Launching Computer Hacking Forensic Investigator (CHFI) v9

January 25 2017

EC-Council

C|HFI™

Computer Hacking Forensic INVESTIGATOR

EC-Council at a Glance

EC-Council Group is a multidisciplinary institution of global Information Security professional services.

EC-Council Group is a dedicated Information Security organization that aims at creating knowledge, facilitating innovation, executing research, implementing development, and nurturing subject matter experts in order to provide their unique skills and niche expertise in cybersecurity.

Some of the finest organizations around the world such as the US Army, US Navy, DoD, the FBI, Microsoft, IBM, and the United Nations have trusted ECC to develop and advance their security infrastructure.

ICECC

International Council of E-Commerce Consultants

EC-Council Group

ECCU

EC-Council University

Division of Academic Education

ECC

EC-Council Training & Certification

Division of Professional Workforce Development

EGS

EC-Council Global Services

Division of Corporate Consulting & Advisory Services

EGE

EC-Council Global Events

Division of Conferences, Forums, Summits, Workshops & Industry Awards

ECF

EC-Council Foundation

Non-Profit Organization for Cyber Security Awareness Increase.

WE ARE INFORMATION SECURITY

- 15+ **YEARS EXPERIENCE**
- 40+ **TRAINING & CERTIFICATION PROGRAMS**
- 145+ **COUNTRIES**
- 350+ **SUBJECT MATTER EXPERTS**
- 700+ **TRAINING PARTNERS WORLDWIDE**
- 3000 **TOOLS & TECHNOLOGIES**
- 150,000 **CERTIFIED MEMBERS**

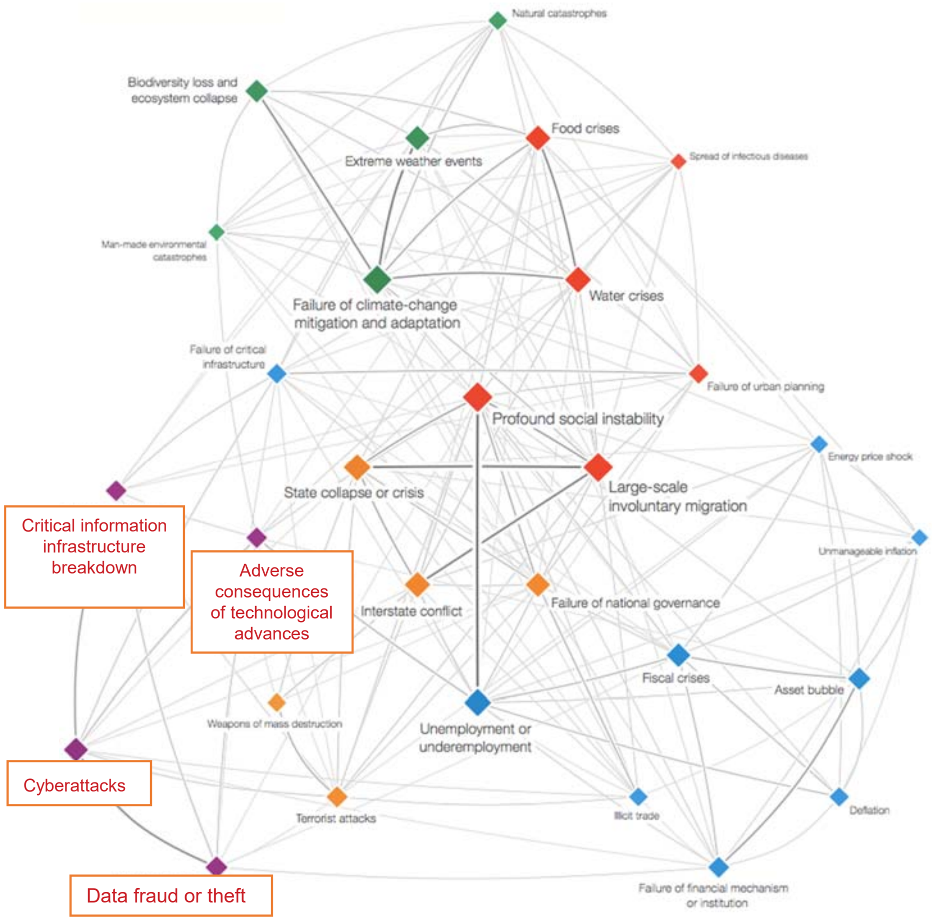
World Economic Forum Ranks Cyber-attacks Among Top Global Risks in its 2016 Report

Cyber Attacks have been ranked as one of the top global threats in The World Economic Forum's (WEF) annual study—The Global Risks Report 2016

The risk of cyber-attacks is ranked highly by the WEF because the organization is concerned that this year, cyber-attacks not only have a strong likelihood of happening, they also have the potential to make a considerable impact.

The report also highlighted the Internet of Things as a major concern related to cyber-attacks. It said:

> *"As the Internet of Things leads to more connections between people and machines, cyber dependency will increase, raising the odds of a cyber-attack with potential cascading effects across the cyber ecosystem….interconnectivity and interdependence can diminish the ability of organizations to fully protect their entire enterprise."*


Natural catastrophes
Biodiversity loss and ecosystem collapse
Food crises
Extreme weather events
Spread of infectious diseases
Man-made environmental catastrophes
Failure of climate-change mitigation and adaptation
Water crises
Failure of critical infrastructure
Failure of urban planning
Profound social instability
Energy price shock
State collapse or crisis
Large-scale involuntary migration
Critical information infrastructure breakdown
Adverse consequences of technological advances
Unmanageable inflation
Interstate conflict
Failure of national governance
Fiscal crises
Asset bubble
Weapons of mass destruction
Unemployment or underemployment
Cyberattacks
Terrorist attacks
Illicit trade
Deflation
Data fraud or theft
Failure of financial mechanism or institution

Source (s): The Global Risks Interconnections Map 2016, WEP The Global Risks Report 2016 11th Edition

Incident Classification Patterns - Verizon's 2015 DBIR

1. Point-of-Sale (POS) Intrusions

POS application/system related attacks

2. Web App Attacks

Web application related stolen credentials or vulnerability exploits

3. Cyberespionage

State-affiliated, targeted attacks

4. Crimeware

Malware used to compromise systems

5. Insider and Privilege Misuse

Unauthorized insider related activity

6. Payment Card Skimmers

Physically installed malicious card readers

7. Miscellaneous Errors

Any mistake that compromises security

8. Physical Theft and Loss

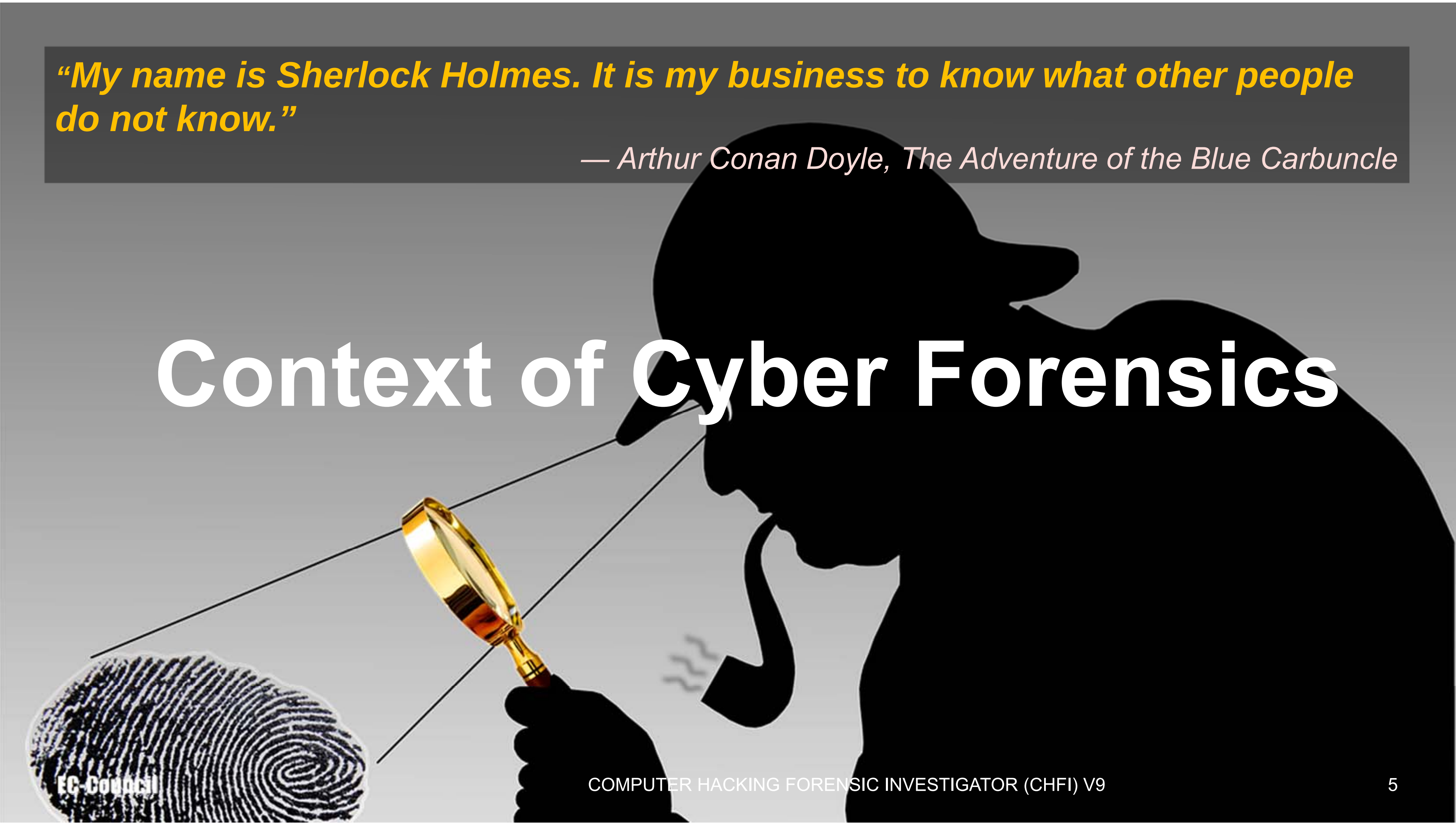
Physical loss or theft of data/IT related assets

9. Denial of Service (DoS) Attacks

Non-breach related attacks affecting business operations

The above exhibit shows the incident classification patterns identified by Verizon's Data Breach Investigations Report (DBIR) 2015 involving confirmed data breaches, in order of frequency, over the past three years.

