Adapting Digital Forensics to New Problems

b!nalyze

Digital Forensics Timeline

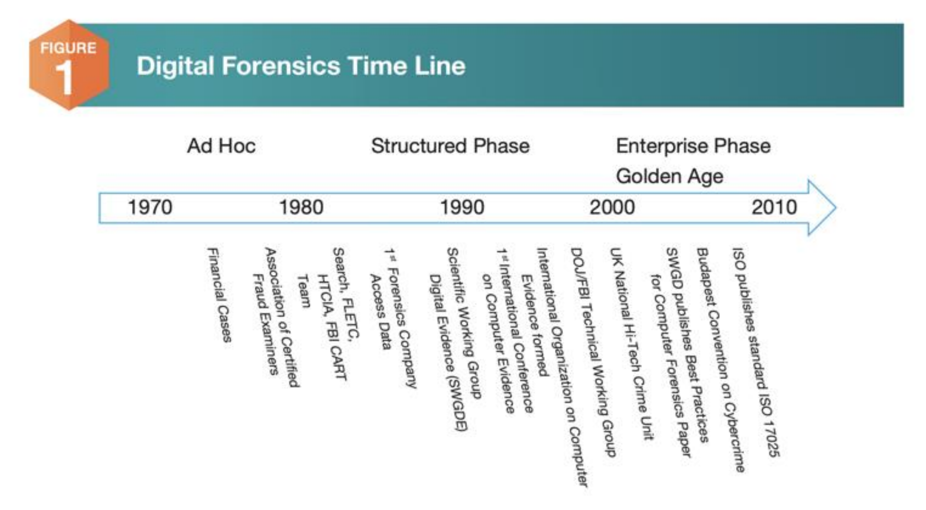


FIGURE 1
Digital Forensics Time Line
Ad Hoc
Structured Phase
Enterprise Phase
Golden Age
1970
1980
1990
2000
2010
Financial Cases
Association of Certified Fraud Examiners
Search, FLETC, HTCIA, FBI CART Team
1st Forensics Company Access Data
Scientific Working Group Digital Evidence (SWGDE)
1st International Conference on Computer Evidence
International Organization on Computer Evidence formed
DOJ/FBI Technical Working Group
UK National Hi-Tech Crime Unit
SWGD publishes Best Practices for Computer Forensics Paper
Budapest Convention on Cybercrime
ISO publishes standard ISO 17025

ISACA - Overview of Digital Forensics
https://informationsecurity.report/Resources/Whitepapers/9c6a1545-f876-48b6-9ca9-85f71e4d06cf_Overview-of-Digital-Forensics_whp_Eng_0315.pdf

Forensic Lab

Traditional Forensics is 40 years old, so are the methods

1. Unplug the drive (if you can)
2. Attach it to a disk duplicator (if you can)
3. Wait for hours (sometimes days)
4. Process the disk image (when you can)
5. Go to step 1 and repeat this N times

ISACA - Overview of Digital Forensics
https://informationsecurity.report/Resources/Whitepapers/9c6a1545-f876-48b6-9ca9-85f71e4d06cf_Overview-of-Digital-Forensics_whp_Eng_0315.pdf

