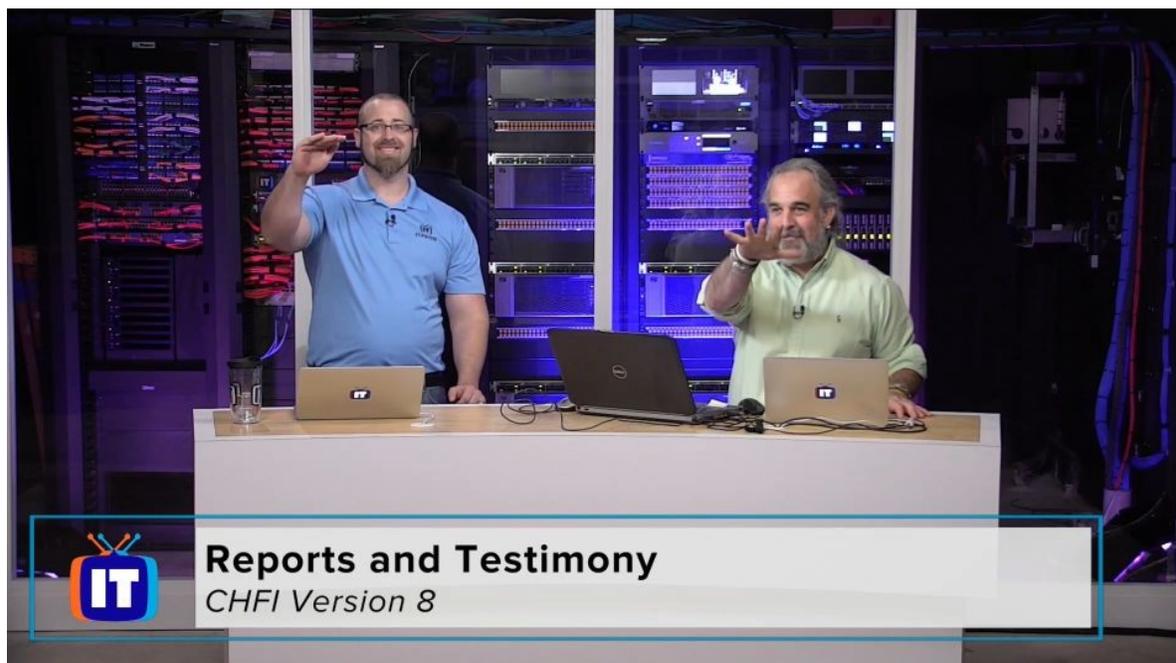


## ITPro TV Computer Hacking Forensics Investigator (CHFI) v8



In this episode, Daniel Lowrie and Adam Gordon talk about what's involved in creating official reports and acting as an expert witness. They explain what qualifies a person as an expert witness to be considered for that duty. Finally, they take a look at an example of what an official CHFI report consists of.

Note: Some folders in the listed curriculum are empty and therefore this set is not complete.

### **Contents:**

#### **Computer\_Forensics\_in\_Today's\_World:**

- 0.0 - Overview (195645124)
- 1.0 - Computer Forensics in Todays World
- 2.0 - Computer Forensics in Todays World Part 2
- 3.0 - Computer Forensics in Todays World Part 3

#### **Computer\_Forensics\_Investigation\_Process:**

- 20.0 - Investigative Process
- 21.0 - Investigative Process Part 2
- 22.0 - Investigative Process Part 3
- 23.0 - Investigative Process Part 4

#### **Searching\_and\_Seizing\_Computers:**

- 30.0 - Search and Seizure of a Computer
- 31.0 - Search and Seizure of a Computer

32.0 - Search and Seizure of a Computer Part 3  
33.0 - Search and Seizure of a Computer Part 4

**Digital Evidence:**

40.0 - Digital Evidence  
41.0 - Digital Evidence Part 2

**First Responder Procedures:**

50.0 - First Responders

**Computer Forensics Labs:**

60.0 - Setting up Forensics Lab

**Understanding Hard Disks and File Systems:**

70.0 - Hard Disks and File Systems  
71.0 - Hard Disks and File Systems Part 2  
72.0 - Hard Disks and File Systems Part 3  
73.0 - Hard Disks and File Systems Part 4

**Windows Forensics:**

80.0 - Windows Forensics  
81.0 - Windows Forensics Part 2  
82.0 - Windows Forensics Part 3  
83.0 - Windows Forensics Part 4  
84.0 - Windows Forensics Part 5

**Data Acquisition and Duplication:**

90.0 - Data Acquisition, Duplication and Recovery  
92.0 - Overview of The Sleuth Kit (TSK)

**Recovering Deleted Files and Deleted Partitions:**

-empty folder-

**Forensics Investigation Using AccessData FTK:**

100.0 - AccessData FTK

**Forensics Investigation Using Encase:**

101.0 - EnCase

**Steganography and Image File Forensics:**

110.0 - Steganography  
111.0 - Steganography Part 2

**Application and Password Crackers:**

120.0 - Password Crackers  
121.0 - Password Crackers Part 2

**Log\_Capturing\_and\_Event\_Correlation:**

130.0 - Log Capturing and Network Forensics

131.0 - Log Capturing and Network Forensics Part 2

132.0 - Log Capturing and Network Forensics Part 3

133.0 - Log Capturing and Network Forensics Part 4

**Network\_Forensics:**

-empty folder-

**Investigating\_Wireless\_Attacks:**

170.0 - Wireless

171.0 - Wireless Part 2

**Investigating\_Web\_Attacks:**

180.0 - Web Forensics

181.0 - Web Forensics Part 2

**Tracking\_Emails\_and+Investigating\_Email\_Crimes:**

190.0 - Email Forensics

**Mobile\_Forensics:**

200.0 - Mobile Forensics

**Investigative\_Reports:**

210.0 - Reports and Testimony

**Becoming\_An\_Expert\_Witness:**

-empty folder-