Steve Watson

Digital Forensics and the Intersection with Spectrum Forensics

Steve Watson, VTO Labs

ISART 2016, Westminster, CO

Digital Forensics and the Intersection with Spectrum Forensics

Steve Watson, VTO Labs

ISART 2016, Westminster, CO

Steve Watson

- technologist
- digital forensics researcher
- new technology evangelist
- information security background
- digital forensics PhD student
- Principal - VTO Labs

VTO Labs

Organization of OSAC Scientific Area Committees for Forensic Science

NIST National Institute of Standards and Technology U.S. Department of Commerce


FORENSIC
SCIENCE

What is Forensic Science?

forensis:

public, to the forum or public discussion; argumentative, rhetorical, belonging to debate or discussion.

Forensic science is the application of sciences such as physics, chemistry, biology, computer science and engineering to matters of law.

ref: DOJ-NIJ

History of Forensic Science

700 AD - Chinese use fingerprints to identify documents and clay sculptures

1000 - Roman courts, bloody palm prints meant to frame a blind man

1609 - France, first treatise on systematic document examination

1784 - England, John Toms q convicted of murder on the basis of the torn edge of wad of newspaper

1835 - London, first bullet comparison to catch a murderer

reference:
Principles and Practice of Forensic Science: The Profession of Forensic Science, 2000


Scope of
Forensic
Science

1. general toxicology;
2. firearms/toolmarks;
3. questioned documents;
4. trace evidence;
5. controlled substances;
6. biological/serology screening (including DNA analysis);
7. fire debris/arson analysis;
8. impression evidence;
9. blood pattern analysis;
10. crime scene investigation;
11. medicolegal death investigation; and
12. digital evidence.

reference:
Strengthening Forensic Science in the United States: A Path Forward

National Research Council, 2009

Digital Forensics and the Intersection with Spectrum Forensics

Steve Watson, VTO Labs

ISART 2016, Westminster, CO

Digital Forensics and the Intersection with Spectrum Forensics

Steve Watson, VTO Labs

ISART 2016, Westminster, CO


DIGITAL
FORENSICS


What is
Digital
Forensics

Digital evidence is information stored or transmitted in binary form that may be relied on in court.


History of
Digital
Forensics

1966 - First criminal prosecution with digital evidence resulting in a conviction.

1976 - Book Crime by Computer describes use of digital information to solve and prosecute crimes.

1993 - First International FBI conference on digital evidence.

