

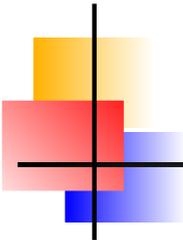
Trau, SCHAU, wem?

—

V-IDS oder eine andere Sicht der Dinge

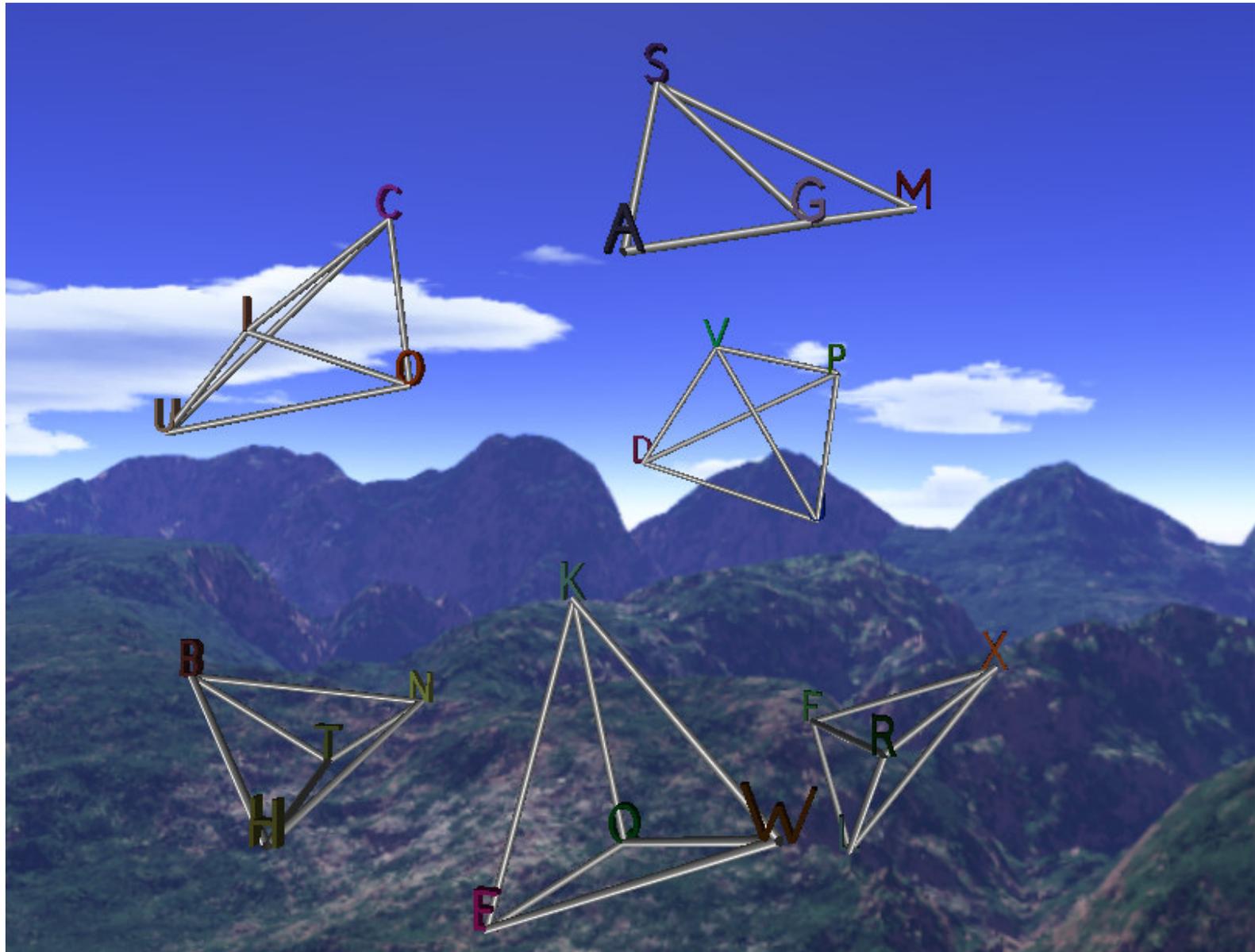
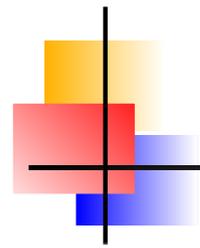
Björn Scheuermann Andreas Lindenblatt
Daniela Lindenblatt Benjamin Guthier

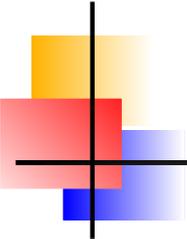
Solution – The Computer People, Mannheim, Germany



Problemstellung

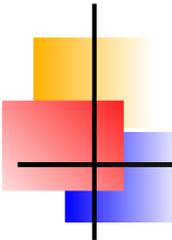
- ▶ Die Komplexität von Netzen wächst stetig
- ▶ Die Komplexität von Angriffen wächst stetig
- ▶ IT-Sicherheitstools werden immer ausgefeilter
- ▶ Dennoch: Komplexe, neuartige Situationen lassen sich nicht ausschließlich automatisiert analysieren