Source (s): Verizon's 2015 DBIR Report, http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf



“My name is Sherlock Holmes. It is my business to know what other people do not know.”

— Arthur Conan Doyle, The Adventure of the Blue Carbuncle

Context of Cyber Forensics

How is This Different From Ethical Hacking, Penetration Testing, and Network Defense?

ETHICAL HACKING

Hacking performed by an expert to penetrate networks and computer systems with the purpose of finding and fixing security vulnerabilities

PENETRATION TESTING

An attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data

NETWORK DEFENSE

Actions taken via computer networks to protect, monitor, analyze, detect & respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple information systems and networks

DIGITAL FORENSICS

The recovery and investigation of material found in digital devices, often in relation to computer crime

What is Cyber Forensics

It is a branch of forensic science that involves a practice of collecting digital data obtained in the digital devices. It is a task of gathering, **analyzing and preserving the digital data in an acceptable form and can be presented in a court of law.**

Digital Forensic Research Workshop, has defined digital forensic as -

"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and preservation of digital evidence derived from the digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

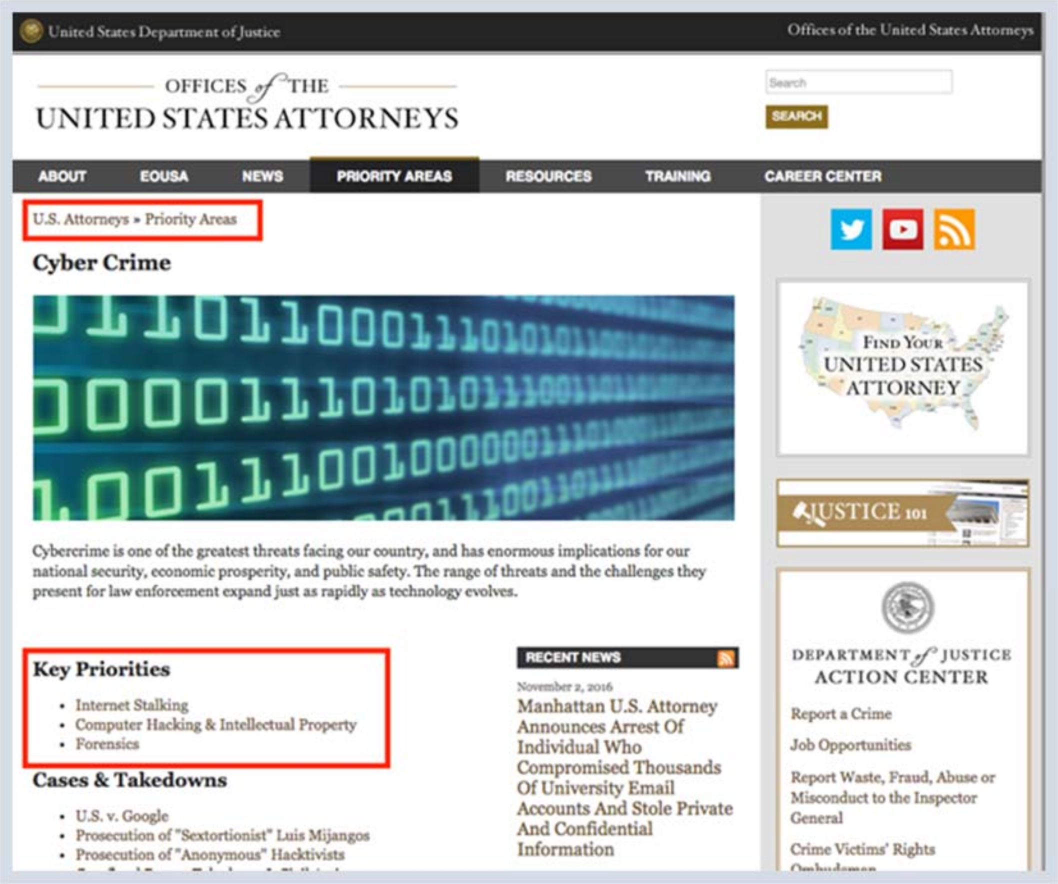
Source (s): DFRWS 2002 USA, https://dfrws.org/sites/default/files/session-files/pres-defining_digital_forensic_examination_and_analysis_tools.pdf

How Forensics Help

- Track and prosecute perpetrators of a cyber crime
- Estimate the potential impact of a malicious activity
- Forensic readiness helps minimize the cost and time to investigate a security incident
- Compliance requirement
- Support in litigations
- Incident response

Forensics is a Key Priority in Fight Against Cybercrimes

Forensics has been cited as a key priority in the fight against cybercrimes by the United States Department of Justice



United States Department of Justice
Offices of the United States Attorneys
OFFICES of THE
UNITED STATES ATTORNEYS
Search
SEARCH
ABOUT
EOUSA
NEWS
PRIORITY AREAS
RESOURCES
TRAINING
CAREER CENTER
U.S. Attorneys » Priority Areas
FIND YOUR UNITED STATES ATTORNEY
JUSTICE 101

Cyber Crime

Cybercrime is one of the greatest threats facing our country, and has enormous implications for our national security, economic prosperity, and public safety. The range of threats and the challenges they present for law enforcement expand just as rapidly as technology evolves.

Key Priorities

- Internet Stalking
- Computer Hacking & Intellectual Property
- Forensics

Cases & Takedowns

- U.S. v. Google
- Prosecution of "Sextortionist" Luis Mijangos
- Prosecution of "Anonymous" Hacktivists

RECENT NEWS

November 2, 2016

Manhattan U.S. Attorney Announces Arrest Of Individual Who Compromised Thousands Of University Email Accounts And Stole Private And Confidential Information

DEPARTMENT of JUSTICE ACTION CENTER

Report a Crime

Job Opportunities

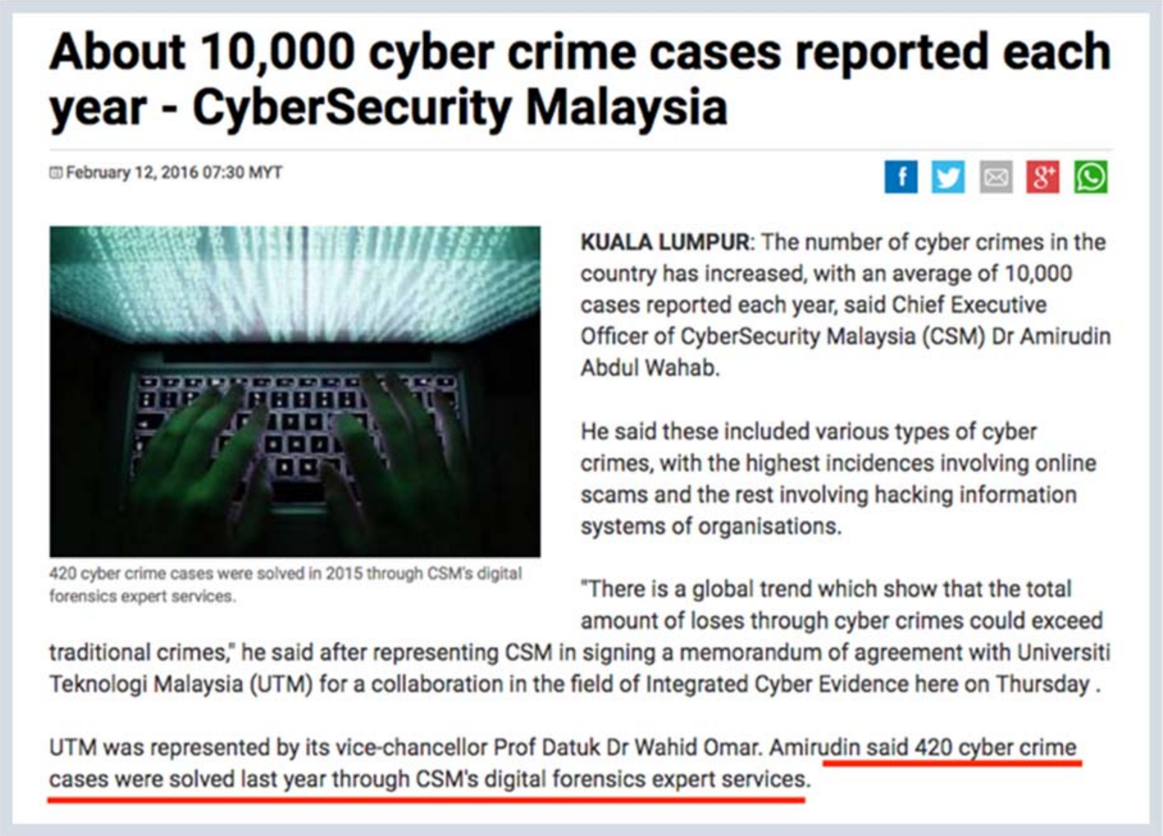
Report Waste, Fraud, Abuse or Misconduct to the Inspector General

Crime Victims' Rights

Source (s): https://www.justice.gov/usao/priority-areas/cyber-crime

Digital Forensics Leads The Fight Against Cybercrime

UTM was represented by its vice-chancellor Prof Datuk Dr Wahid Omar. Amirudin said 420 cyber crime cases were solved last year through CSM's digital forensics expert services.