The Source: Hard Drive

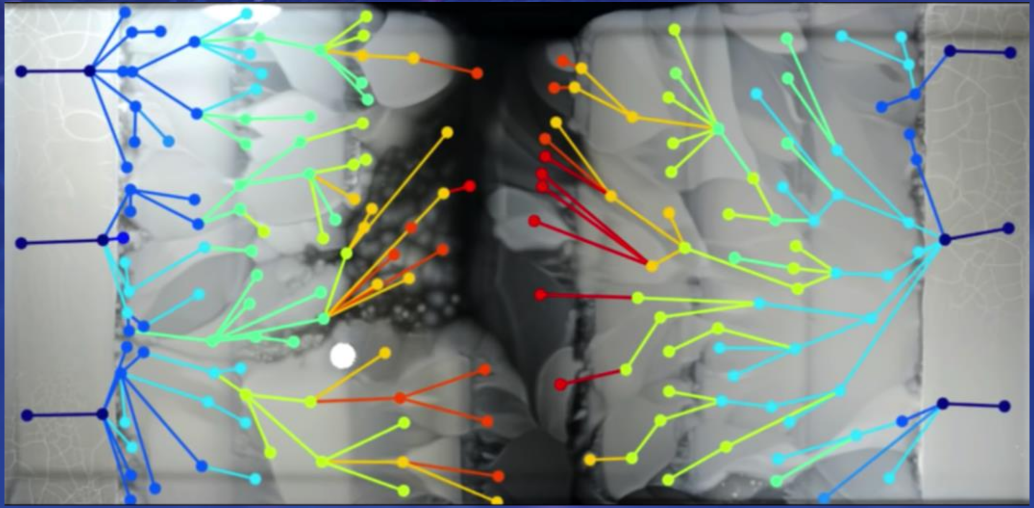
1984	1995	2006	2021
10MB	4-10GB	200GB	20TB

x2,000,000 in 35 years

https://en.wikipedia.org/wiki/History_of_hard_disk_drives

What needs to change?

Let the Nature "Answer it"



Question #1

Aren’t you “overriding” evidence?

(ref. Memory Forensics)

Yes. As much as every investigator does.

Question #2

Is the evidence accepted at the court?

Let’s take a look at the “Elements of a Case”

1. The existence of a legal duty that the defendant owed to the plaintiff
2. The defendant's breach of that duty
3. The plaintiff's sufferance of an injury
4. Proof that defendant's breach caused the injury

Elements of a Case
https://www.law.cornell.edu/wex/elements_(of_a_case)

Short Answer

In our era, priority #1 is to stop bleeding, find the smoking gun,
and business continuity.

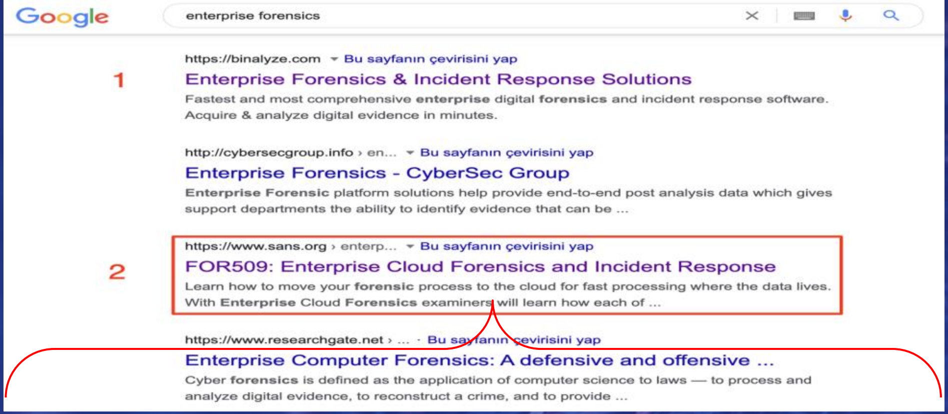
Court is not a priority until the case escalates.

New Era of Digital Forensics

Comparison

Traditional Forensics	What we need?
Slow	Fast
Physical	Remote
Reactive	Proactive
Siloed	Integrated
Noise	Signal
In Working Hours	24/7

An Emerging Industry



1
https://binalyze.com ▾ Bu sayfanın çevirisini yap
Enterprise Forensics & Incident Response Solutions
Fastest and most comprehensive **enterprise** digital **forensics** and incident response software. Acquire & analyze digital evidence in minutes.

