

# RE: Spam: RE: Forensic/Cyber Crime Investigator

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-02/msg00117.html>

---

- *From:* "dave kleiman" <dave@xxxxxxxxxxxxxxxx>
  - *Date:* Tue, 7 Feb 2006 09:00:24 -0500
- 

Craig,

A. Information Technology Forensics defined: IT forensics is the practice of investigating electronic systems, devices, and media for the purpose of discovering and analyzing available information that may serve as useful evidence.

B. IT Forensics is an investigation process that is rapidly becoming a field in its own, it is the process of identifying, preserving, and analyzing electronic data in a forensically sound manner, conducting examinations within the constraints of local law, in a reproducible manner, and compiling the results in such a way as to withstand courtroom scrutiny.

C. Investigations are the systematic and thorough gathering, examining, and studying of factual information that results in the factual explanation of what transpired.

D. Forensics Management is defined as those concepts and principles that information security professionals (i.e., CISSPs) need to know in order to successfully participate in a forensics-related event.

A. What makes up a good Forensic Incident Response team?

i. The Incident Response Teams may well have to act in a forensically sound manner when performing their duties. This may not necessarily require a second, separate Incident Response team, from one that may well already be in place to address non-forensic security issues.

B. The team should include representatives from legal counsel and Human Resources. They should be consulted on all policies and procedures before implementation. Additionally, their expertise will be invaluable once the data is collected and examined.

A. Electronic Discovery defined: ?The process of identifying, locating, securing and producing electronic data for evidence in litigation. Also called: Electronic Evidence Discovery, eMail Evidence Discovery, Electronic-discovery, eMail Search and Discovery, Email Discoverability, Content Discovery, Electronic Content Discovery, Electronic Evidence,

RE: Spam: RE: Forensic/Cyber Crime Investigator

Computer-based Discovery, Legal Discovery, Electronic Data Discovery, e-Mail Discoverability, Electronic Data Management, eDiscovery, Digital Evidence Discovery, Enterprise Search and Discovery, EDD, e-Discovery, Digital Discovery, Electronic Information Discovery, Digital Evidence, and Electronic Document Discovery.?

<http://www.bitpipe.com/tlist/Electronic-Discovery.html>

B. Evidence defined: All the means by which any alleged matter of fact, the truth of which is submitted to investigation at judicial trial, is established or disproved. Evidence includes the testimony of witnesses, introduction of records, exhibits, objects or any other probative matter offered for the purpose of inducing belief in the party's contention by the fact-finder.

C. It is best practice to treat all cases as they may end up in litigation. Therefore, we should ensure our evidence follows the rules of evidence.

Now that we all proved we now how to use a dictionary, an Incident Response team MUST act in a forensically sound manner and be made up of Forensic Investigators. This is particularly true in the First Responder team, where the Forensic Investigator decides the persons and procedures for the particular incident.

Respectfully,

---

Dave Kleiman, CAS,CCE,CIFI,CISM,CISSP,ISSAP,ISSMP,MCSE

<http://www.davekleiman.com/about.php>

-----Original Message-----

From: Craig Wright [<mailto:cwright@xxxxxxxxxxxxxx>]

Sent: Monday, February 06, 2006 17:00

To: Craig Wright; Robinson, Sonja;

security-basics@xxxxxxxxxxxxxx

Subject: RE: Spam: RE: Forensic/Cyber Crime Investigator

Hello,

Just to be particularly annoying...

Forensic 1. relating to, connected with, or used in courts of law or public discussion and debate.

RE: Spam: RE: Forensic/Cyber Crime Investigator

RE: Spam: RE: Forensic/Cyber Crime Investigator

2. adapted or suited to argumentation; argumentative.
3. applied to the process of collecting evidence for a legal case: forensic accounting; forensic archaeology; forensic linguistics. [Latin forens(is) of the forum + -IC] ---forensically, adverb

Just to reiterate. Forensic = court. Incident response is the correct terminology that most people are in all actuality coming to the belief to be forensics.

Regards  
Craig

-----Original Message-----

From: Craig Wright Sent: 7 February 2006 8:51  
To: 'Robinson, Sonja'; security-basics@xxxxxxxxxxxxxxxxxxxx  
Subject: RE: Spam: RE: Forensic/Cyber Crime Investigator

Hello,

There is a confusion between forensic analysis and incident response.