About 10,000 cyber crime cases reported each year - CyberSecurity Malaysia

February 12, 2016 07:30 MYT

420 cyber crime cases were solved in 2015 through CSM's digital forensics expert services.

KUALA LUMPUR: The number of cyber crimes in the country has increased, with an average of 10,000 cases reported each year, said Chief Executive Officer of CyberSecurity Malaysia (CSM) Dr Amirudin Abdul Wahab.

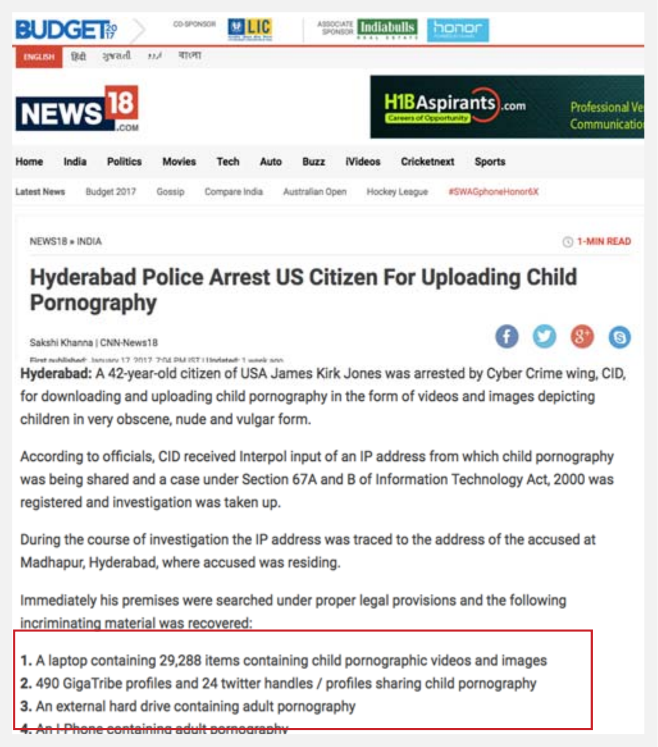
He said these included various types of cyber crimes, with the highest incidences involving online scams and the rest involving hacking information systems of organisations.

"There is a global trend which show that the total amount of loses through cyber crimes could exceed traditional crimes," he said after representing CSM in signing a memorandum of agreement with Universiti Teknologi Malaysia (UTM) for a collaboration in the field of Integrated Cyber Evidence here on Thursday .

UTM was represented by its vice-chancellor Prof Datuk Dr Wahid Omar. Amirudin said 420 cyber crime cases were solved last year through CSM's digital forensics expert services.

Source (s): http://english.astroawani.com/malaysia-news/about-10-000-cyber-crime-cases-reported-each-year-cybersecurity-malaysia-93905

Digital Forensics Leads The Fight Against Cybercrime (Cont'd)


BUDGET 2017
CO-SPONSOR LIC
ASSOCIATE SPONSOR Indiabulls REAL ESTATE
honor
ENGLISH हिंदी ગુજરાતી বাংলা
NEWS18.COM
H1BAspirants.com Careers of Opportunity
Professional Ve Communicatio
Home India Politics Movies Tech Auto Buzz iVideos Cricketnext Sports
Latest News Budget 2017 Gossip Compare India Australian Open Hockey League #SWAGphoneHonor6X

NEWS18 » INDIA

1-MIN READ

Hyderabad Police Arrest US Citizen For Uploading Child Pornography

Sakshi Khanna | CNN-News18

First published: January 17, 2017, 7:04 PM IST | Updated: 1 week ago

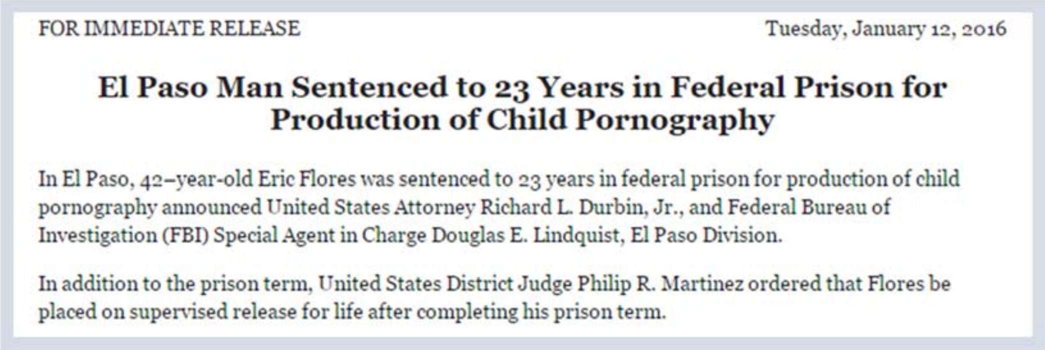
Hyderabad: A 42-year-old citizen of USA James Kirk Jones was arrested by Cyber Crime wing, CID, for downloading and uploading child pornography in the form of videos and images depicting children in very obscene, nude and vulgar form.

According to officials, CID received Interpol input of an IP address from which child pornography was being shared and a case under Section 67A and B of Information Technology Act, 2000 was registered and investigation was taken up.

During the course of investigation the IP address was traced to the address of the accused at Madhapur, Hyderabad, where accused was residing.

Immediately his premises were searched under proper legal provisions and the following incriminating material was recovered:

1. A laptop containing 29,288 items containing child pornographic videos and images
2. 490 GigaTribe profiles and 24 twitter handles / profiles sharing child pornography
3. An external hard drive containing adult pornography
4. An I-Phone containing adult pornography



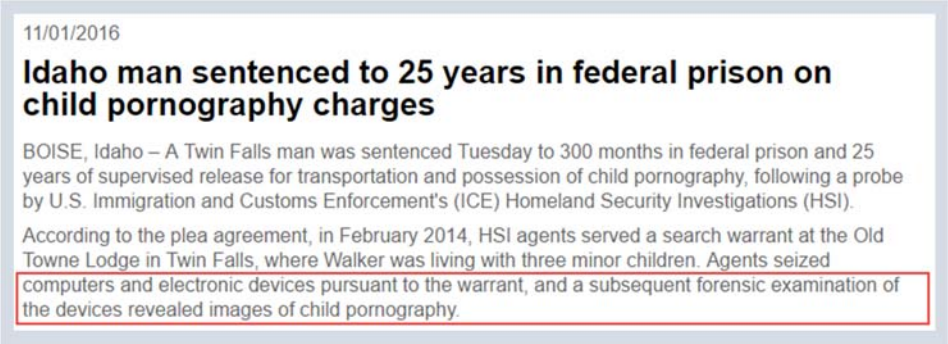
FOR IMMEDIATE RELEASE

Tuesday, January 12, 2016

El Paso Man Sentenced to 23 Years in Federal Prison for Production of Child Pornography

In El Paso, 42–year-old Eric Flores was sentenced to 23 years in federal prison for production of child pornography announced United States Attorney Richard L. Durbin, Jr., and Federal Bureau of Investigation (FBI) Special Agent in Charge Douglas E. Lindquist, El Paso Division.

In addition to the prison term, United States District Judge Philip R. Martinez ordered that Flores be placed on supervised release for life after completing his prison term.



11/01/2016

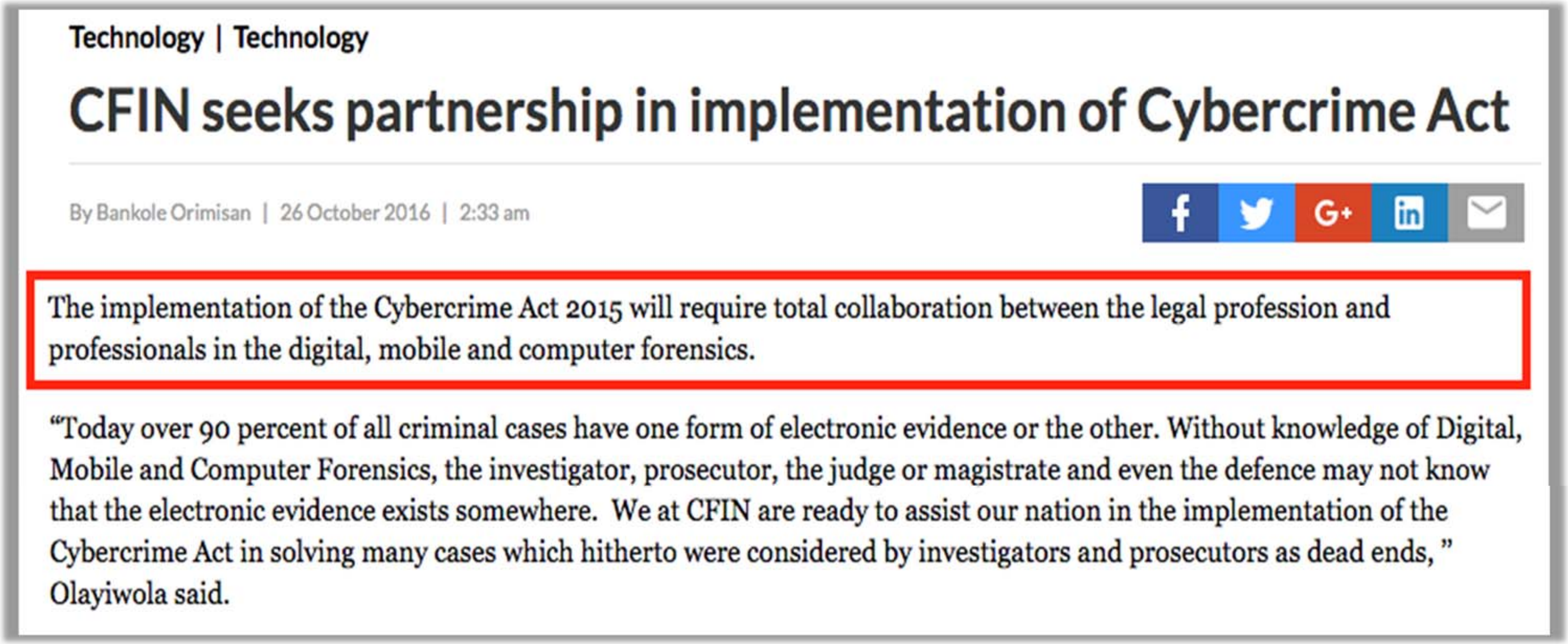
Idaho man sentenced to 25 years in federal prison on child pornography charges

BOISE, Idaho – A Twin Falls man was sentenced Tuesday to 300 months in federal prison and 25 years of supervised release for transportation and possession of child pornography, following a probe by U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI).