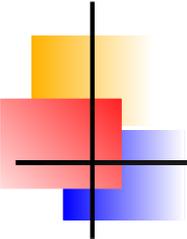
Problemstellung (2)

- ▶ **Der Mensch bleibt in der IT-Sicherheit auf absehbare Zeit der zentrale Informationsverarbeiter**
- ▶ Daher *zwei* wichtige Funktionen von Sicherheitssoftware:
 - ▶ Zugriffsschutz (Paket-Drops, Unterbinden von Dateizugriffen,...)
 - ▶ Generierung und Aufbereitung von Information für Analyse komplexerer Zusammenhänge durch den Menschen



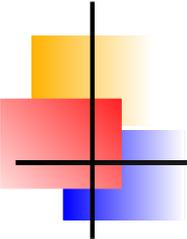
Problemstellung (3)

- ▶ Erstellung von spezialisierten Analysetools mit komplexen Darstellungsformen ist aufwändig
- ▶ Meist außerhalb des Fokus der Projekte
- ▶ Generische Tools könnten die Erstellung von spezialisierten Analyseanwendungen stark vereinfachen



Anforderungen

- ▶ Was müssten solche generischen Werkzeuge leisten?
 - ▶ Daten unterschiedlicher Quellen sollen kombiniert werden können
 - ▶ Tools sollen zur Echtzeit- und Protokollanalyse taugen
 - ▶ Intuitive Darstellungsformen sollen möglich sein
 - ▶ Analysewerkzeuge müssen leicht angepasst werden können an:
 - ▶ unterschiedliche Eingabedaten
 - ▶ unterschiedliche Darstellungsformen



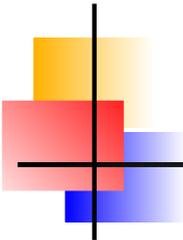
Anforderungen an Analysetools

- ▶ Entkoppeln von Datenquellen / Datenformaten und Darstellungsweise:

„Trennung von Inhalt und Layout“

- ▶ Entkoppeln von Darstellungsweise und Darstellungstechnik:

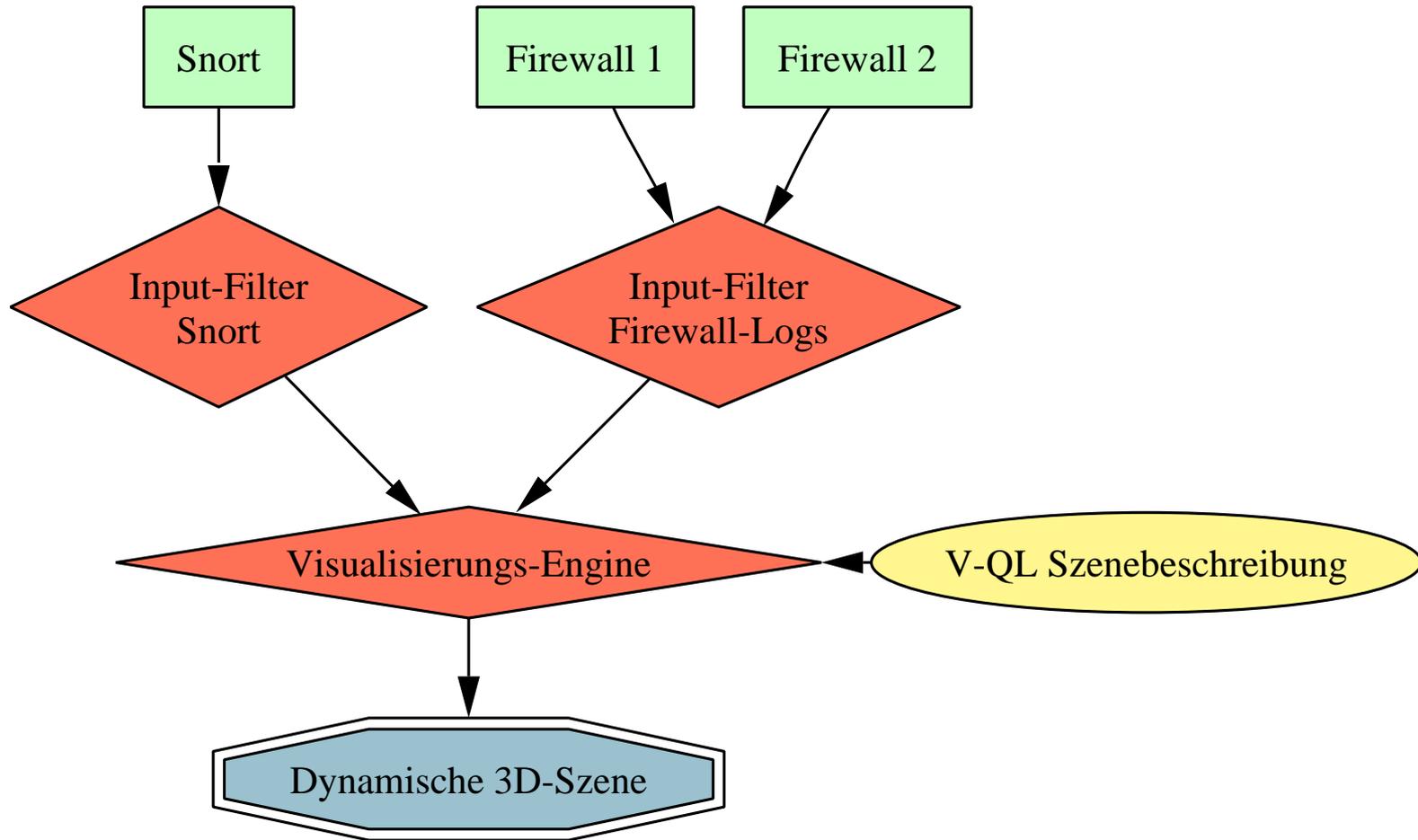
„Trennung von Layout und techn. Umsetzung“