Although these are related and in fact many people do both, they are not the same. Incident response teams or personal are needed in many organisations. Having a good investigative team makes life easier for a forensic analyst.

They are however different roles. Oft the roles will overlap, but the primary focus of forensics is obtaining and preserving evidence. This may go against a corporations aims to have production systems running as soon as possible.

I am not talking of LE at all. Rather I am stating insolvency support, litigation support, etc.

Network security does not mean knowing where to look for logs. This is a technical skill. Again a case where people get the more esoteric nature of the role confused with the technical skills.

Very few people can investigate a hard drive in a manner that is acceptable without challenger in court. This is the role of forensics.

General investigation is a role in incident response.

I am sure that this will garnish further comment – but I am a purist when it comes to definitive terminology. Incident response and Forensics are separate (though related disciplines). Most of the comments are asking about the former though stating them as the latter.

Regards

RE: Spam: RE: Forensic/Cyber Crime Investigator

Craig

-----Original Message-----

From: Robinson, Sonja [<mailto:SRobinson@xxxxxxxxxxx>]

Sent: 7 February 2006 1:51

To: Craig Wright; security-basics@xxxxxxxxxxxxxxxxxxxx

Subject: Spam: RE: Forensic/Cyber Crime Investigator

I'm Sorry but I have to disagree with some of your statements while I agree with some others.

1) Many corporations in the US and around the world are hiring EXPERIENCED forensic personnel. I have worked as a consultant and for private companies doing forensics for over 8 years now. My start was private. I have never been "employed" by LE however, I have been hired by govts/military for jobs. You can start entry level Info Security and get trained by one of their staff if they feel you are up to the challenge. I am training a few co-workers myself and am helping them on the career path. Why corporate? Espionage, sexual harrasment, porn, assault/murder, hacking/incident response, identity theft, HIPAA/SOX, resource abuse, etc. etc. Believe me, there's plenty of work on the corporate side – you don't have to go LE if you don't want to. That's just the tip of the iceberg. You must assume that your cases will go to court, especially if employees are terminated as a result of your investigation. Sometimes you work hand in hand with LE. You can get more than they can until you become their agent for internal investigations. But that's where you need ot know the law aspect.

Sometimes you need their assistance with items such as subpoenas, etc.

Also with the Calif law that is being adopted throughout the US, you will be working with LE for disclousres.

2) Network security is essential if you want to perform and investigation. How will you know where to look, what logs to obtain, etc. You must also know the law in the country, states and other jurisdictions that the case involves (i.e subpoena in another state/country). Nothing personal but with the right tools, most anyone can investigate a hard drive although they will most likely screw up the acquisition, chain of custody and legal aspects thereby nullifying their review. Point being, it takes a lot of training and experience and if you can't find your way around a network you;ve got no business doing an investigation because you will only be looking at a small part of the picture in many cases. 3) There is no "one" certification. There are ones that are more common, advisable etc. but there is no one stop shopping.

4) I agree with everything up to the "after incident response". This is because, IT people will most likely trample your evidence. Ideally you should be preserving evidence while they correct a problem so it should be in tandem. Of course, many times it does occur after IT has responded and corrected an issue. Your company should make a decision beforehand whether their primary goal is recovery, forensics or both.

The answer will vary by system, issue, etc.

5) There are classes you can take, some proprietary/some not. There are many groups you can join to learn if you are truly interested. The job can be boring and monotonous (i.e. Log reading and correlation) but it's also a lot of fun. It's a big game of hide and seek and I think it's a blast. It's never the same and you find out a lot about people.

6) I totally agree with pretty much every other statement of Craig's.

It's work, it's integrity, it's honesty, a lot of good communication skills, a knowledge of law, operating systems, networking, incident response and recovery, network security, cryptography/steganography, and the ability to think like criminals/abusers without actually being one.

You must also remember that you can not speculate. You present facts.

7) Forensics is a science of processes. It deals in facts. There ARE a lot of people and products who purport to be "forensics" but are not and are well, we'll just say, "not able to present or be presentable" in court for a number of reasons.