According to the plea agreement, in February 2014, HSI agents served a search warrant at the Old Towne Lodge in Twin Falls, where Walker was living with three minor children. Agents seized computers and electronic devices pursuant to the warrant, and a subsequent forensic examination of the devices revealed images of child pornography.

Source (s):
https://www.ice.gov/news/releases/idaho-man-sentenced-25-years-federal-prison-child-pornography-charges,
https://www.justice.gov/usao-wdtx/pr/el-paso-man-sentenced-23-years-federal-prison-production-child-pornography
http://www.news18.com/news/india/hyderabad-police-arrest-us-citizen-for-uploading-child-pornography-1337067.html

90 % of All Criminal Cases Have One Form of Electronic Evidence or The Other



Technology | Technology

CFIN seeks partnership in implementation of Cybercrime Act

By Bankole Orimisan | 26 October 2016 | 2:33 am

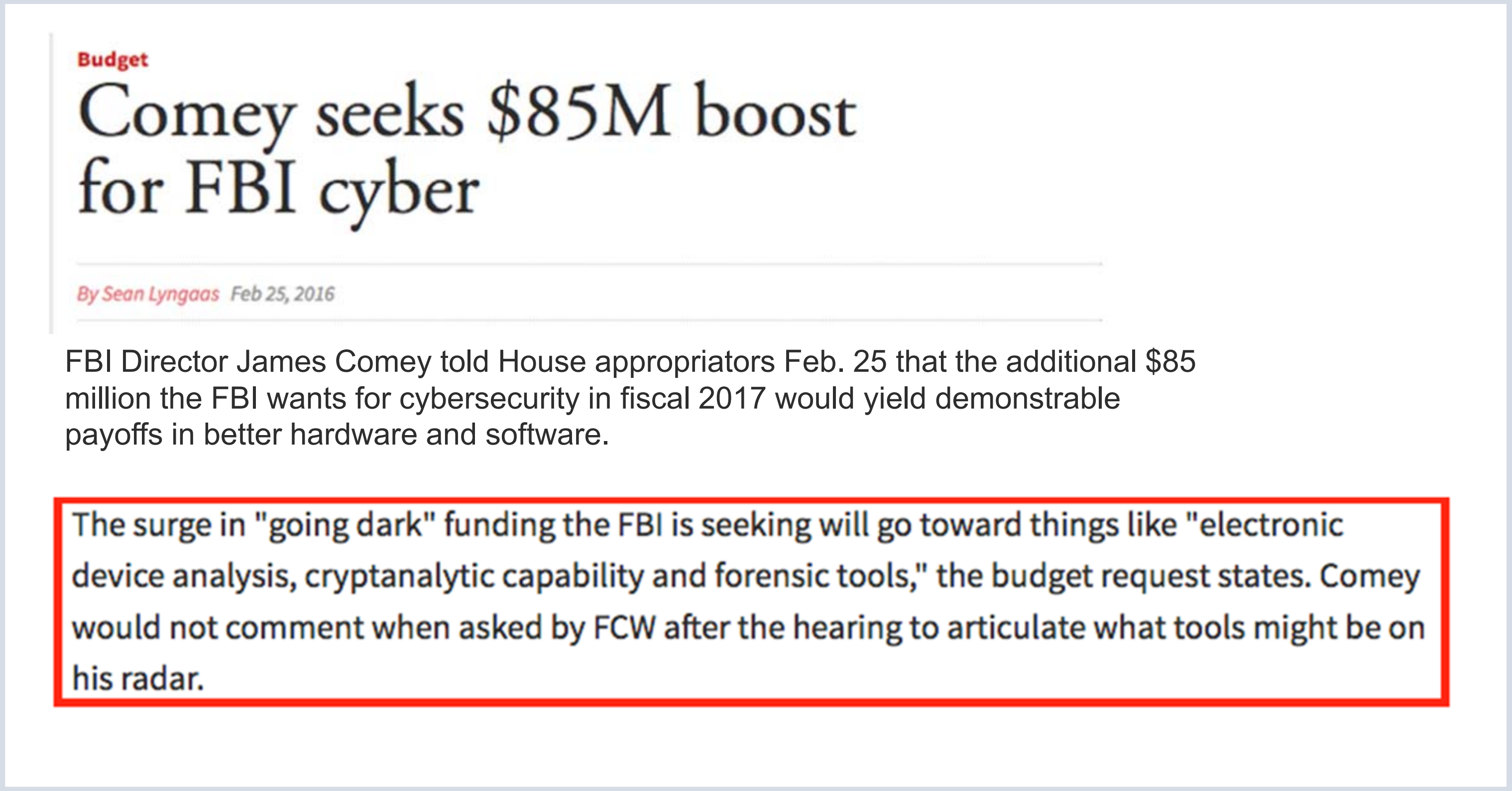
The implementation of the Cybercrime Act 2015 will require total collaboration between the legal profession and professionals in the digital, mobile and computer forensics.

“Today over 90 percent of all criminal cases have one form of electronic evidence or the other. Without knowledge of Digital, Mobile and Computer Forensics, the investigator, prosecutor, the judge or magistrate and even the defence may not know that the electronic evidence exists somewhere. We at CFIN are ready to assist our nation in the implementation of the Cybercrime Act in solving many cases which hitherto were considered by investigators and prosecutors as dead ends, ” Olayiwola said.

Source (s): http://guardian.ng/technology/cfin-seeks-partnership-in-implementation-of-cybercrime-act/

FBI Seeks Funds on Cyber Forensics

FBI been a trendsetter, and others to follow soon..



Budget

Comey seeks $85M boost for FBI cyber

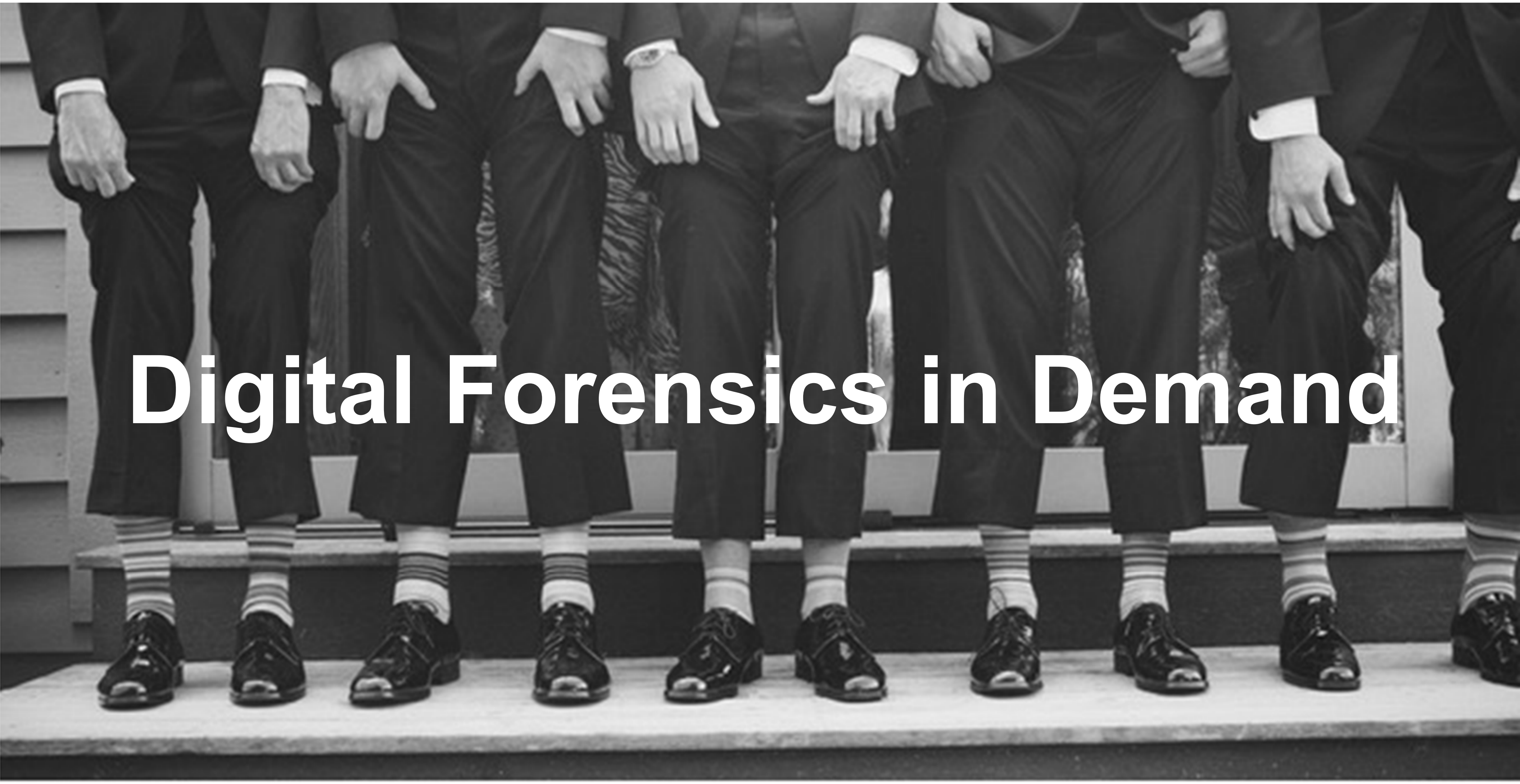
By Sean Lyngaas Feb 25, 2016

FBI Director James Comey told House appropriators Feb. 25 that the additional $85 million the FBI wants for cybersecurity in fiscal 2017 would yield demonstrable payoffs in better hardware and software.