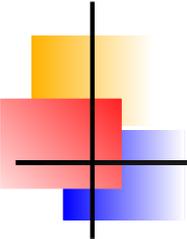


Generische Analysetools

- ▶ Dreiteilung der Aufgaben:
 - ▶ Bereitstellen der Daten in einem einheitlichen Format (datenquellenspezifisch)
 - ▶ Definition der Art und Weise der Darstellung (variabel, je nach konkretem Einsatz)
 - ▶ Tool, das die Daten einliest und entsprechend der Darstellungsdefinition aufbereitet
- ▶ V-IDS setzt diesen Ansatz für dreidimensionale, dynamische Darstellungen um

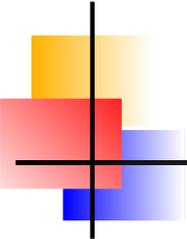
Architektur von V-IDS





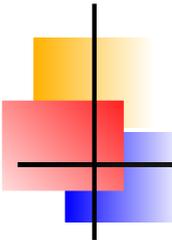
Entwurfsprinzipien

- ▶ Definitionssprache V-QL für Umsetzung der eingehenden Daten in eine 3D-Szene
- ▶ Szenendefinition soll das Abstrahieren von hardwarenahen Aspekten ermöglichen
- ▶ Einfache Aufgaben brauchen einfache Lösungen
- ▶ Die Definition einer Darstellungsweise ist *kein* Programm



Vorteile dieses Ansatzes

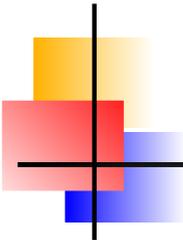
- ▶ Darstellungen zur gezielten Analyse einzelner Aspekte sind im Verdachtsfall leicht maßgeschneidert
- ▶ Angreifern wird ein gezieltes Verschleiern erschwert
- ▶ Austausch bewährter Darstellungen zwischen Anwendern bietet sich an



Freiheitsgrade bei 3D-Darstellung

- ▶ Form
- ▶ Oberfläche: Farbe, Textur, . . .
- ▶ Größe
- ▶ Position
- ▶ Dynamik: Änderung über die Zeit

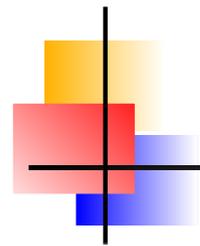
Diese Freiheitsgrade müssen sich zur Informationsvermittlung nutzen lassen!

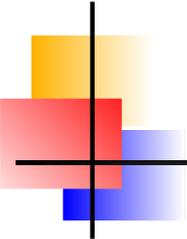


V-QL konkret

- ▶ Eine Zeile V-QL kann schon komplexe Objekte erstellen:

```
SHOW(Torus(0.4), Color([1,0,0]), Scale(2));
```





V-QL konkret

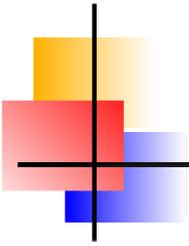
- ▶ Zwei Zeilen mehr: Bewegung kommt ins Spiel

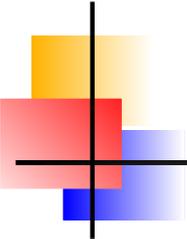
```
STATE angle = 0;
```

```
angle ~ = Pi;
```

```
SHOW(Torus(0.4), Color([1,0,0]),
```

```
  Rotate([0,1,0], angle) * Scale(2));
```





