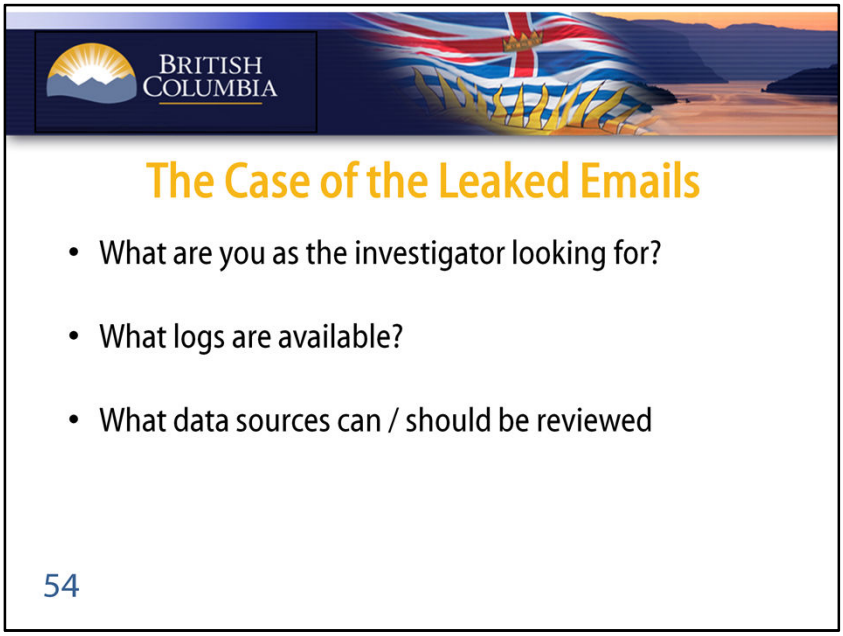
slide52


BRITISH
COLUMBIA
Guided Case Study
THE CASE OF THE LEAKED EMAILS
52

slide53


BRITISH
COLUMBIA
The Case of the Leaked Emails
Initial Report
• Compromised Credentials
• What questions come to mind?
• Reporter is evasive in his answers
• What does this tell you?
• Finally provides two emails of interest
• What are your next steps?
53