The surge in "going dark" funding the FBI is seeking will go toward things like "electronic device analysis, cryptanalytic capability and forensic tools," the budget request states. Comey would not comment when asked by FCW after the hearing to articulate what tools might be on his radar.

Source (s): https://fcw.com/articles/2016/02/25/fbi-cyber-budget.aspx

Digital Forensics in Demand



Digital Forensics is on The Agenda of Global Leaders

“The rise and rise of cyber-crime” is, even in a climate of political upheaval and social realignment, still a headline-grabber on a regular basis. For example, in the kind of personal scam barely known five years ago, dating fraud increased by 10 percent from 2014 to 2015 and now accounts for around £33 million a year in the UK alone. In one astonishing case, a newly divorced mother signed over £1.6 million in a matter of weeks.

SOURCE: https://fcw.com/articles/2016/02/25/fbi-cyber-budget.aspx

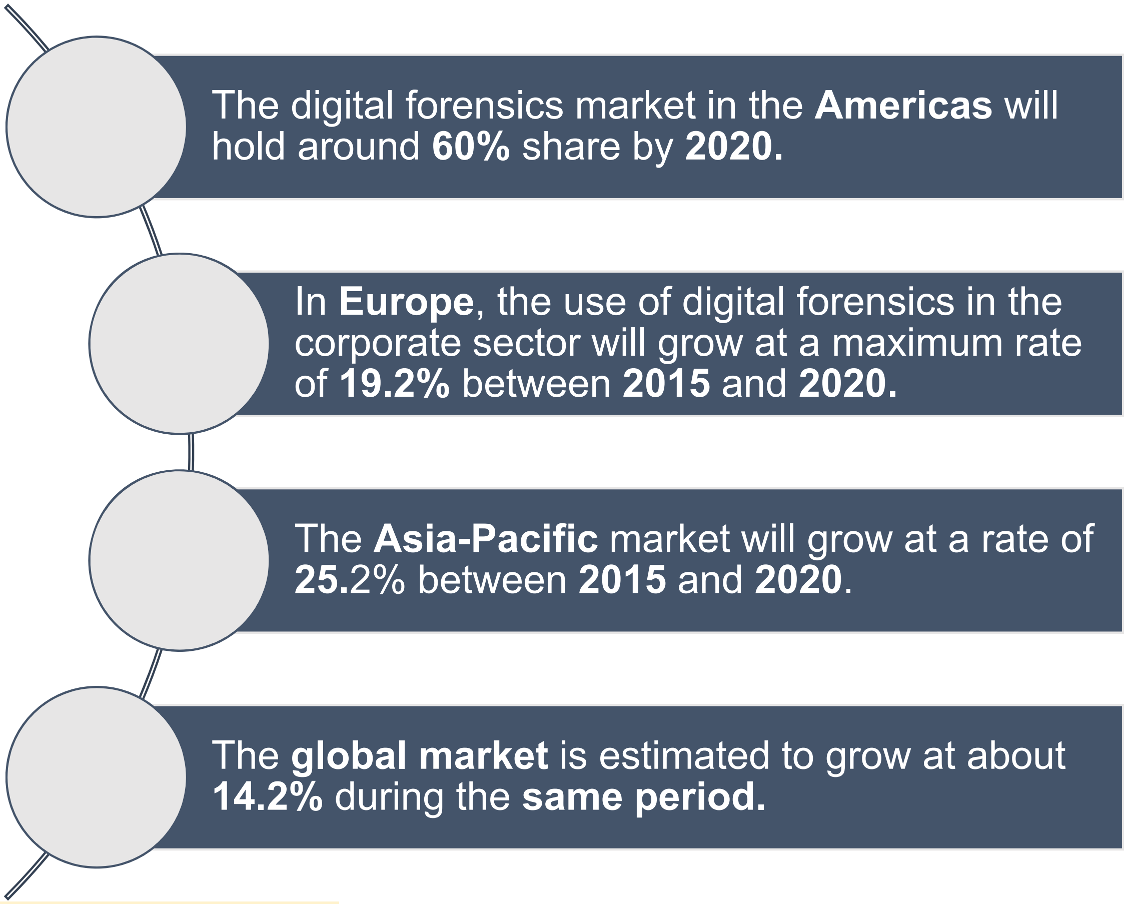
> *“We want… to free up officers' time to focus on the jobs only they can carry out. At the same time, we want to encourage those with **skills** in particular demand, such as those with specialist IT or accounting skills, to **work alongside** police officers to **investigate cyber or financial crime** and help officers and staff fight crime more easily.”*
>
> *– **Theresa May**, Prime Minister of the United Kingdom*

Source (s): http://www.scmagazineuk.com/digital-forensics-leads-the-fight-against-cyber-crime/article/525657

Digital Forensics Market to Hit 4.8 Billion USD in Revenues by 2020

The exponential growth in the volume of data with the proliferation of a wide variety of mobile devices and formats has led to a rise in the use of digital forensics.

According to IndustryARC most of the market growth will occur in the Americas



The digital forensics market in the **Americas** will hold around **60%** share by **2020.**

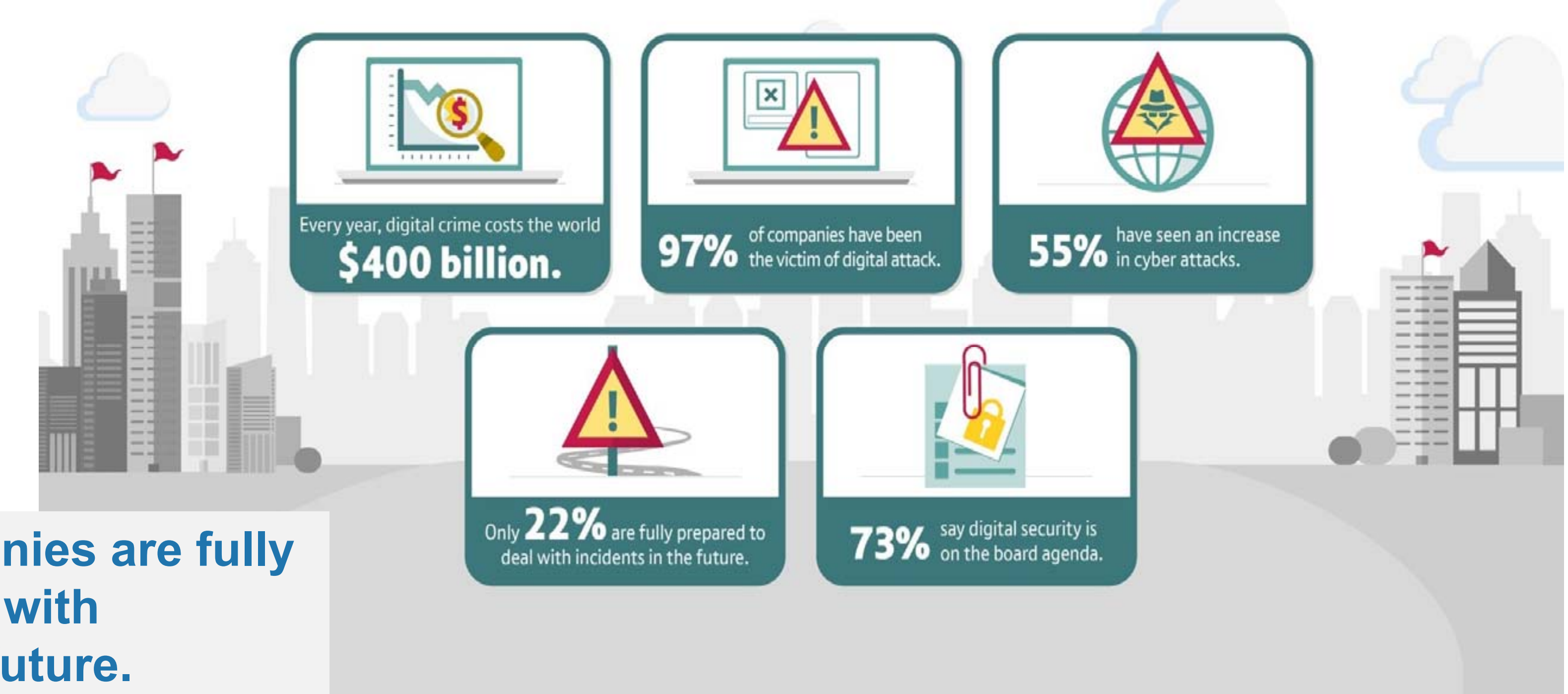
In **Europe**, the use of digital forensics in the corporate sector will grow at a maximum rate of **19.2%** between **2015** and **2020.**

The **Asia-Pacific** market will grow at a rate of **25.**2% between **2015** and **2020**.