Sonja L. Robinson, CISSP, CIFI, CISA, CISM Forensic Specialist, Digital Investigations HIP Information Security Group  
Tel: 212-806-4125  
srobinson@xxxxxxxxxx

-----Original Message-----

From: Craig Wright [<mailto:cwright@xxxxxxxxxxxxxx>]  
Sent: Thursday, February 02, 2006 5:22 PM  
To: security-basics@xxxxxxxxxxxxxxxxxxxx  
Subject: RE: Forensic/Cyber Crime Investigator

First, Computer Forensics is a separate discipline to Computer Security.

Next, incident response in business is not generally about forensics nor does it have a lot to do with it.

Other than a low level knowledge of systems (and forget

the tools based

– Encase training only – approach). A strong knowledge of law is required.

Your job/role as a forensic services provider (of any type) is to provide court support. This is it – full stop.

Your job is;

- 1 Investigate. Document Preserve the "chain of evidence",
- 2 Document everything. This is for and against. You have to be impartial.
- 3 Be prepared to sit in court and have your life, experience and training picked apart.
- 4 Answer the facts simply and succinctly, no more, no less. What you are asked you answer. Your opinion only comes into this when and IF your have been directly asked.

The role is slow and methodological. If you think accounting and being an auditor is fun, than you may fit into the role.

Complete some courses in English grammar and report writing. This is an essential skill. Spelling and punctuation can make or break your career in this field.

Forensics has NOTHING to do with detection of an attack. It comes after the attack. It comes after the initial incident response process.

Knowledge of incident response is needed to ensure the "chain of evidence", but it is not generally part of your role as a forensic analyst.

SANs GCFA is a good preliminary as is CCE. Neither will make you more than an intern level by itself. You will be judged (at more than an intern level) on how you handle cases. How you respond in court. Many prospective employers will expect to view transcripts of cases you have been involved with to see how you handle under cross.

You want to be top of the field. Many years. Much training. Calm demeanour. Honesty. Integrity. This is the simple answer. There is a great deal more as well. You need at least knowledge of the law (a degree is not necessary, but does help. This is how experience as an officer of the law aides). Absolutely NO knowledge of information security is required (in contradiction to popular belief). It does help.

Familiarity of file-systems is crucial. Learn both Linux and Windows at the least. Understand how to create a timeline. Know how to extract and analyse slack space

RE: Spam: RE: Forensic/Cyber Crime Investigator

while maintaining evidential integrity. These are some of the required skills (tip of the iceberg).

There are many people who profess to have computer forensic skills. There are very few who really have these skills. There are even fewer who can use their skills in court.

Regards  
Craig

Dr Craig S Wright DTh MNSA MMIT CISA CISM CISSP ISSMP ISSAP  
G7799 GCFA AFAIM Manager – Computer Assurance Services BDO  
Chartered Accountants & Advisers Level 19, 2 Market  
Street, Sydney, NSW 2001  
Telephone: +61 2 9286 5555  
Fax: +61 2 9993 9705  
Direct: +61 2 9286 5497  
<[Mailto:CWright@xxxxxxxxxxxxxx](mailto:CWright@xxxxxxxxxxxxxx)>

-----Original Message-----

From: mhayden [[mailto:mike\\_hayden@xxxxxxxxxxxxxx](mailto:mike_hayden@xxxxxxxxxxxxxx)]

Sent: 2 February 2006 7:46

To: security-basics@xxxxxxxxxxxxxxxxxxxxxx

Subject: RE: Forensic/Cyber Crime Investigator

Koolk3,

I am also looking into this, I don't have much information but this is what I've gathered:

- There seem to generally be 2 facets of Forensics:
  - \* Computer Forensics – pouring over someone's harddrive to gather and document evidence.
  - \* Network Forensics – Alot of what the folks on this list do on a day to day basis, intrusion protection, detection and analysis.

You can persue one or the other but it sounds like you want a combination of both.

- It has been suggested to me that if I was interested I should persue a Law Enforcement career and go at it from that angle. I have been a Software developer for almost 20 years, in the US I'm too old for Law Enforcement (35 yrs is the cutoff in my state) so that option is out for me.