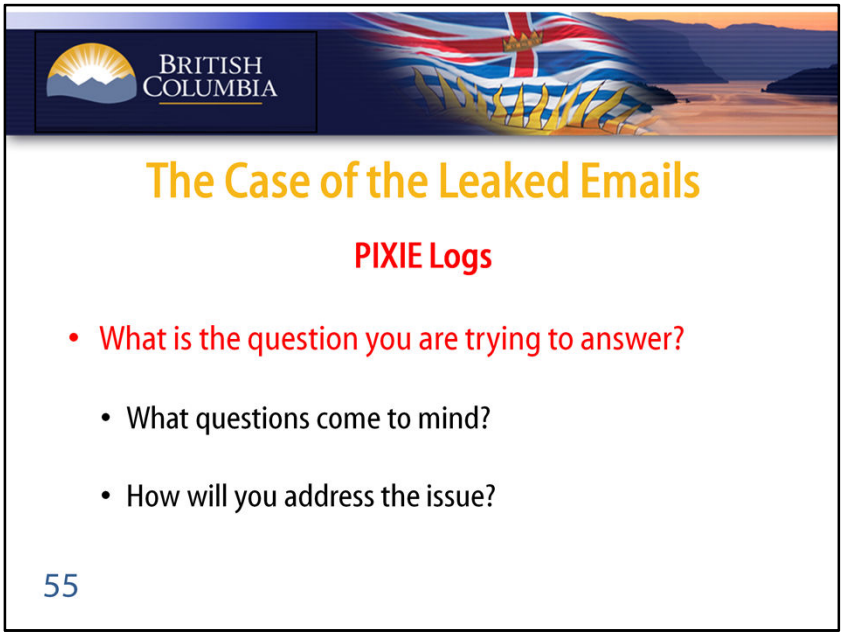
slide54



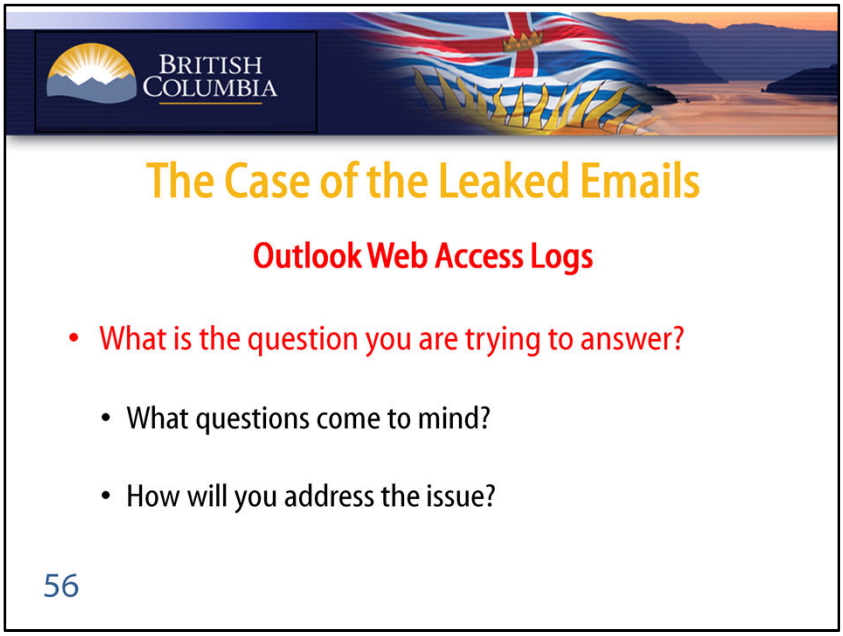
The Case of the Leaked Emails

- What are you as the investigator looking for?
- What logs are available?
- What data sources can / should be reviewed

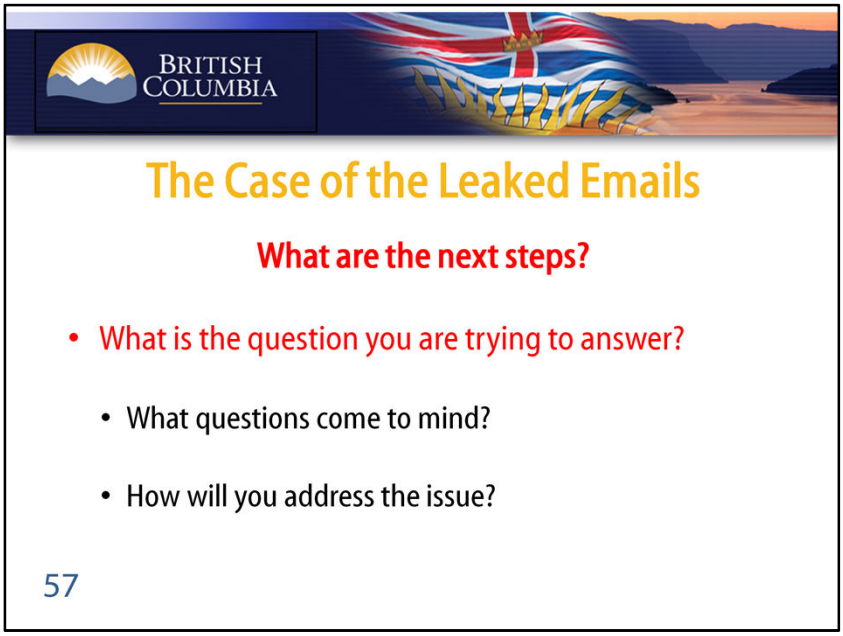
slide55


BRITISH
COLUMBIA
The Case of the Leaked Emails
PIXIE Logs
• What is the question you are trying to answer?
• What questions come to mind?
• How will you address the issue?
55

slide56


BRITISH
COLUMBIA
The Case of the Leaked Emails
Outlook Web Access Logs
• What is the question you are trying to answer?
• What questions come to mind?
• How will you address the issue?
56

slide57


BRITISH
COLUMBIA
The Case of the Leaked Emails
What are the next steps?
• What is the question you are trying to answer?
• What questions come to mind?
• How will you address the issue?
57