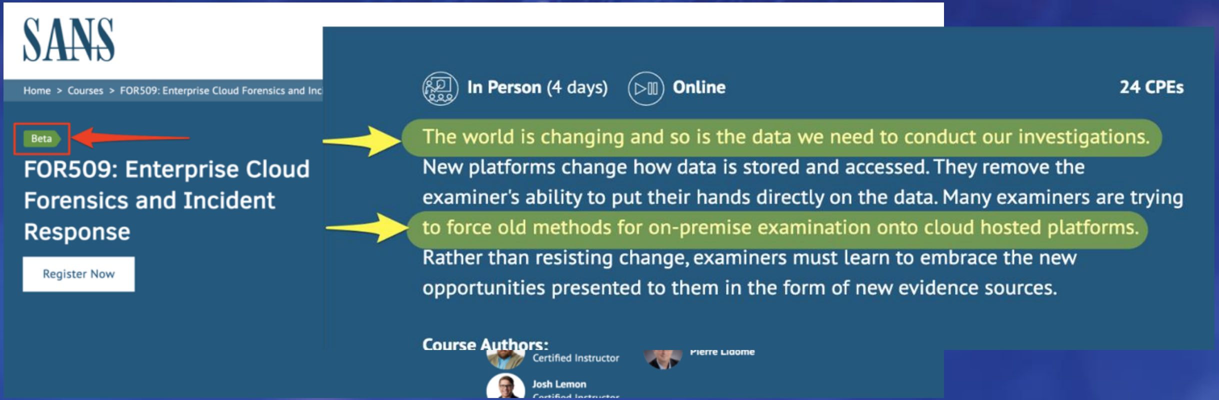
http://cybersecgroup.info › en... ▾ Bu sayfanın çevirisini yap
Enterprise Forensics - CyberSec Group
Enterprise Forensic platform solutions help provide end-to-end post analysis data which gives support departments the ability to identify evidence that can be ...

2
https://www.sans.org › enterp... ▾ Bu sayfanın çevirisini yap
FOR509: Enterprise Cloud Forensics and Incident Response
Learn how to move your **forensic** process to the cloud for fast processing where the data lives. With **Enterprise** Cloud **Forensics** examiners will learn how each of ...

https://www.researchgate.net › ... ▾ Bu sayfanın çevirisini yap
Enterprise Computer Forensics: A defensive and offensive ...
Cyber **forensics** is defined as the application of computer science to laws — to process and analyze digital evidence, to reconstruct a crime, and to provide ...

Gartner - Market Guide to Digital Forensics and Incident Response (2020)

Clients increasingly depend on vendors to dig deeper into incidents, providing advanced analytics and detailed forensics reporting. This requires IR providers to bring highly specialized combinations of products and processes to reduce the mean time to contain (MTTC) and mean time to remediate (MTTR) an active incident.

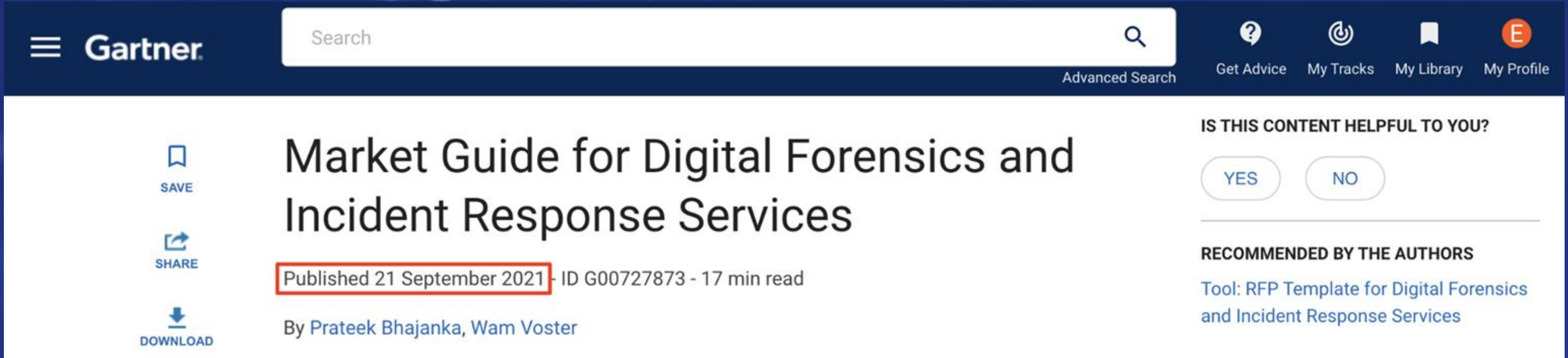


FOR509: Enterprise Cloud Forensics and Incident Response

The world is changing and so is the data we need to conduct our investigations. New platforms change how data is stored and accessed. They remove the examiner's ability to put their hands directly on the data. Many examiners are trying to force old methods for on-premise examination onto cloud hosted platforms. Rather than resisting change, examiners must learn to embrace the new opportunities presented to them in the form of new evidence sources.