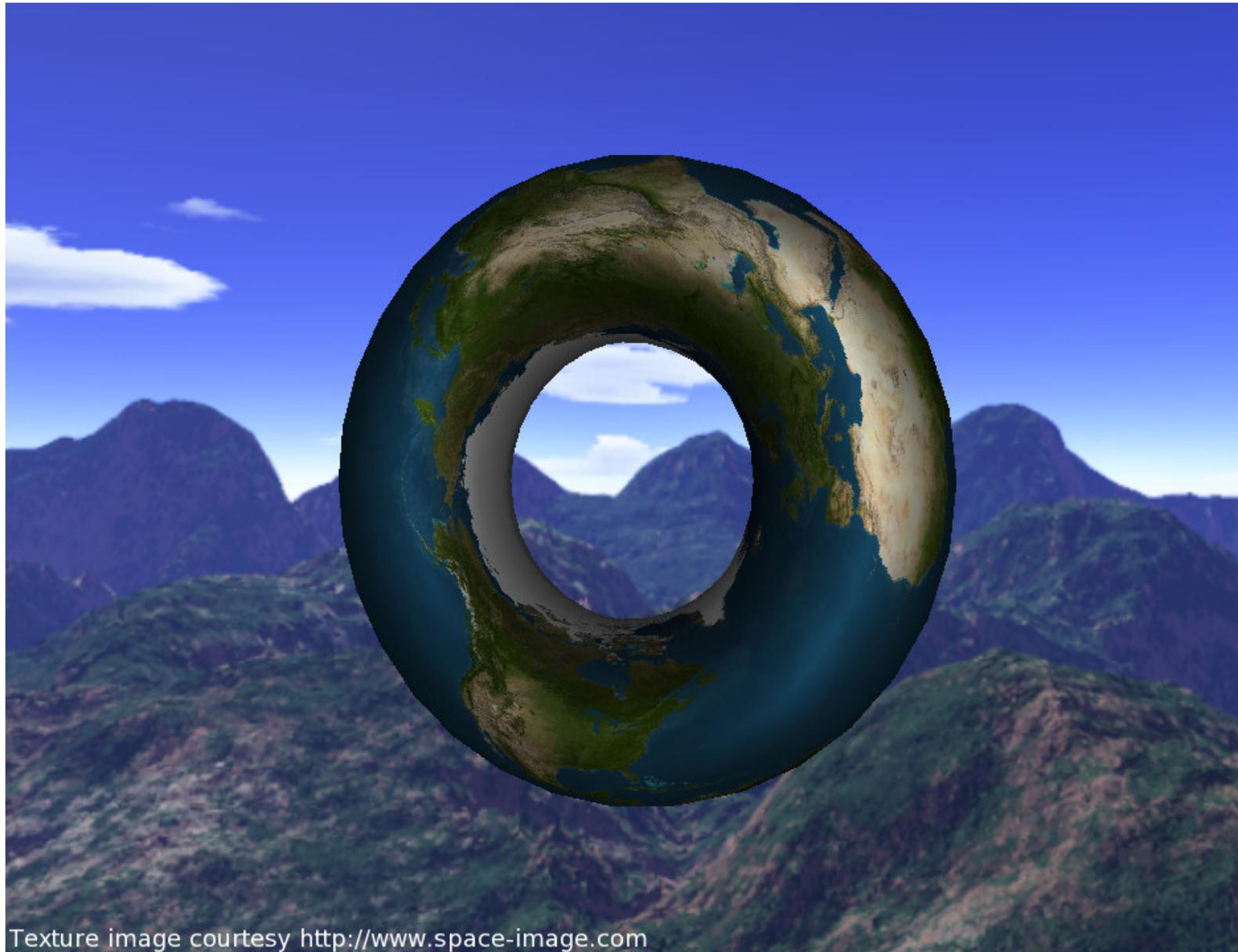
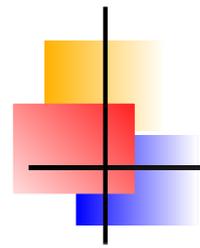
V-QL konkret

- ▶ Textur auf dem Torus:

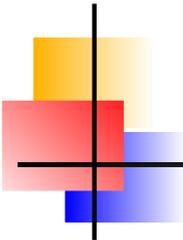
```
STATE angle = 0;
```

```
angle ~ = Pi;
```

```
SHOW(Torus(0.4), Texture([1,1,1], Image("map.png")),  
      Rotate([0,1,0], angle) * Scale(2));
```