The **global market** is estimated to grow at about **14.2%** during the **same period.**

Source (s): http://www.arma.org/r1/news/newswire/2016/03/22/digital-forensics-to-grow-to-$4.8-billion-by-2020

Why is it Gaining Importance?


Every year, digital crime costs the world
$400 billion.
97% of companies have been the victim of digital attack.
55% have seen an increase in cyber attacks.
Only 22% are fully prepared to deal with incidents in the future.
73% say digital security is on the board agenda.

Only 22% companies are fully prepared to deal with incidents in the future. Cyber Crime Hunting and Forensic investigation

Source (s): http://www.globalservices.bt.com/uk/en/point-of-view/disrupting-cyber-crime

About CHFI v9

C|HFI™

Computer Hacking Forensic INVESTIGATOR

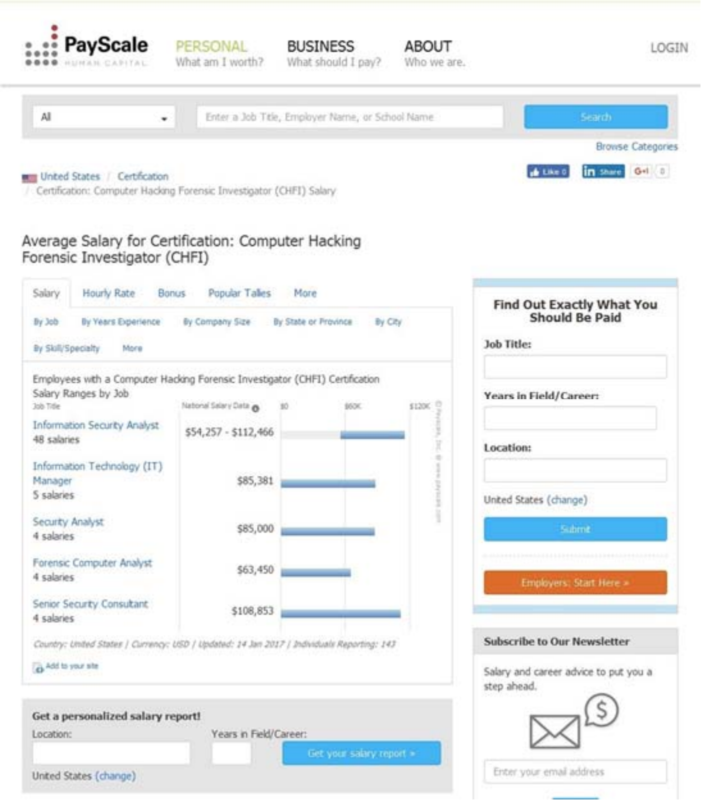
What is CHFI

Computer Hacking Forensic Investigator (CHFI) course will give participants the necessary skills to perform an effective digital forensics investigation

It is a comprehensive course covering major forensic investigation scenarios that enables students to acquire necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carryout a computer forensic investigation leading to prosecution of perpetrators

CHFI presents a methodological approach to computer forensics including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence

CHFI Trends on PayScale



United States / Certification / Certification: Computer Hacking Forensic Investigator (CHFI) Salary

Average Salary for Certification: Computer Hacking Forensic Investigator (CHFI)

Employees with a Computer Hacking Forensic Investigator (CHFI) Certification
Salary Ranges by Job

Job Title	National Salary Data
Information Security Analyst 48 salaries	$54,257 - $112,466
Information Technology (IT) Manager 5 salaries	$85,381
Security Analyst 4 salaries	$85,000
Forensic Computer Analyst 4 salaries	$63,450
Senior Security Consultant 4 salaries	$108,853

Country: United States | Currency: USD | Updated: 14 Jan 2017 | Individuals Reporting: 143

Add to your site

Find Out Exactly What You Should Be Paid

Job Title:

Years in Field/Career:

Location:

United States (change)

Get a personalized salary report!

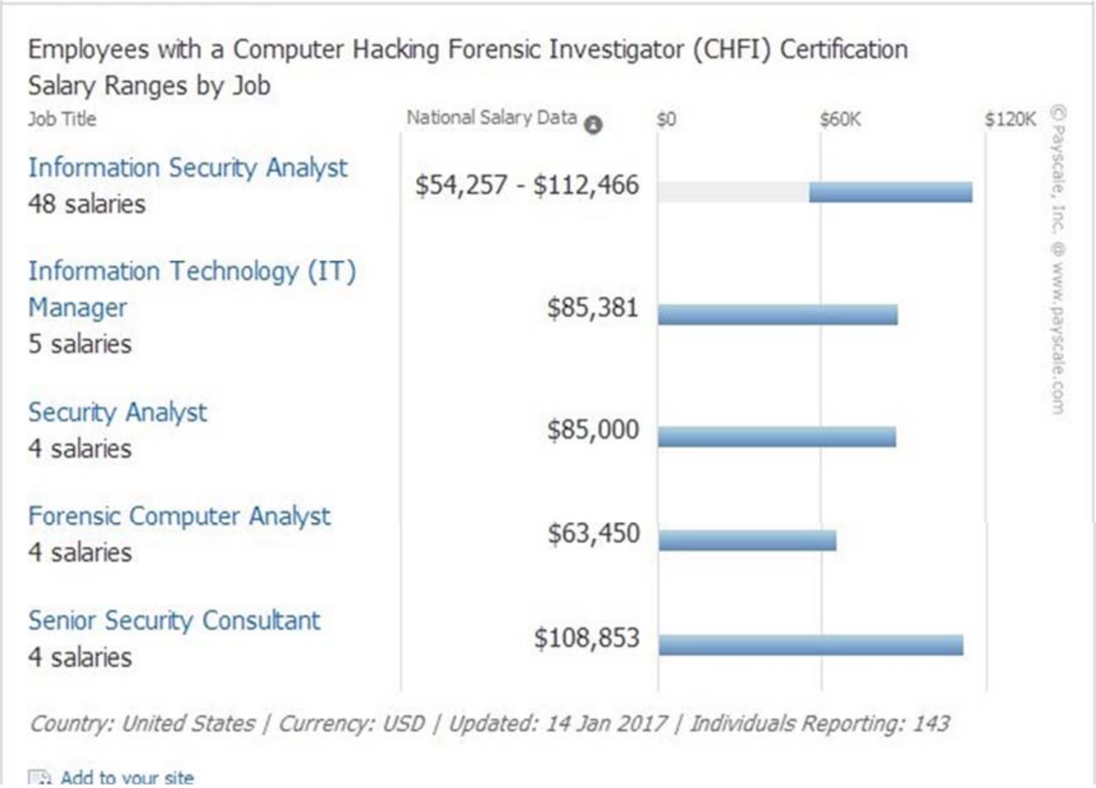
Location:

Years in Field/Career:

United States (change)

Subscribe to Our Newsletter

Salary and career advice to put you a step ahead.



Employees with a Computer Hacking Forensic Investigator (CHFI) Certification
Salary Ranges by Job

Job Title	National Salary Data
Information Security Analyst 48 salaries	$54,257 - $112,466
Information Technology (IT) Manager 5 salaries	$85,381
Security Analyst 4 salaries	$85,000
Forensic Computer Analyst 4 salaries	$63,450
Senior Security Consultant 4 salaries	$108,853

Country: United States | Currency: USD | Updated: 14 Jan 2017 | Individuals Reporting: 143

Add to your site

Source (s): PayScale, http://www.payscale.com/research/US/Certification=Computer_Hacking_Forensic_Investigator_(CHFI)/Salary

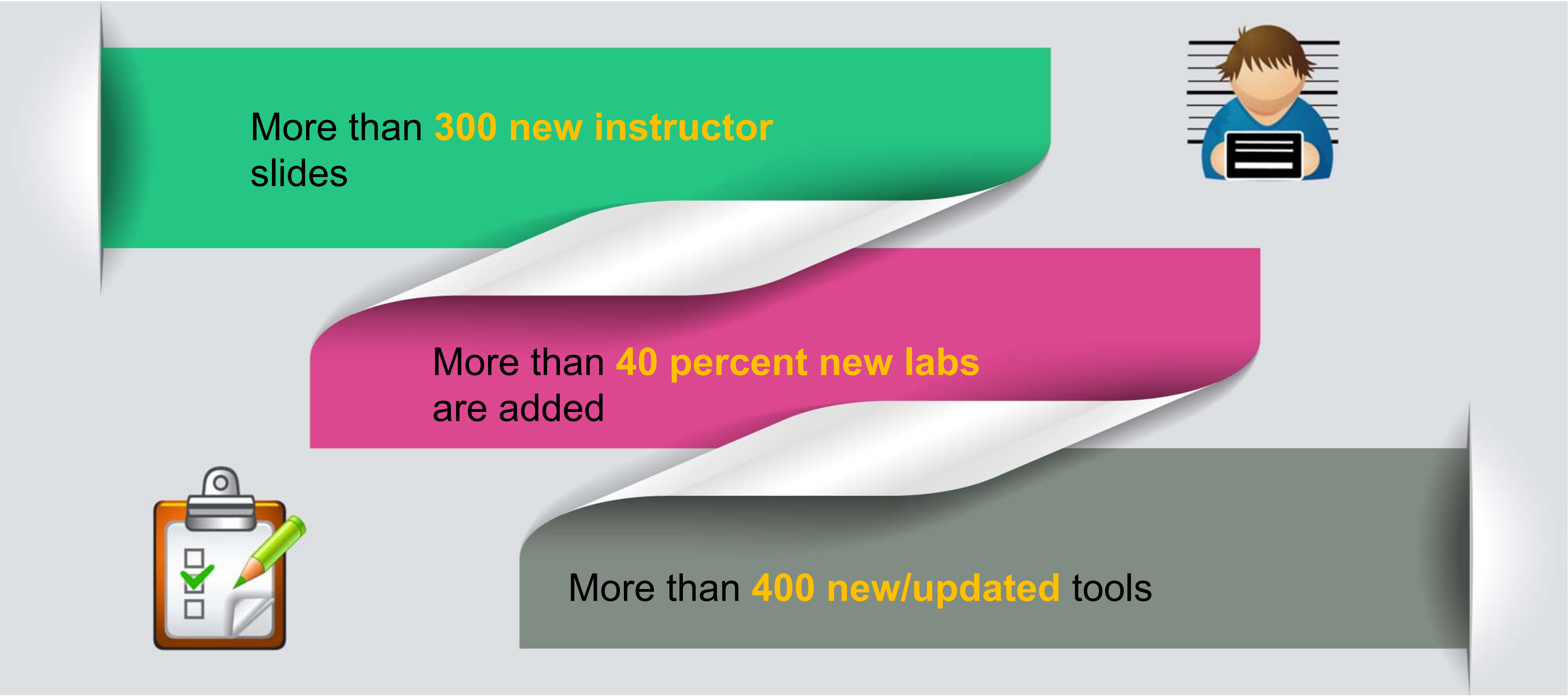
What is New in CHFI v9?

