



# Elektronische Erfassung von Beweismitteln bei Nachprüfungen der Europäischen Kommission

**Dirk VAN ERPS**

Abteilungsleiter Kartelle II

Forensic IT Project Manager

Bonn, 5 December 2013



# Elektronische Beweismittelerfassung: Befugnisse

VO 1/2003, Art. 20(2):

"Die Bediensteten [...] sind befugt:

b) die Bücher und sonstigen Geschäftsunterlagen, unabhängig davon, in welcher Form sie vorliegen, zu prüfen;

c) Kopien oder Auszüge gleich welcher Art aus diesen Büchern und Unterlagen anzufertigen oder zu erlangen"



# Elektronische Beweismittelerfassung: Befugnisse

Das bedeutet:

- Wir dürfen elektronische Dokumente anschauen
- Wir dürfen elektronische Kopien von (elektronischen oder papierenen) Dokumenten anfertigen (Sehe Punkt 9 der 'Explanatory Note')



# Elektronische Beweismittelerfassung: Befugnisse

GD COMP hat im April 2013 damit angefangen,  
systematisch elektronische Kopien von  
elektronischen Dokumenten anzufertigen

GD COMP wird ab jetzt auch systematisch  
elektronische Kopien (Scans) von  
Papierdokumenten anfertigen



# Die überarbeitete "Explanatory Note"

Zweck:

- bietet dem Unternehmen Transparenz, wie ein FAQ
- wird am Anfang der Nachprüfung an Unternehmensvertreter überreicht
- ist im [internet](#) veröffentlicht

Ausschließlich zur Information und ohne Verbindlichkeit bezüglich formeller Auslegung der Untersuchungsbefugnisse



## Erläuterungen zur Fassung "18. 3. 2013"

- Mehr Beispiele von Dingen, die durchsucht werden:  
"Mobiltelefone, Laptops, Desktops, Tablets, CDs, DVDs, USB-key etc." (Punkt 10)
- Hinweis zur 'Verpflichtung zur vollständigen und aktiven Zusammenarbeit bei der Nachprüfung' (Punkt 11)
- Mehr Beispiele dazu:
  - "Erläuterung der Organisation und der IT Umgebung"



## Erläuterungen zur Fassung "18. 3. 2013"

- "zeitweilige Trennung laufender Rechner vom Netzwerk, Aus- und Einbau von Festplatten sowie Bereitstellung von Zugriffsrechten als Administrator"
- Möglichkeit, Hardware des Unternehmens zu verwenden (diese wird am Ende der Nachprüfung nicht von der Kommission "gewiped") (Punkt 11)
- Inspektoren können Datenträger bis zum Ende der Nachprüfung aufbewahren, oder nach Anfertigung einer forensischen Kopie vorher zurückgeben (Punkt 12)



## Erläuterungen zur Fassung "18. 3. 2013"

- Die Kommission "wiped" (löscht endgültig) alle kommissionseigenen Datenträger mit denen Daten transferiert worden sind (Punkt 13)
- Die überarbeitete Note wurde mit der Einführung der neuen Arbeitsweise veröffentlicht