Texture image courtesy <http://www.space-image.com>



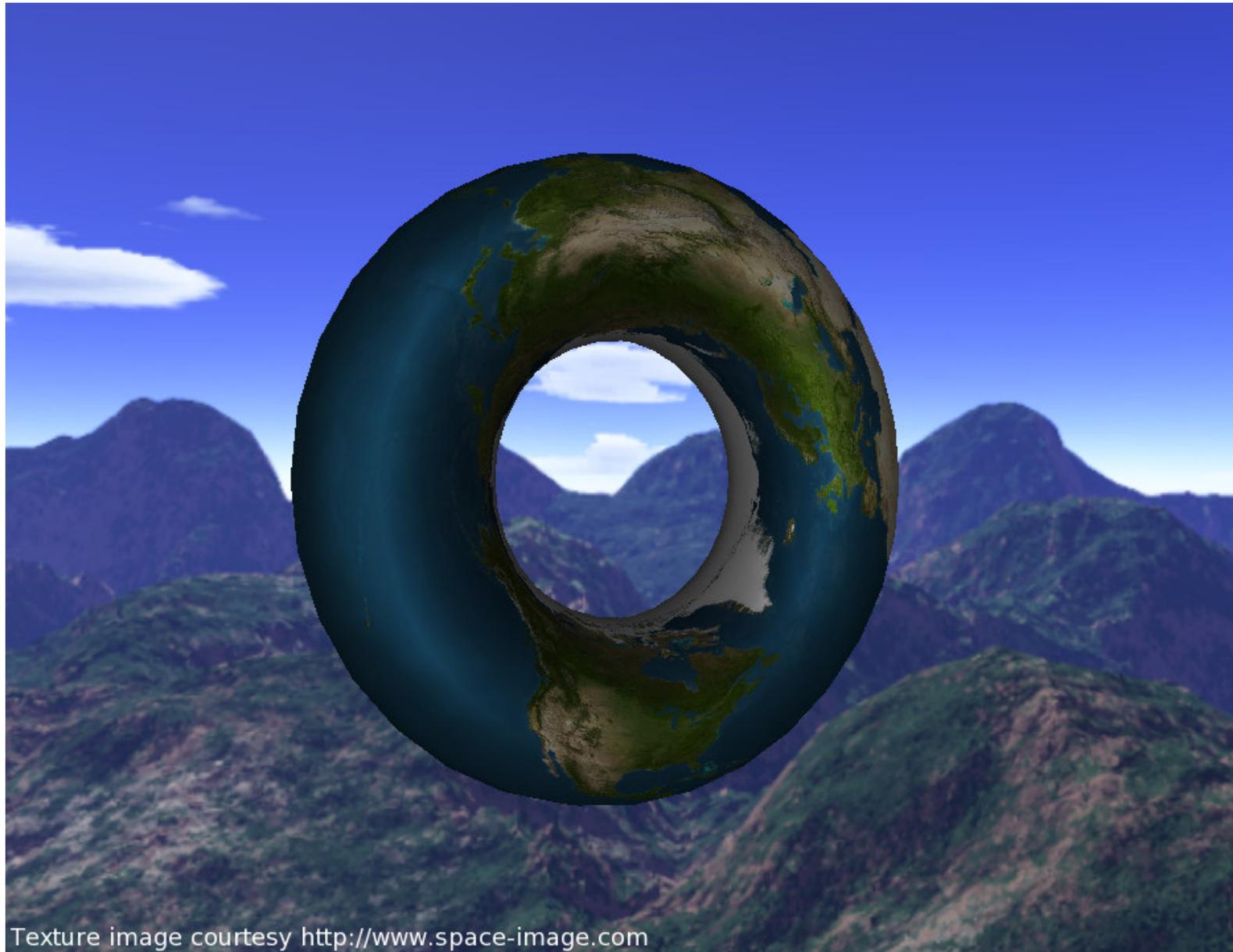
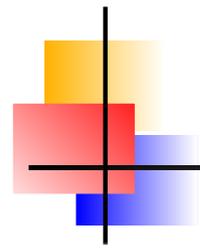
V-QL konkret

- ▶ Einbinden von Eingabegeräten:

```
STATE angle = 0;
```

```
angle ~ = Pi * JAxis(1);
```

```
SHOW(Torus(0.4), Texture([1,1,1], Image("map.png")),  
      Rotate([0,1,0], angle) * Scale(2));
```



Texture image courtesy <http://www.space-image.com>

► Mehrere Tori:

```
tori := SETOFSIZE(5);
```

```
EnumID tori->num;
```

```
IN tori {
```