Coverage of latest forensics examination techniques, including Linux and MAC Forensics

Courseware covers Digital Forensics Laws and Standards

Labs on Defeating Anti-forensics Techniques, Database Forensics, Cloud Forensics and Malware Forensics

What is New in CHFI v9?



More than **300 new instructor** slides

More than **40 percent new labs** are added

More than **400 new/updated** tools

Course Outline

1. Computer Forensics in Today's World
2. Computer Forensics Investigation Process
3. Understanding Hard Disks and File Systems
4. Data Acquisition and Duplication
5. Defeating Anti-forensics Techniques
6. Operating System Forensics
7. Network Forensics
8. Investigating Web Attacks
9. Database Forensics
10. Cloud Forensics
11. Malware Forensics
12. Investigating Email Crimes
13. Mobile Forensics
14. Forensics Report Writing and Presentation

CHFIv9 Improvements

CHFIv8	CHFIv9
Module 01: Computer Forensics in Today’s World	Module 01: Computer Forensics in Today's World
Module 02: Computer Forensics Investigation Process	Module 02: Computer Forensics Investigation Process, Module 03: Searching and Seizing Computers, Module 04: Digital Evidence, Module 05: First Responder Procedures, and Module 06: Computer Forensics Lab are merged as Module 02: Computer Forensics Investigation Process as they belong to the same domain
Module 03: Searching and Seizing Computers	
Module 04: Digital Evidence	
Module 05: First Responder Procedures	
Module 06: Computer Forensics Lab	
Module 07: Understanding Hard Disks and File Systems	Module 03: Understanding Hard Disks and File Systems
Module 08: Windows Forensics	Module 06: Operating System Forensics (Added Linux and MAC Forensics in CHFI version 9)
Module 09: Data Acquisition and Duplication	Module 04: Data Acquisition and Duplication
Module 10: Recovering Deleted Files and Deleted Partitions	Module 10: Recovering Deleted Files and Deleted Partitions, Module 13: Steganography and Image File Forensics and Module 14: Application Password Crackers are merged as Module 05: Defeating Anti-forensics Techniques as they belong to the same domain
Module 13: Steganography and Image File Forensics	
Module 14: Application Password Crackers	

CHFIv9 Improvements (Cont’d)

CHFIv8	CHFIv9
Module 11: Forensics Investigation using AccessData FTK	Removed this module
Module 12: Forensics Investigation Using EnCase	Removed this module
Module 15: Log Capturing and Event Correlation	Merged Module 15: Log Capturing and Event Correlation, Module 16: Network Forensics, Investigating Logs and Investigating Network Traffic, and Module 17: Investigating Wireless Attacks as Module 07 Network Forensics as they belong to the same domain
Module 16: Network Forensics, Investigating Logs and Investigating Network Traffic	
Module 17: Investigating Wireless Attacks	
Module 18: Investigating Web Attacks	Module 08: Investigating Web Attacks.
	Module 09: Database Forensics (New Module)
	Module 10: Cloud Forensics (New Module)
	Module 11: Malware Forensics (New Module)
Module 19: Tracking Emails and Investigating Email Crimes	Module 12: Investigating Email Crimes

CHFIv9 Improvements (Cont'd)

CHFIv8	CHFIv9
Module 20: Mobile Forensics	Module 13: Mobile Forensics
Module 21: Investigative Reports	Module 14: Forensics Report Writing and Presentation

IN SUMMARY

CHFIv8	CHFIv9
	Updated information as per the latest developments with a proper flow
	Classroom friendly with diagrammatic representation of concepts and attacks
	New and rich presentation style with eye catching graphics
	Latest OS covered and a patched testing environment
	Well tested, result oriented, descriptive and analytical lab manual to evaluate the presented concepts
22 Modules	14 Modules
42 Labs	39 Labs
2400 Slides	1222 Slides (concise, yet more information has been covered)

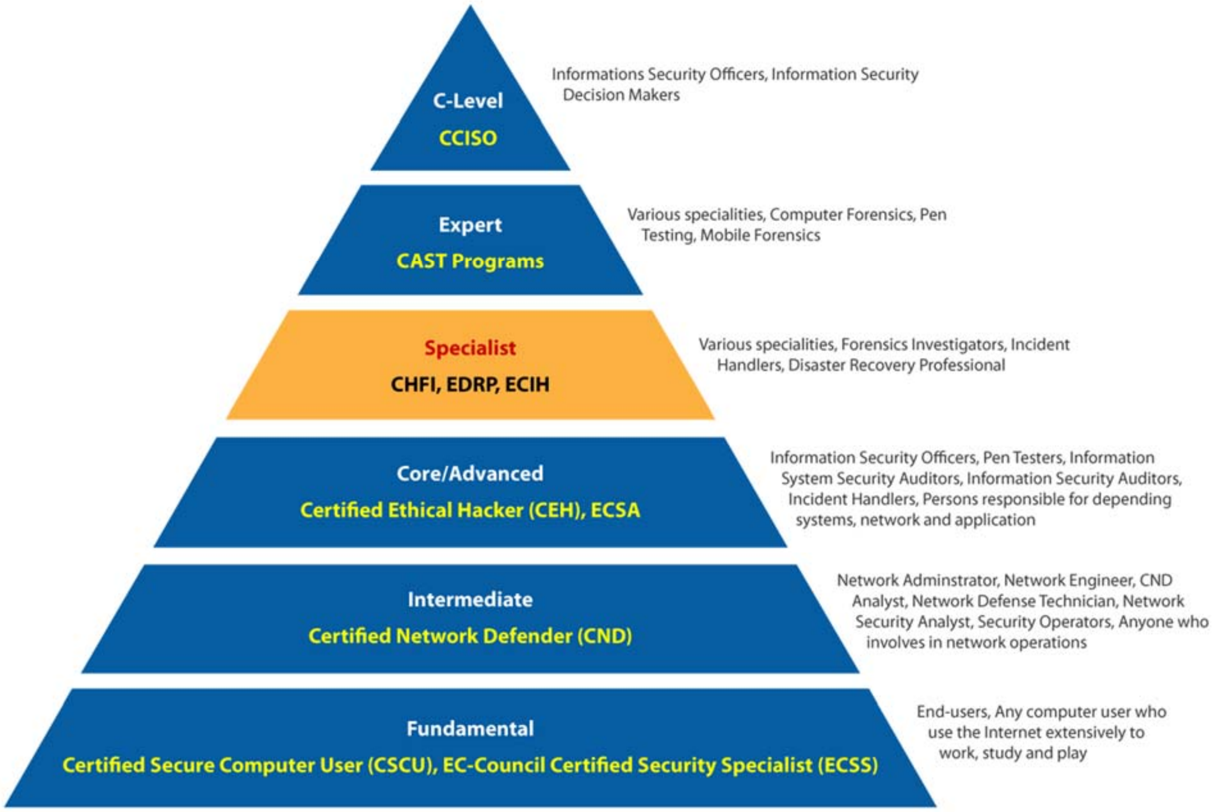
Key Takeaways From CHFI Training

- ☑ Perform incident response and Forensics
- ☑ Perform electronic evidence collections
- ☑ Perform digital forensic acquisitions
- ☑ Perform Bit stream Imaging/acquiring of the Digital Media Seized during the process of Investigation
- ☑ Examine and analyze text, graphics, multimedia, and digital images.
- ☑ Conduct thorough examinations of computer hard disk drives, and other electronic data storage media
- ☑ Recover information and electronic data from computer hard drives and other data storage devices
- ☑ Follow strict data and evidence handling procedures
- ☑ Maintain audit trail (i.e., chain of custody) and/or evidence of integrity
- ☑ Work on technical examination, analysis and reporting of computer based evidence
- ☑ Prepare and maintain case files
- ☑ Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files.
- ☑ Gather volatile and non-volatile information from Windows, MAC and Linux
- ☑ Recover deleted files and partitions in Windows, Mac OS X, and Linux
- ☑ Perform Keyword searches including using target words or phrases
- ☑ Investigate events for evidence of insider threats or attacks
- ☑ Support the generation of Incident Reports and other collateral
- ☑ Investigate and analyze all response activities related to cyber incidents
- ☑ Plan, coordinate and direct recovery activities and incident analysis tasks
- ☑ Examine all available information and supporting evidence or artifacts related to an incident or event
- ☑ Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents
- ☑ Conduct reverse engineering for known and suspected malware files
- ☑ Identify of data, images and/or activity which may be the target of an internal investigation
- ☑ Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event

Key Takeaways From CHFI Training (Cont'd)