- Another suggestion was the FBI or CIA as a civilian

RE: Spam: RE: Forensic/Cyber Crime Investigator

RE: Spam: RE: Forensic/Cyber Crime Investigator

professional or if you meet the age/citizenship criteria an Agent.

– There are also private companies that do Computer Forensics and are hired out by Lawyers or Law Enforcement that need the help when computers are acquired in crimes.

I have taken a Computer Forensics class at the college level to get a feel for that but unfortunately that isn't enough to get you in the door (unless you get lucky). I also get the feeling that without an IT background you are out in the cold.

Another suggestion was to join one of the local chapters of the IACIS (International Association of Computer Investigative Specialists). I think you would need to be invited in by an existing member and I'm not sure if its only open to Law Enforcement folks checkout there website (<http://www.iacis.info/iacisv2/pages/home.php>). There are many different groups, some are open to civilians and some are not.

Hope this helps a bit. I look forward to comments from others to help me in my quest also.

MH

-----Original Message-----

From:  
security-basics-return-38141-mike\_hayden=quintum.com@securityfocus.com  
[\[mailto:security-basics-return-38141-mike\\_hayden=quintum.com@securityfocus.com\]](mailto:security-basics-return-38141-mike_hayden=quintum.com@securityfocus.com)On Behalf Of Koolk3  
Sent: Wednesday, February 01, 2006 12:21 PM  
To: security-basics@xxxxxxxxxxxxxxxxxxxxx  
Subject: Forensic/Cyber Crime Investigator

Hi List,

I tried posting this before, didn't go through. So I am trying again.

I am interested in becoming a Forensics/Cyber Crime Investigator preferably with any law enforcement agency in Canada. I will graduate this April with a Bachelor in Computer Engineering. I have some experince in Forensics and IT security from coop placements and wanted to take this option as a career.

RE: Spam: RE: Forensic/Cyber Crime Investigator

My questions are:

- 1) What kind of certification is the most demanding/respected among law enforcement agencies in Canada/US?
- 2) If anyone on the list is with RCMP, OPP or any other law enforcement agency here could you please give me any information on a possible career path. Where do I start? Are these kind of jobs considered as a civilian job?
- 3) Those in the USA: could you please tell me if I can have any prospect there as a Canadian citizen. I would imagine you would need an US citizen to work in the law enforcement agencies, but what about private organizations?
- 4) Any information in building a career path in this field would be helpful.

Thanks everyone.

---  
KoolK3

-----  
-----  
---  
**EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE**

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>

-----  
-----  
---  
**EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE**

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>

-----  
-----  
-----

Liability limited by a scheme approved under Professional Standards Legislation in respect of matters arising within those States and Territories of Australia where such legislation exists.

**DISCLAIMER**

The information contained in this email and any attachments is confidential. If you are not the intended recipient, you must not use or disclose the information. If you have received this email in error, please inform us promptly by reply email or by telephoning +61 2 9286 5555. Please delete the email and destroy any printed copy.

Any views expressed in this message are those of the individual sender.  
You may not rely on this message as advice unless it has been electronically signed by a Partner of BDO or it is subsequently confirmed by letter or fax signed by a Partner of BDO.

BDO accepts no liability for any damage caused by this email or its attachments due to viruses, interference, interception, corruption or unauthorised access.

-----  
-----  
-----

**EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE**

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience. Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity

RE: Spam: RE: Forensic/Cyber Crime Investigator

Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>

---

Liability limited by a scheme approved under Professional Standards Legislation in respect of matters arising within those States and Territories of Australia where such legislation exists.

**DISCLAIMER**

The information contained in this email and any attachments is confidential. If you are not the intended recipient, you must not use or disclose the information. If you have received this email in error, please inform us promptly by reply email or by telephoning +61 2 9286 5555. Please delete the email and destroy any printed copy. Any views expressed in this message are those of the individual sender. You may not rely on this message as advice unless it has been electronically signed by a Partner of BDO or it is subsequently confirmed by letter or fax signed by a Partner of BDO.

BDO accepts no liability for any damage caused by this email or its attachments due to viruses, interference, interception, corruption or unauthorised access.

---

**EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE**

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>

---

---

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>

---