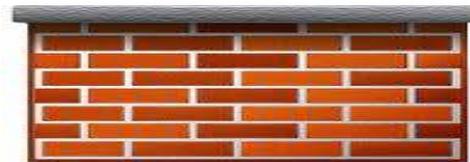


# Alte Arbeitsweise



IT Inspector

Company Computer  
No Dedicated Search Tools



DG COMP FIT Laptop  
Forensic Software

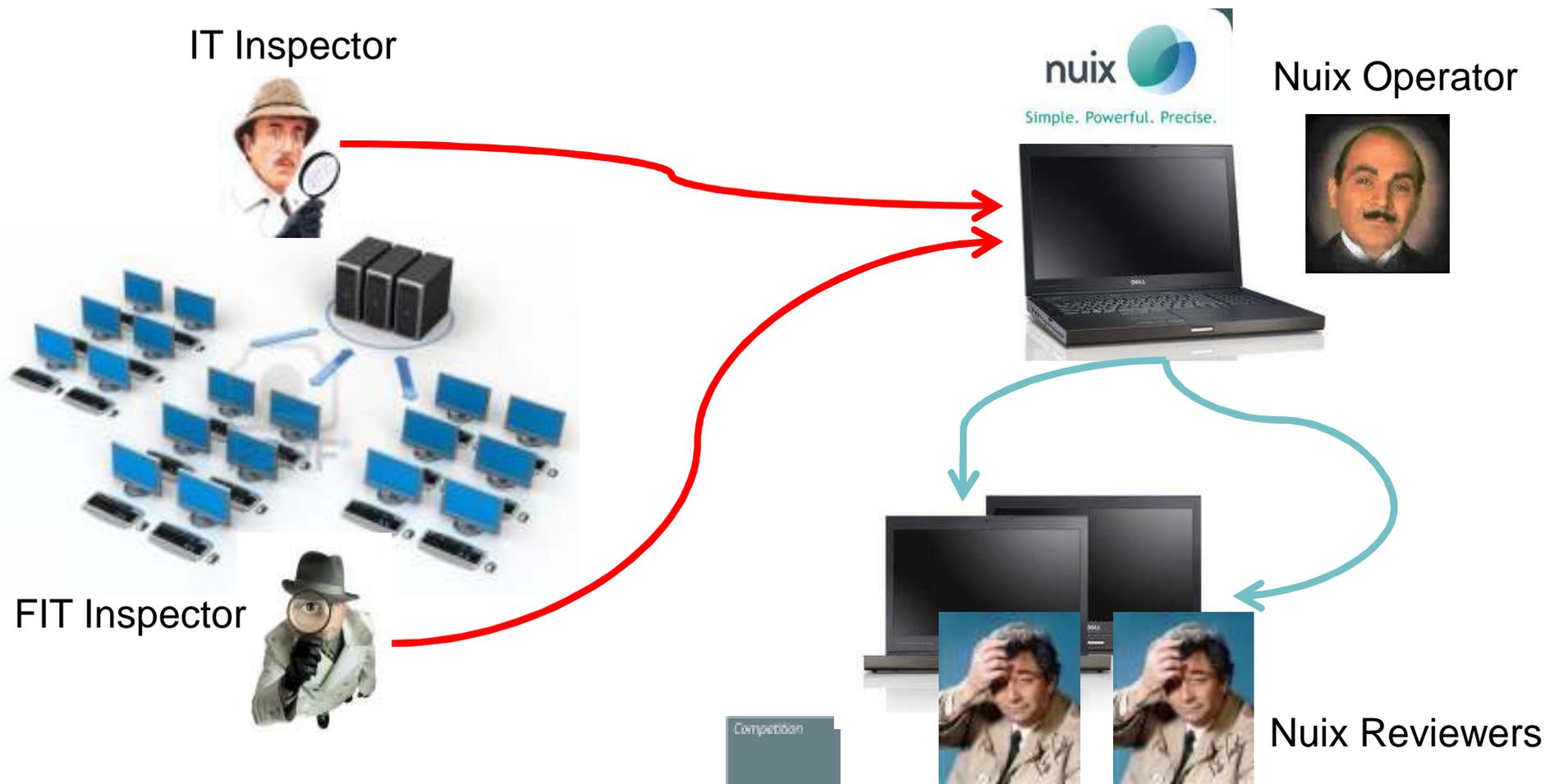


FIT Inspector

Competition



# Neue Arbeitsweise





# Die Methodik der elektronischen Überprüfung hat sich nicht geändert

- Möglicherweise relevante Dokumente werden "gesammelt" (kein systematisches "imaging" kompletter Inhalte, aber weiterhin Möglichkeit der forensischen Kopie von Desktops/Laptops)
- Möglicherweise relevante Dokumente werden indexiert
- Möglicherweise relevante Dokumente werden gesichtet, jetzt auf "Plattform" Basis
- Kommissionsbedienstete entscheiden welche Dokumente relevant sind
- Das Unternehmen erhält Liste(n) und Kopien der relevanten Dokumente



# Die Methodik der elektronischen Überprüfung hat sich nicht geändert

Prinzipiell wird die Überprüfung vor Ort und anhand der einzelnen Dokumenteninhalte durch einen Kommissionsbediensteten vorgenommen (im Beisein von Unternehmensvertretern)

Die Vorgehensweise "versiegelter Umschlag" ("continued inspection") bleibt Ausnahme:

- In der Vergangenheit in weniger als 10% der Fälle
- Oftmals auf Anfrage des Unternehmens (als 'Nuix' noch nicht vor Ort verfügbar war)



# Wir sind nicht verpflichtet

- Die Relevanz eines Dokumentes festzustellen, indem das "Kommissionsauge" jedes Dokument individuell anschaut (aber wir tun es)
- Unser Verständnis unserer Befugnisse zu erklären (aber wir tun es – Transparenz durch die "Inspection Explanatory Note")
- Die Arbeitsweise und Werkzeuge zu beschreiben (aber wir tun es – Artikel und Präsentationen wie diese)
- Unsere Werkzeuge bei Beendigung der Nachprüfung zu "säubern" (aber wir tun es - "Sanitize"/"Wipe")



# Juristische Fragen

- Serverstandort: unerheblich: zugänglich für die Kommissionsbediensteten ist alles, was für Angehörige des Unternehmens zugänglich ist
- LPP: kann vom 'search data' ausgenommen und vom Team-Leader mit Unternehmensvertretern getrennt behandelt werden
- Keywords: nicht ausgehändigt, da sie nur ein Hilfsmittel zur Auffindung der einzelnen möglicherweise relevanten Dokumente (welche ausgehändigt werden) sind
- Beweismittelkette: Unternehmen unterschreibt eine "Dokumentenliste", die Dokumente mit Namen und Zugriffspfad beschreibt; Hash Value für "Dokumentenbündel"



# Juristische Fragen

- "Continued inspection" oder "sealed envelope" Prozedur: Nexans/Prysmian Anfechtung (General Court): Maßnahme zur Durchführung eines Nachprüfungsentscheidung; keine eigenständige Maßnahme
- Persönliche Daten: Verarbeitung nach VO 45/2001 wie auf die Kommission anwendbar, stellt kein Hindernis für den Zugang zu den Daten dar
- Keine Harmonisierung von Vorgehensweise innerhalb ECN wohl aber Austausch von Erfahrungen und Methoden innerhalb der ECN Forensic IT Working Group



# DEMO

Vorstellung der Demo CD, welche dem betroffenen Unternehmen zu Beginn der Nachprüfung zur Erläuterung der Vorgehensweise zur Verfügung gestellt wird

Auf GD COMP Website veröffentlicht :

[http://ec.europa.eu/competition/antitrust/information\\_en.html#inspections](http://ec.europa.eu/competition/antitrust/information_en.html#inspections)



## Zum Schluss

Vielen Dank für Ihre Aufmerksamkeit  
Weitere Fragen?

[Dirk.Van-Erps@ec.europa.eu](mailto:Dirk.Van-Erps@ec.europa.eu)

\* Die vorgebrachten Aussagen geben persönliche Meinungen wieder und ziehen keinerlei Verpflichtung der Kommission nach sich