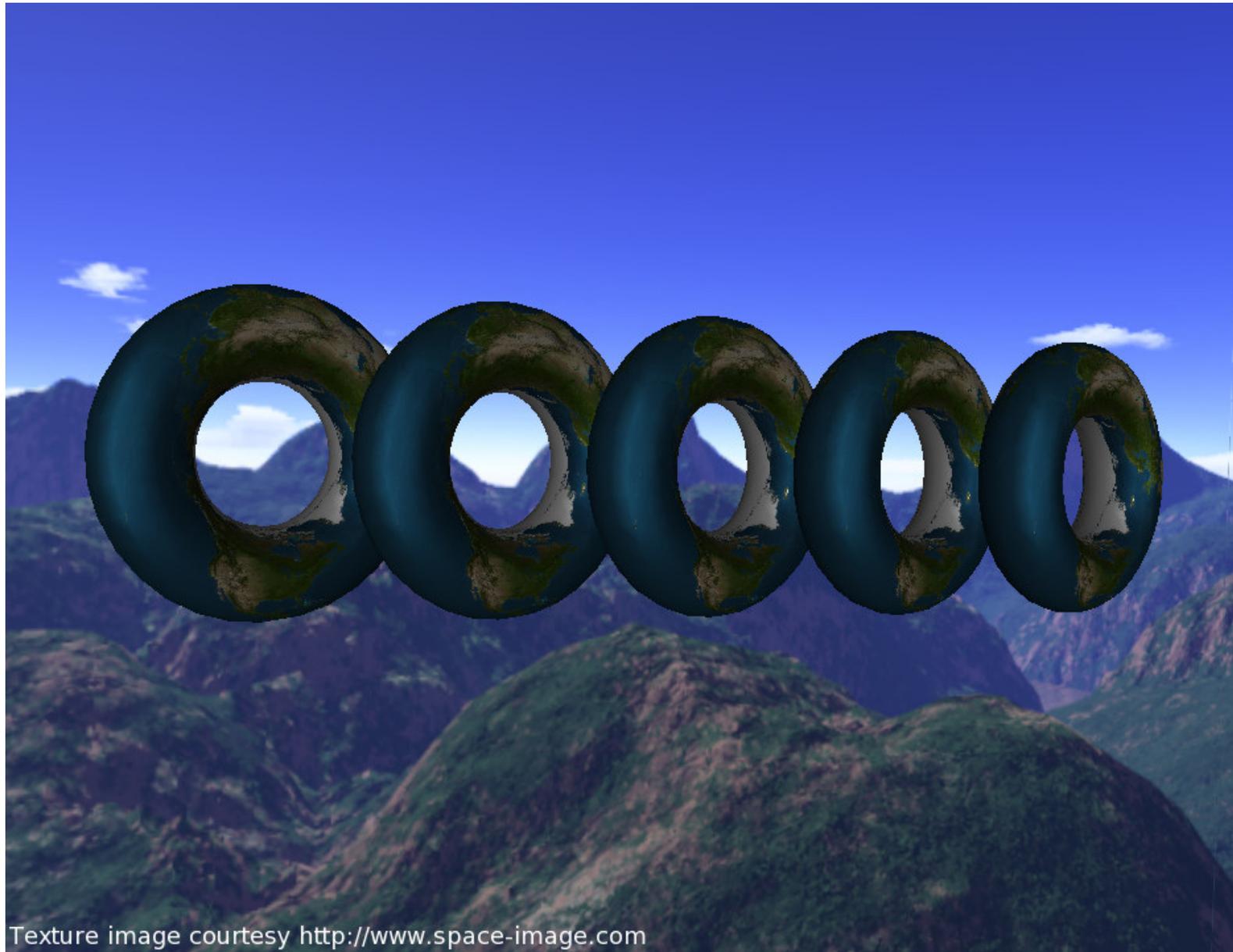
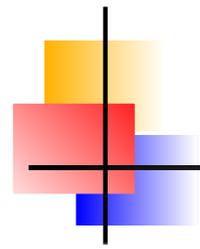
```
    STATE angle = 0;
```

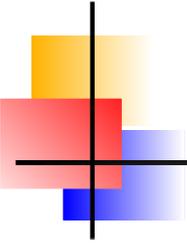
```
    angle ~ = Pi * JAxis(1);
```

```
    SHOW(Torus(0.4), Texture([1,1,1], Image("map.png")),
```

```
        Translate([num*2,0,0]) * Rotate([0,1,0], angle));
```

```
};
```