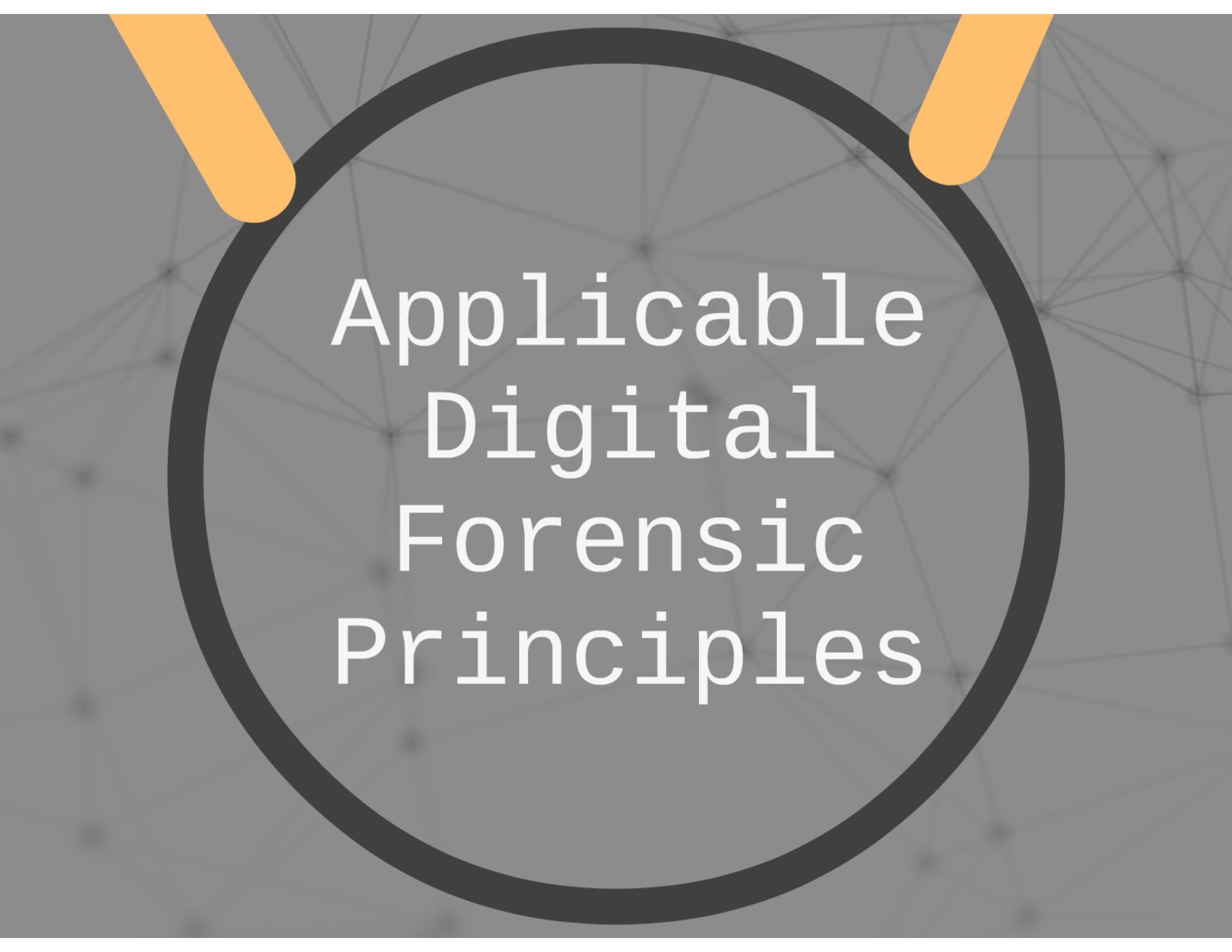
2006 - US Courts adopt Rules for Civil Procedure for addressing digital evidence in federal cases.


Scope of
Digital
Forensics


SPECTRUM
FORENSICS


Intersection
with
Digital
Forensics


New
techology
devices
utilizing
wireless
capability.


Applicable
Digital
Forensic
Principles

ACPO Good Practice Guide for Digital Evidence - UK ACPO

Principle 1:
No action taken by law enforcement agencies or their agents ***should change data*** held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:
In circumstances where a person finds it necessary ***to access original data*** held on a computer or on storage media, that ***person must be competent to do so*** and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:
An audit trail or other record of all processes applied to computer-based electronic evidence ***should be created and preserved***. An independent third party should be able to examine those processes and achieve the same result.

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, DOJ NIJ.

"general forensic and procedural principles"

1. ***Actions taken*** to secure and collect digital evidence ***should not affect*** the integrity of that ***evidence***.

2. ***Persons conducting an examination*** of digital evidence ***should be trained*** for that purpose.

3. ***Activity relating to*** the seizure, examination, storage, or transfer of ***digital evidence*** should be ***documented, preserved, and available*** for review.

Bottom line:

1. Don't alter evidence.
2. Personnel should be trained.
3. Activities should be logged.


Special
Considerations


Volatility
Location
Authentication

Volatility

Memory-resident or ephemeral data may be lost if not captured.

Is there volatile data on the devices you are securing?

Location is a frequent consideration when identifying new technology wireless devices.

UAS(drones), autonomous vehicles, robots, Internet-of-Things, mobile devices...

Authentication

What unique characteristics exists within the ***spectrum forensic*** captures...

...to connect the evidence to the equipment, location, individual?

Summary Thoughts

Is spectrum forensics, ***forensics***?

If yes...

There is significant movement occurring now in forensic sciences and digital forensics that you MUST be engaged in.

Resources:

ACPO Good Practice Guide for Digital Evidence.

Strengthening Forensic Science in the United States: A Path Forward.

ENISA Electronic evidence - a basic guide for First Responders

DOJ-NIJ Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders

DOJ-NIJ Forensic Examination of Digital Evidence: A Guide for Law Enforcement

Thank you!

VTO Labs

The art and science of digital forensics

stevewatson@vtolabs.com