- ☑ Establish threat intelligence and key learning points to support pro-active profiling and scenario modeling
- ☑ Search file slack space where PC type technologies are employed
- ☑ File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences
- ☑ Examine file type and file header information
- ☑ Review e-mail communications; including web mail and Internet Instant Messaging programs.
- ☑ Examine the internet browsing history
- ☑ Generate reports which detail the approach and an audit trail which documents actions taken in order to support the integrity of the internal investigation process
- ☑ Recover active, system and hidden filenames with date/time stamp information.
- ☑ Crack (or attempt to crack) password protected files
- ☑ Perform anti-forensic methods detection
- ☑ Execute a file and view the data contents
- ☑ Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures
- ☑ Play a role of first responder by securing and evaluating cyber crime scene, conducting preliminary interviews, documenting crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting of the crime scene
- ☑ Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
- ☑ Apply advanced forensic tools and techniques for attack reconstruction
- ☑ Perform fundamental forensic activities and form a base for advanced forensics
- ☑ Identify & check the possible source / incident origin.
- ☑ Perform event co-relation
- ☑ Extract and analyze of logs from various devices like proxy, firewall, IPS, IDS, Desktop, laptop, servers, SIM tool, router, firewall, switches AD server, DHCP logs, Access Control Logs & conclude as part of investigation process.
- ☑ Ensure reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality.
- ☑ Verify the correctness of the computer's internal clock.
- ☑ Assist in the preparation of search and seizure warrants, court orders, and subpoenas
- ☑ Provide expert witness testimony in support of forensic examinations conducted by the examiner

Where Does CHFI Fits in EC-Council Career Path?



C-Level
CCISO

Informations Security Officers, Information Security Decision Makers

Expert
CAST Programs

Various specialities, Computer Forensics, Pen Testing, Mobile Forensics

Specialist
CHFI, EDRP, ECIH

Various specialities, Forensics Investigators, Incident Handlers, Disaster Recovery Professional

Core/Advanced
Certified Ethical Hacker (CEH), ECSA

Information Security Officers, Pen Testers, Information System Security Auditors, Information Security Auditors, Incident Handlers, Persons responsible for depending systems, network and application

Intermediate
Certified Network Defender (CND)

Network Adminstrator, Network Engineer, CND Analyst, Network Defense Technician, Network Security Analyst, Security Operators, Anyone who involves in network operations

Fundamental
Certified Secure Computer User (CSCU), EC-Council Certified Security Specialist (ECSS)

End-users, Any computer user who use the Internet extensively to work, study and play

Program Details

PREQUISITES

The CHFI course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute

Prerequisites: It is strongly recommended that you attend the CEH class before enrolling into CHFI program.

Duration: 5 days (9:00 – 5:00)

EXAM PATTERN

- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 Hours
- Test Format: MCQ
- Test Delivery: ECC Exam Portal

TARGET GROUP

- Computer Forensic and Intrusion Analyst
- Cyber Forensics Investigator
- Cyber Incident Analyst & Responder
- Defense and Military Personnel
- e-Business Security Professionals
- eDiscovery & Forensics Examiner
- Government Agencies
- Information Security Professionals
- Insurance and other Professionals
- IT Security Managers
- Legal Professionals
- Police and Other Law Enforcement Personnel
- Security and Privacy Consultant
- Security Operations Center (SOC) Personnel
- Systems and Network Administrators

Why CHFI v9

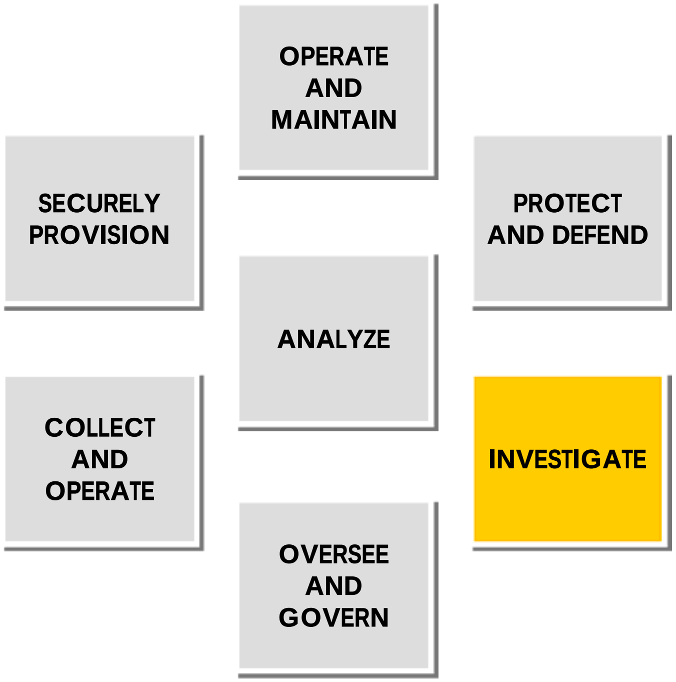
C|HFI ™

Computer Hacking Forensic INVESTIGATOR

Why CHFI

- The program is developed after a thorough Job Task analysis and market research
- It is designed and developed by experienced SMEs and digital forensics practitioners
- A complete vendor neutral course covering all major forensics investigations technologies and solutions
- Detailed labs for hands-on learning experience; approximately 50% of training time is dedicated to labs
- It covers all the relevant knowledge-bases and skills to meets with regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- More than 30 GB of digital forensics and evidence analysis tools
- The student kit contains large number of white papers for additional reading
- The program presents a repeatable forensics investigation methodology required from a versatile digital forensic professional which increases your employability
- The student kit contains many forensics investigation templates for evidence collection, chain-of-custody, final investigation reports, etc.
- The program comes with cloud-based virtual labs enabling students to practice various investigation techniques in a real time and simulated environment

CHFI Maps to NICE Framework



Compliance with National Initiative for Cybersecurity Education (NICE) “Investigate” specialty area

Individual working under this specialty area holds following job titles:

- Computer Forensic Analyst
- Computer Network Defense (CND) Forensic Analyst
- Digital Forensic Examiner
- Digital Media Collector
- Forensic Analyst
- Forensic Analyst (Cryptologic)
- Forensic Technician
- Network Forensic Examiner
- Computer Crime Investigator
- Special Agent

EC-Council Strong Cyber security Domain Experience

- EC-Council is one of the largest information security training provider
- EC-Council's courses are **delivered with a strong emphasis of hands on techniques** that will enable you to apply what you have learnt as soon as you complete your class
- CHFIv9 is a **comprehensive course** covering all possible forensic investigation scenarios that enables students to acquire necessary hands-on experience on various forensic investigation techniques and standard **forensic tools necessary to successfully carryout a computer forensic investigation** leading to prosecution of perpetrators
- EC-Council's courseware's are **developed by subject matter experts** from all over the world and are constantly updated to ensure that you are exposed to the latest advances in the space
- EC-Council's courses feature some of the best names in the **infosec world**. The EC-Council Master trainers are all practitioners and experts in their field
- EC-Council's courses are extremely advanced and can be **delivered in a number of formats** including, **Live**, **Online**, **Instructor Led**, **Custom Classes**, **Blended Learning** and much more
- EC-Council's courses have attained the world renowned **CNSS 4011 – 4016 Certification** from the US National Security Council

Endorsements

EC-Council's CHFI courseware was certified to have met the 4012 (Senior System Managers) training standards for information security professionals in the federal government by the United States National Security Agency (NSA) and the Committee on National Security Systems (CNSS)

CHFI programs have been accepted into National Infocomm Competency Framework (NICF) Infocomm professionals competency requirement list

The Department of Veterans Affairs has included CHFI under its GI Bill for the reimbursement of test fees for veterans and other eligible persons in accordance with the provisions of PL 106-419

The Malaysian Military Cyber Security Warfare Department (KOMLEK) has stipulated their military professionals to be CHFI Certified as part of their Cyber Warfare Training Program (CPS)

Testimonials

"It is my pleasure to take the time to praise the EC Council for having such a magnificent class, specifically THE Computer Hacking Forensic Investigator course. The course had an abundance of information, utilities, programs, and hands on experience. I am a consultant at Dell and we do have a lot of technical training, but I must comment that this one is one of the best trainings I have seen in several years. I will definitively recommend this course to all my colleagues."

Hector Alvarez, CHFI, Enterprise & Storage Consultant, DELL Corporation, Austin, Texas

" All the treatment has been excellent, the material and the content of the course overcomes my expectations. Thanks to the instructor and to Itera for their professionalism."

Sergio Lopez Martin, CHFI, Security Sales, IBM, Spain

" CHFI is a certification that gives an complete overview of the process that a forensic investigator must follow when is investigating a cybercrime. It includes not only the right treatment of the digital evidence in order to be accepted in the Courts but also useful tools and techniques that can be applied to investigate an incident."

Virginia Aguilar, CHFI,KPMG, Madrid

" The CHFI training and certification was very important as it gives a structure and form of the skills and knowledge which I developed and acquired through the years. On the other side this certification helps our company and team to build trust in our customers. The qualification which I attain through CHFI certification was of big importance to establish our team by raising the performance and the quality of the delivered service."

Victor Tashev, HP Enterprise Security Services

" The Computer Hacking Forensic Investigator (CHFI) certification has been instrumental in assuring both my company and our clients that my skillset is among the elite in the cyber security and response profession. The CHFI allows my company to readily identify to our DoD clients that our team is trained to perform the rigorous functions required of cyber threat response team. Our company can now better brand our capability to investigate cyber security incidents, perform computer/malware forensic analysis, identify active threats, and report our findings."

Brad W. Beatty, Cyber Security Analyst, Booz Allen Hamilton, USA

EC-Council

C|HFI Computer Hacking Forensic INVESTIGATOR™