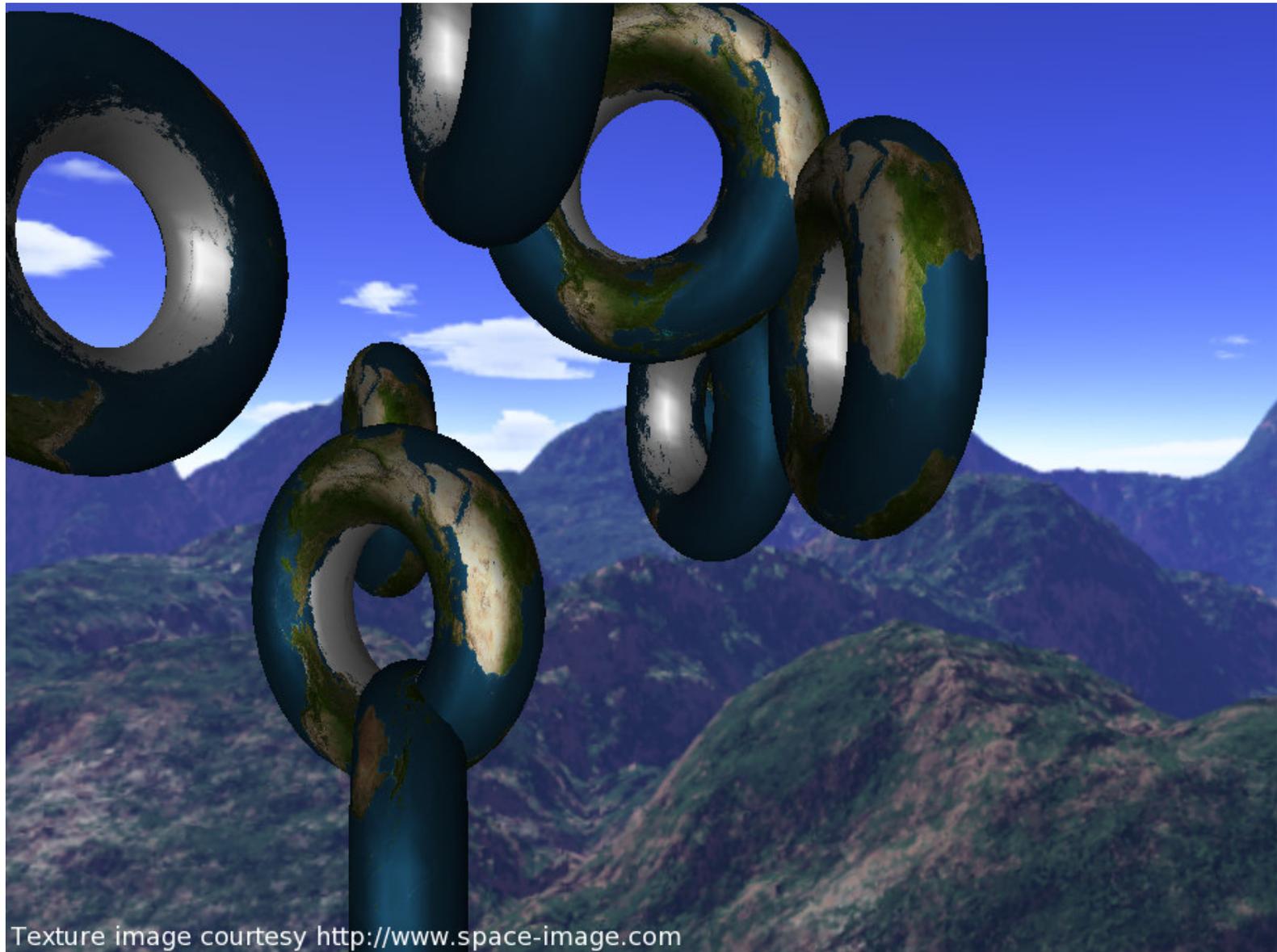
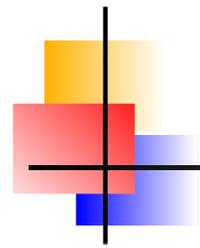


V-QL konkret

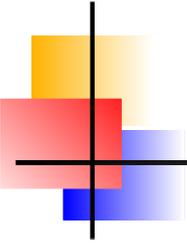
- ▶ Tori aus Eingabedaten:

```
INPUT tori {  
    position = [0,0,0];  
};
```

```
IN tori {  
    STATE angle = 0;  
    angle ~ = Pi * JAxis(1);  
    SHOW(Torus(0.4), Texture([1,1,1], Image("map.png")),  
        Translate(position) * Rotate([0,1,0], angle));  
};
```

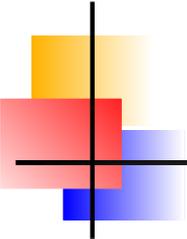


Texture image courtesy <http://www.space-image.com>



Was tut die VE?