Course Authors:
Certified Instructor
Pierre Lidome
Josh Lemon
Certified Instructor

Gartner 2021



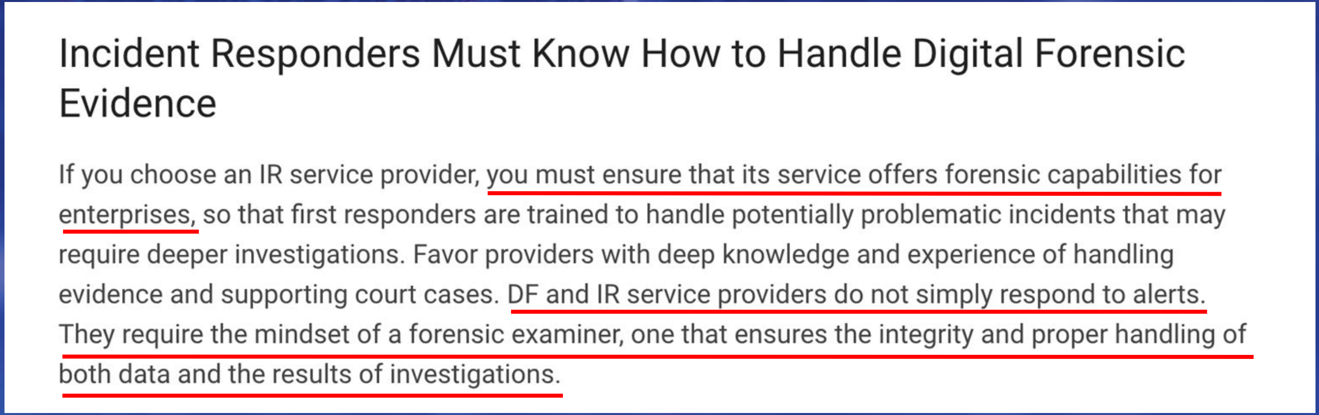
Market Guide for Digital Forensics and Incident Response Services

Published 21 September 2021 - ID G00727873 - 17 min read

By Prateek Bhajanka, Wam Voster

RECOMMENDED BY THE AUTHORS

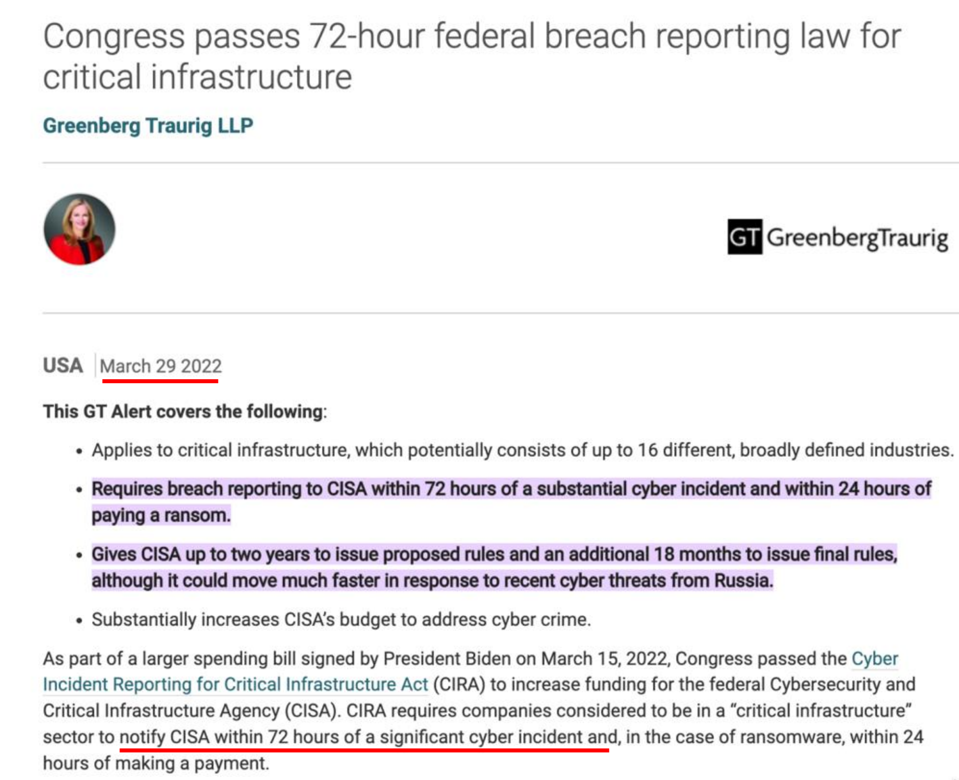
Tool: RFP Template for Digital Forensics and Incident Response Services



Incident Responders Must Know How to Handle Digital Forensic Evidence

If you choose an IR service provider, you must ensure that its service offers forensic capabilities for enterprises, so that first responders are trained to handle potentially problematic incidents that may require deeper investigations. Favor providers with deep knowledge and experience of handling evidence and supporting court cases. DF and IR service providers do not simply respond to alerts. They require the mindset of a forensic examiner, one that ensures the integrity and proper handling of both data and the results of investigations.

Regulations / US



Congress passes 72-hour federal breach reporting law for critical infrastructure

Greenberg Traurig LLP

GT GreenbergTraurig

USA | March 29 2022

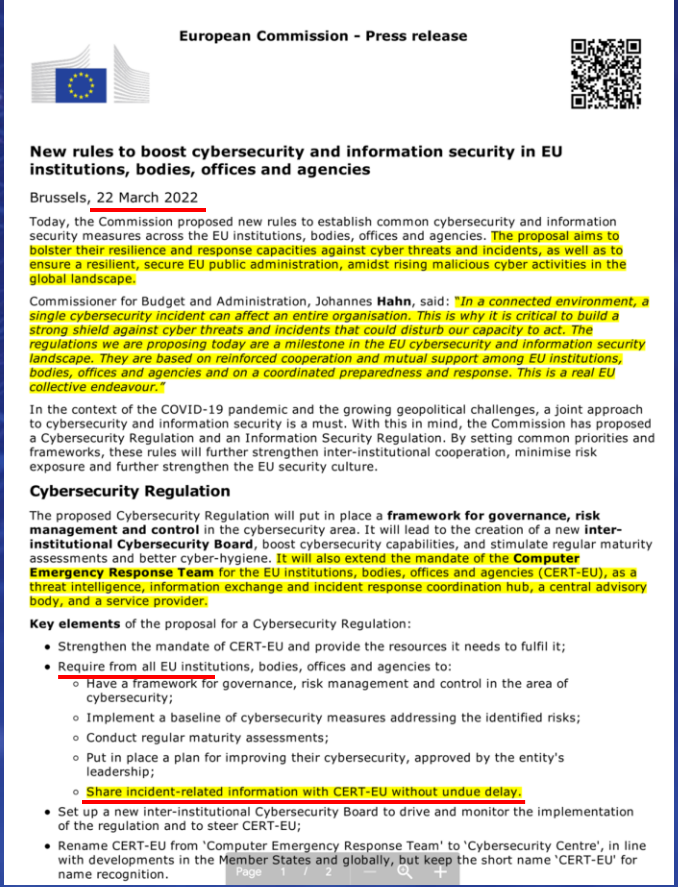
This GT Alert covers the following:

- Applies to critical infrastructure, which potentially consists of up to 16 different, broadly defined industries.
- **Requires breach reporting to CISA within 72 hours of a substantial cyber incident and within 24 hours of paying a ransom.**
- **Gives CISA up to two years to issue proposed rules and an additional 18 months to issue final rules, although it could move much faster in response to recent cyber threats from Russia.**
- Substantially increases CISA's budget to address cyber crime.