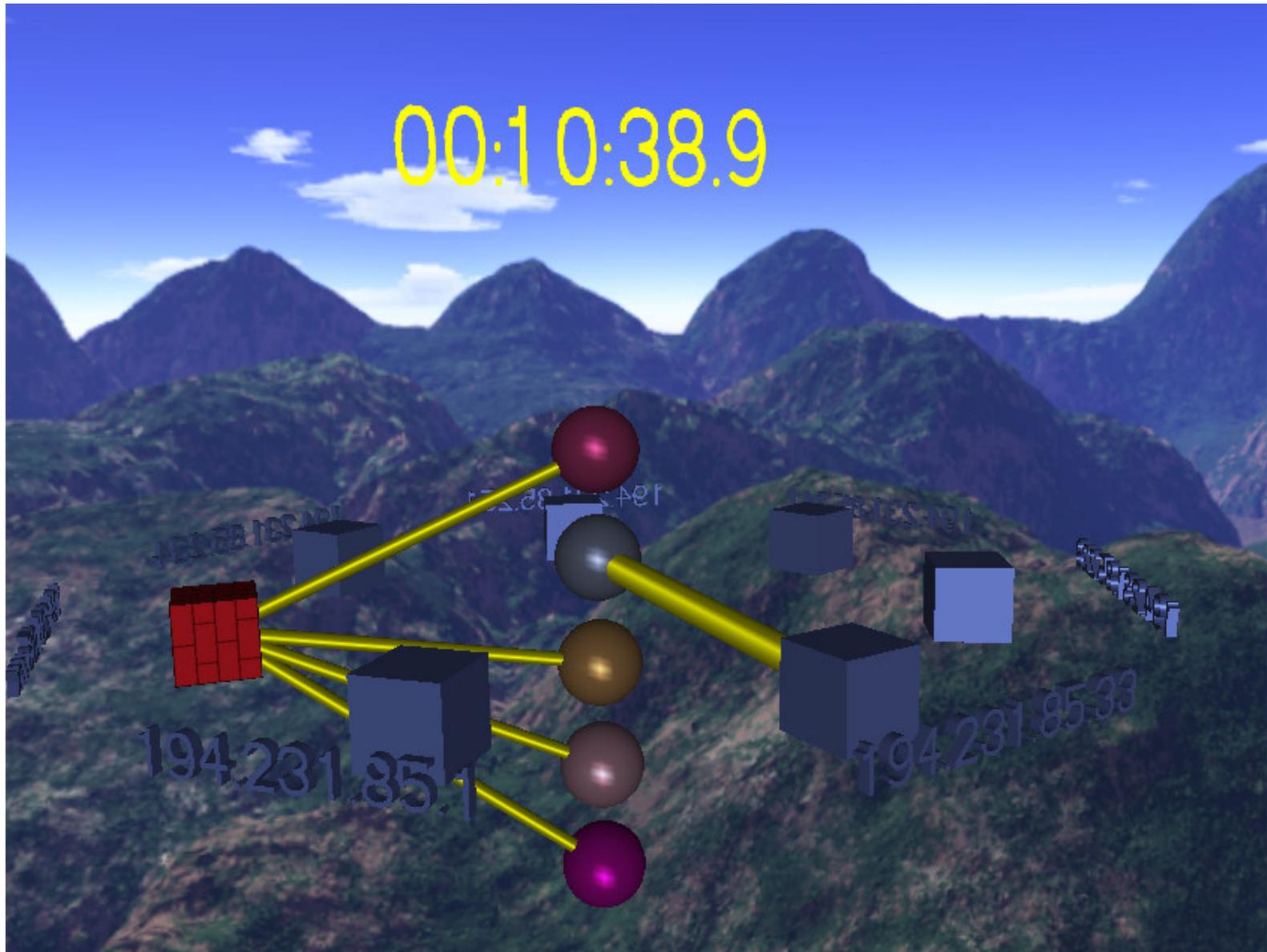
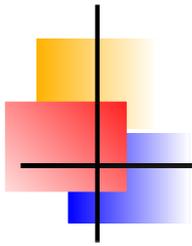
- ▶ Speicherverwaltung
- ▶ Erzeugen der 3D-Darstellung:
 - ▶ Geometrieberechnungen
 - ▶ Texturmapping
 - ▶ Kamerapositionierung
 - ▶ Clipping / Culling
- ▶ Frameratenunabhängige Bewegungen
- ▶ Festlegen der Berechnungsreihenfolge und Aktualisierungshäufigkeit
- ▶ ...

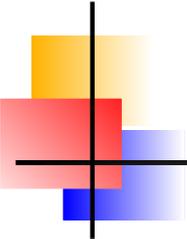


Real World Applications

Realistisches Einsatzszenario 1: Echtzeitdarstellung von Snort-Logs

- ▶ Feste Menge interner Ziel-IPs
- ▶ Darstellung aller externen IPs, die im Log auftauchen
- ▶ Anzahl der Events und maximaler Schweregrad durch Größe und Farbe der Verbindungslinie
- ▶ Class-C-Netz der IP durch deren Farbe
- ▶ In weniger als 60 Zeilen V-QL rudimentäre, aber einsatzbereite Szenendefinition



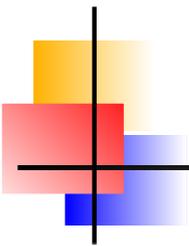


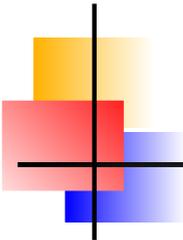
Real World Applications

Realistisches Einsatzszenario 2:

Wireless-LAN-Simulationsdaten (ns-2)

- ▶ Entwicklung und Analyse von mobilen Ad-Hoc-Routing-Algorithmen
- ▶ Darstellung aller MAC-Layer-Übertragungen
- ▶ non-real-time, non-linear-time





Fazit

- ▶ Vieles deutet darauf hin, dass dreidimensionale grafische Darstellungen die Analyse von Sicherheitsdaten erleichtern können
- ▶ Die Erfahrungen bezüglich geeigneter Darstellungsformen sind noch sehr eingeschränkt
- ▶ V-IDS als generisches Tool lässt sich sowohl an neue Datenquellen als auch in Bezug auf die Darstellungsform innerhalb großer Grenzen anpassen
- ▶ Die nächste Herausforderung: Darstellungsformen entwickeln, testen, Erfahrungen sammeln