As part of a larger spending bill signed by President Biden on March 15, 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRA) to increase funding for the federal Cybersecurity and Critical Infrastructure Agency (CISA). CIRA requires companies considered to be in a "critical infrastructure" sector to notify CISA within 72 hours of a significant cyber incident and, in the case of ransomware, within 24 hours of making a payment.

https://www.lexology.com/library/detail.aspx?g=b70dd100-5026-4494-8b5a-7050ea4b5632

Regulations / EU



European Commission - Press release

New rules to boost cybersecurity and information security in EU institutions, bodies, offices and agencies

Brussels, 22 March 2022

Today, the Commission proposed new rules to establish common cybersecurity and information security measures across the EU institutions, bodies, offices and agencies. The proposal aims to bolster their resilience and response capacities against cyber threats and incidents, as well as to ensure a resilient, secure EU public administration, amidst rising malicious cyber activities in the global landscape.

Commissioner for Budget and Administration, Johannes **Hahn**, said: *"In a connected environment, a single cybersecurity incident can affect an entire organisation. This is why it is critical to build a strong shield against cyber threats and incidents that could disturb our capacity to act. The regulations we are proposing today are a milestone in the EU cybersecurity and information security landscape. They are based on reinforced cooperation and mutual support among EU institutions, bodies, offices and agencies and on a coordinated preparedness and response. This is a real EU collective endeavour."*

In the context of the COVID-19 pandemic and the growing geopolitical challenges, a joint approach to cybersecurity and information security is a must. With this in mind, the Commission has proposed a Cybersecurity Regulation and an Information Security Regulation. By setting common priorities and frameworks, these rules will further strengthen inter-institutional cooperation, minimise risk exposure and further strengthen the EU security culture.

Cybersecurity Regulation

The proposed Cybersecurity Regulation will put in place a **framework for governance, risk management and control** in the cybersecurity area. It will lead to the creation of a new **inter-institutional Cybersecurity Board**, boost cybersecurity capabilities, and stimulate regular maturity assessments and better cyber-hygiene. It will also extend the mandate of the **Computer Emergency Response Team** for the EU institutions, bodies, offices and agencies (CERT-EU), as a threat intelligence, information exchange and incident response coordination hub, a central advisory body, and a service provider.

Key elements of the proposal for a Cybersecurity Regulation:

- Strengthen the mandate of CERT-EU and provide the resources it needs to fulfil it;
- Require from all EU institutions, bodies, offices and agencies to:
  - Have a framework for governance, risk management and control in the area of cybersecurity;
  - Implement a baseline of cybersecurity measures addressing the identified risks;
  - Conduct regular maturity assessments;
  - Put in place a plan for improving their cybersecurity, approved by the entity's leadership;
  - Share incident-related information with CERT-EU without undue delay.
- Set up a new inter-institutional Cybersecurity Board to drive and monitor the implementation of the regulation and to steer CERT-EU;
- Rename CERT-EU from 'Computer Emergency Response Team' to 'Cybersecurity Centre', in line with developments in the Member States and globally, but keep the short name 'CERT-EU' for name recognition.

Cyber Security

↓

Cyber Resilience

Crime Scene Picture

Crime Scene Picture

“The highest resolution forensic snapshot that contains almost everything you need for an investigation so that you are not required to ask any further details”

Key Takeaways

- Digital Forensics is
  - Not a post-mortem job anymore
  - Not a nice-to-have capability
  - It is a must-have one
- It is a part of our daily lives whether you are a SOC Analyst or an MSSP
- Immediate visibility is the key for any investigation
- We “have to” embrace the modern approaches and rethink our priorities

Final Words

“Every contact leaves a trace”

Edmond Locard

The question is:

How much of it is visible to you and how fast you can have access to it?

Thank you

emre@binalyze.com